Overview Report: Financial Action Task Force

I. Scope of Overview Report

1. This overview report describes the Financial Action Task Force ("**FATF**") and attaches documents created by the FATF and/or FATF-style regional bodies ("**FSRBs**").

II. The FATF and FSRBs

2. The FATF is an independent international body established at the initiative of the G7 in 1989.[1] The FATF currently comprises 37 member-jurisdictions[2] and two regional organizations,[3] representing most major financial centres in all parts of the globe, including Canada,[4] one of the 16 founding members of the FATF.[5]

3. There are also 32 international and regional organizations which are Associate Members or Observers of the FATF and participate in its work.[6] Among these are nine FSRBs, each with their own membership. The nine FSRBs include:[7]

---

[1] Maria Bergström, "The Global AML Regime and the EU AML Directives: Prevention and Control" in Colin King, Clive Walker and Jimmy Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Law* (London: Palgrave Macmillan, 2018) at 35-36; Doug Hopton, *Money Laundering*, 2nd ed. (London: Gower, 2016) at 8.

2 Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, Greece, Hong Kong, China, Iceland, India, Ireland, Israel, Italy, Japan, Republic of Korea, Luxembourg, Malaysia, Mexico, Netherlands, Kingdom of, New Zealand, Norway, Portugal, Russian read down, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States: Financial Action Task Force, "FATF Members and Observers" (2019) online: *FATF* <https://www.fatf-gafi.org/about/membersandobservers/>

[3] European Commission, Gulf Co-operation Council: Financial Action Task Force, "FATF Members and Observers" (2019) online: *FATF* <https://www.fatf-gafi.org/about/membersandobservers/>

[4] Financial Action Task Force, "FATF Members and Observers" (2019) online: *FATF* <https://www.fatf-gafi.org/about/membersandobservers/>.

[5] Financial Action Task Force, "FATF Members and Observers" (2019) online: *FATF* <https://www.fatf-gafi.org/about/membersandobservers/>; Financial Action Task Force, "History of the FATF" (2019) online: *FATF* <https://www.fatf-gafi.org/about/historyofthefatf/>; Financial Action Task Force, " Canada" online: *FATF* <https://www.fatf-gafi.org/countries/#Canada>; FATF (2019), Financial Action Task Force – 30 years, FATF, Paris <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF30-(1989-2019).pdf> at 10.

[6] Financial Action Task Force, "FATF Members and Observers" (2019) online: *FATF* <https://www.fatf-gafi.org/about/membersandobservers/>.

[7] Asia-Pacific Group on Money Laundering, "APG History and Background" (2020) online: *APG* < http://www.apgml.org/about-us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162>. The nine FSRBs include the Asia/Pacific Group on Money Laundering, the Caribbean Financial Action Task Force, the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, the Eurasian Group, the Eastern and Southern Africa Anti-Money Laundering Group, the Financial Action Task Force of Latin America, the Inter Governmental Action Group against

a. The Asia/Pacific Group on Money Laundering ("**APG**") – 41 members[8]

b. The Caribbean Financial Action Task Force ("**CFATF**") – 25 members[9]

c. The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism ("**MONEYVAL**") – 34 members[10]

d. The Eurasian Group ("**EAG**") – 9 members[11]

e. The Eastern and Southern Africa Anti-Money Laundering Group ("**ESAAMLG**") – 18 members[12]

f. The Financial Action Task Force of Latin America ("**GAFILAT**") – 17 members[13]

g. The Inter Governmental Action Group against Money Laundering in West Africa ("**GIABA**") – 16 members[14]

h. The Middle East and North Africa Financial Action Task Force ("**MENAFATF**") – 21 members[15]

i. The Task Force on Money Laundering in Central Africa ("**GABAC**") – 7 members[16]

Money Laundering in West Africa, the Middle East and North Africa Financial Action Task Force and the Task Force on Money Laundering in Central Africa: Financial Action Task Force, "FATF Members and Observers" (2019) online: *FATF* <https://www.fatf-gafi.org/about/membersandobservers/>.

[8] Asia/Pacific Group on Money Laundering, "Asia/Pacific Group on Money Laundering" (2020) online" *APG* <http://www.apgml.org/>.

[9] Caribbean Financial Action Task Force, *CFATF Annual Report 2018-2019* (2020) < https://www.cfatf-gafic.org/home/cfatf-overview/cfatf-annual-reports/13810-cfatf-annual-report-2018-2019/file>.

[10] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, "Jurisdictions" (2020) online: *Council of Europe* < https://www.coe.int/en/web/moneyval/jurisdictions>.

[11] Eurasian Group, "About EAG" (2020) online: *Eurasian Group* <https://eurasiangroup.org/en>.

[12] Eastern and Southern Africa Anti-Money Laundering Group, "Who we are" (2018) online: *ESAAM* <https://www.esaamlg.org/index.php/about>.

[13] Financial Action Task Force of Latin America, "El Organismo Internacional" online: *GAFILAT* <http://www.gafilat.org/index.php/es/gafilat/quienes-somos/organismo-internacional>.

[14] Inter Governmental Action Group Against Money Laundering in West Africa, "Member States" (2012) online <https://www.giaba.org/member-states/index_-1.html>.

[15] Middle East and North Africa Financial Action Task Force, "MENAFATF Members" (2018) online *MENAFATF* <http://www.menafatf.org/about/Members-Observers/members>.

[16] Financial Action Task Force, "GABAC" (2019) online: *FATF* <https://www.fatf-gafi.org/pages/gabac.html>.

4. The objectives of the FATF, as articulated in its open-ended mandate, approved on April 12, 2019, "are to protect financial systems and the broader economy from threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security.[17]

5. The mandate identifies the FATF's "functions and tasks" as follows:[18]

a. Identifying and analysing money laundering, terrorist financing and other threats to the integrity of the financial system, including the methods and trends involved; examining the impact of measures designed to combat misuse of the international financial system; supporting national, regional and global threat and risk assessments;

b. Developing and refining the international standards for combating money laundering and the financing of terrorism and proliferation (the FATF Recommendations) to ensure that they are up-to-date and effective;

c. Assessing and monitoring its Members, through 'peer reviews' ('mutual evaluations') and follow-up processes, to determine the degree of technical compliance, implementation and effectiveness of systems to combat money laundering and the financing of terrorism and proliferation; refining the standard assessment methodology and common procedures for conducting mutual evaluations and evaluation follow-up;

d. Identifying and engaging with high-risk, non-co-operative jurisdictions and those with strategic deficiencies in their national regimes, and co-ordinating action to protect the integrity of the financial system against the threat posed by them;

e. Promoting full and effective implementation of the FATF Recommendations by all countries through the global network of FATF-style regional bodies (FSRBs) and international organisations; ensuring a clear understanding of the FATF standards and consistent application of mutual evaluation and follow-up processes throughout the FATF global network and strengthening the capacity of the FSRBs to assess and monitor their member countries, including through standards training and outreach;

[17] Financial Action Task Force, "Mandate" (12 April 2019) <http://www.fatf-gafi.org/media/fatf/content/images/FATF-Ministerial-Declaration-Mandate.pdf> at 5.
[18] Financial Action Task Force, "Mandate" (12 April 2019) <http://www.fatf-gafi.org/media/fatf/content/images/FATF-Ministerial-Declaration-Mandate.pdf> at 5-6.

f. Responding as necessary to significant new and emerging threats and risks to the integrity of the financial system consistent with the needs identified by the international community, including the United Nations Security Council, the G20 and the FATF itself; preparing guidance as needed to facilitate implementation of relevant international obligations in a manner compatible with the FATF standards (e.g. continuing work on money laundering, terrorist financing, including new and emerging trends, and other misuse of the financial system relating to corruption);

g. Assisting jurisdictions in implementing financial provisions of the United Nations Security Council resolutions on terrorism and non-proliferation, assessing the degree of implementation and the effectiveness of these measures in accordance with the FATF mutual evaluation and follow-up process, and preparing guidance as needed to facilitate implementation of relevant international obligations in a manner compatible with the FATF standards;

h. Maintaining engagement with other international organisations and bodies, in particular the United Nations, to increase the outreach of the activities and objectives of the FATF;

i. Engaging and consulting with the private sector and civil society on matters related to the overall work of the FATF, through the annual consultative forum and other methods for maintaining regular contact to foster transparency and dialogue towards more effective implementation of the FATF standards;

j. Undertaking any new tasks agreed by its Members in the course of its activities and within the framework of this Mandate; and taking on these new tasks only where it has a particular additional contribution to make while avoiding duplication of existing efforts elsewhere.

6. The FATF is comprised of the following internal structures:[19]

a. The Plenary;
b. The President, assisted by a Vice-President;
c. The Steering Group; and
d. The Secretariat.

[19] Financial Action Task Force, “Mandate” (12 April 2019) <http://www.fatf-gafi.org/media/fatf/content/images/FATF-Ministerial-Declaration-Mandate.pdf> at 7.

7. The role of each of these structures is addressed in detail in the FATF mandate.[20]

8. Operationally, the FATF is organized and divided among five working groups with the following responsibilities:[21]

a. ***Evaluation and compliance group*** – assessing and monitoring members, through 'peer reviews' and follow-up processes to determine the effectiveness of a country's measures to combat money laundering and the financing of terrorism and proliferation, and their technical compliance with the FATF Recommendations.[22]

b. ***Policy development group*** – developing and refining the international standards for combating money laundering and the financing of terrorism and proliferation (the FATF Recommendations).

c. ***Risk, Trends and Methods group*** – identifying and analyzing money laundering, terrorist financing and other threats to the integrity of the financial system.

d. ***International Cooperation and Review group*** – identifying and engaging with high-risk and non-cooperative jurisdictions and those with strategic deficiencies in their national regimes.

e. ***Global network coordination group*** – promoting full and effective implementation of the FATF Recommendations by all countries through the global network of FSRBs and international organizations.

9. Canada is a member of the APG. The objective of the APG is to ensure the adoption, implementation and enforcement of internationally accepted anti-money laundering and counter-terrorist financing FATF standards.[23]

10. The APG assists countries and territories of the region in: enacting laws to deal with proceeds of crime, mutual legal assistance, confiscation, forfeiture and extradition;

---

[20] Financial Action Task Force, "Mandate" (12 April 2019) <http://www.fatf-gafi.org/media/fatf/content/images/FATF-Ministerial-Declaration-Mandate.pdf> at 7-10.
[21] Financial Action Task Force, "FATF Secretariat" (2019) online: *FATF* <https://www.fatf-gafi.org/about/fatfsecretariat/>.
[22] Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures Canada Mutual Evaluation Report, September 2016* (Paris: FATF, 2016) < https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf>.
[23] Financial Action Task Force, "APG" (2019) online: *FATF* <http://www.fatf-gafi.org/countries/#APG>.

providing guidance in setting up systems for reporting and investigating suspicious transactions; and helping in the establishment of financial intelligence units. The APG also ensures that regional factors are taken into account in the implementation of anti-money laundering measures.[24] It identifies its five "primary functions" as follows:[25]

a. **Mutual evaluations:** The APG assesses the levels of compliance by its member jurisdictions with the global AML/CFT standards through a mutual evaluation (peer review) programme.

b. **Technical assistance and training**: The APG Secretariat coordinates bi-lateral and donor-agency technical assistance and training in the Asia/Pacific region for its member jurisdictions in order to improve compliance with the global standards;

c. **Typologies research**: Research and analysis into money laundering and terrorist financing methods and trends is a key function of the APG to assist policy and law makers as well as law enforcement agencies and the general public to identify and respond to new and emerging trends, methods, risks and vulnerabilities;

d. **Global engagement**: The APG contributes to international AML/CFT policy development and actively engages with the global network of FSRBs. The APG also participates in a number of FATF working groups and in its plenary meetings; and

e. **Private sector engagement**: Private sector engagement is critical to the APG's overall objectives. The APG actively engages with financial and non-financial institutions, NPOs, training centres and universities in the Asia-Pacific to better inform the general public and specialists about global issues relating to money laundering, terrorist financing and proliferation financing.

11. Canada is also a Cooperating and Supporting Nation ("**COSUN**") of the CFATF along with France, Mexico, the Netherlands, Spain, the United Kingdom and the United States of America. COSUNs are "countries or territories that are not members or observers of the CFATF and which have expressed support for the objectives of the

[24] Financial Action Task Force, "APG" (2019) online: *FATF* <http://www.fatf-gafi.org/countries/#APG>.
[25] Asia/Pacific Group on Money Laundering, "APG History and Background" (2020) online" *APG* <http://www.apgml.org/about-us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162>.

CFATF and have been approved by the [CFATF] Council of Ministers. COSUNs make such contributions to the work and/or resources of the CFATF as are permitted by their respective national laws and policies."[26]

III. The FATF 40 Recommendations

12. In April 1990, the FATF issued a report containing a set of *Forty Recommendations*, intended to provide a comprehensive plan of action to fight money laundering.[27]

13. The original 1990 recommendations are attached as Appendix 'A'.

14. In 1991, the FATF began monitoring its members' implementation of the *Forty Recommendations* through a self-assessment process.[28]

15. In 1996, the FATF approved revisions to the *Forty Recommendations* issued in 1990. The revisions were intended to reflect evolving money laundering trends and techniques, and to broaden the scope of the recommendations to encompass the proceeds of predicate offences other than drug offences.[29]

16. The 1996 revised recommendations are attached as Appendix 'B'.

17. In October 2001, following the terrorist attacks of September 11, 2001, the FATF issued *Eight Special Recommendations* to address the issue of terrorist financing.[30] In

[26] Caribbean Financial Action Task Force, "How are we organized?" (2020) online: *CFATF* < cfatf-gafic.org/how-are-we-organized#COSUNs%20and%20Observers>.
[27] Financial Action Task Force, "History of the FATF" (2019) online: *FATF* <https://www.fatf-gafi.org/about/historyofthefatf/>; Financial Action Task Force, *The Forty Recommendations of the Financial Action Task Force on Money Laundering* (Paris: FATF, 1990).
[28] FATF, *Financial Action Task Force – 30 years* (Paris: FATF, 2019) <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF30-(1989-2019).pdf> at 11.
[29] Financial Action Task Force, *Financial Action Task Force on Money Laundering: Annual Report 1995-1996* (Paris: FATF, 1996) at 3 <https://www.fatf-gafi.org/media/fatf/documents/reports/1995%201996%20ENG.pdf>; Financial Action Task Force, *The Forty Recommendations* (Paris: FATF, 1996).
[30] Financial Action Task Force, "History of the FATF" (2019) online: *FATF* <https://www.fatf-gafi.org/about/historyofthefatf/>.

October 2004 the FATF published a *Ninth Special Recommendation* aimed at "cash couriers."[31]

18. The nine special recommendations (updated to February 2008) are attached as Appendix 'C'.

19. In June 2003, the continued evolution of money laundering techniques led the FATF to undertake a comprehensive revision of the FATF standards.[32] The *Revised Forty Recommendations* applied not only to money laundering but also to terrorist financing, and when combined with the Eight Special Recommendations, they provided a set of enhanced measures intended to help countries prevent terrorism.[33]

20. The 2003 revised recommendations (updated to October 2004) are attached as Appendix 'D'.

21. In February 2012, the FATF completed a review of its standards and approved a further revision of the Recommendations. This revision was intended to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime. The Recommendations were expanded to deal with new threats such as the financing and proliferation of weapons of mass destruction, and to be clearer on transparency and tougher on corruption. The nine Special Recommendations on terrorist financing were integrated with the measures against money laundering.[34]

22. The 2012 recommendations (updated to June 2019)[35] are attached as Appendix 'E'.

---

[31] Financial Action Task Force, "History of the FATF" (2019) online: *FATF* <https://www.fatf-gafi.org/about/historyofthefatf/>; Financial Action Task Force, *FATF Standards: FATF IX Special Recommendations* (Paris: FATF, 2008).
[32] Financial Action Task Force, "History of the FATF" (2019) online: *FATF* <https://www.fatf-gafi.org/about/historyofthefatf/>.
[33] Financial Action Task Force, *The Forty Recommendations* (Paris: FATF, 2004) < www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf>.
[34] Financial Action Task Force, "History of the FATF" (2019) online: *FATF* <https://www.fatf-gafi.org/about/historyofthefatf/>.
[35] The Recommendations have been subject to occasional revisions since 2012. See Financial Action Task Force, *The FATF Recommendations* (Paris: FATF, 2019) <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html# UPDATESl>.

23. The FATF identified the adoption of a "risk-based" approach as central to the effective implementation of the 2012 recommendations:[36]

> At the core of today's Recommendations is the risk-based approach, which ensure that countries, as well as private sector, identify, assess and understand the risks they are exposed to and focus their resources on areas where the risks are highest. Given each country's unique risk situation, the FATF Recommendations provide countries a level of flexibility to determine which actions they need to take to address the particular money laundering and terrorist financing risks they face.[37]

24. The current version (June 2019) of the *Revised FATF Recommendations* includes Interpretive Notes for some but not all of the Recommendations.[38] The FATF has published the interpretive notes alongside the current version of the recommendations. The interpretive notes can be found in Appendix 'E'.

25. Those recommendations for which one or more interpretive notes have been issued include:[39]

a. Recommendation 1;
b. Recommendation 3;
c. Recommendation 4;
d. Recommendation 5;
e. Recommendation 6;
f. Recommendation 7;
g. Recommendation 8;
h. Recommendation 10;
i. Recommendation 12;
j. Recommendation 13;
k. Recommendation 14;
l. Recommendation 15;
m. Recommendation 16;

---

[36] Financial Action Task Force, "Risk-Based Approach" (2019) online: *FATF* <http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate)>.
[37] FATF (2019), Financial Action Task Force – 30 years, FATF, Paris <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF30-(1989-2019).pdf> at 10.
[38] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Paris: FATF, 2019) < https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.
[39] For updates to these interpretive notes since 2012, see: Financial Action Task Force, "The FATF Recommendations" (2019) online: *FATF*: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html# UPDATESl>.

n. Recommendation 17;
o. Recommendation 18
p. Recommendation 19;
q. Recommendation 20;
r. Recommendation 22;
s. Recommendation 23;
t. Recommendation 24;
u. Recommendation 25;
v. Recommendation 26;
w. Recommendation 28;
x. Recommendation 29;
y. Recommendation 30;
z. Recommendation 32;
aa. Recommendation 38;
bb. Recommendation 40.

IV. Mutual Evaluation Process

26. In 1991, the year following its creation, the FATF established a self-assessment process in which countries reported to the FATF on steps taken to implement the recommendations.[40] In September 1991, the FATF undertook its first mutual evaluations in which teams of expert examiners from FATF member countries conducted reviews of implementation of the recommendations.[41] The FATF currently describes mutual evaluations as follows:[42]

> FATF mutual evaluations are in-depth country reports analysing the implementation and effectiveness of measures to combat money laundering and terrorist financing. Mutual evaluations are peer reviews, where members from different countries assess another country. A mutual evaluation report provides an in-depth description and analysis of a country's system for preventing criminal abuse of the financial system as well as focused recommendations to the country to further strengthen its system.

[40] FATF (2019), Financial Action Task Force – 30 years, FATF, Paris <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF30-(1989-2019).pdf> at 10.
[41] FATF (2019), Financial Action Task Force – 30 years, FATF, Paris <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF30-(1989-2019).pdf> at 10.
[42] Financial Action Task Force, "Mutual Evaluations" (2019) online: *FATF* < https://www.fatf-gafi.org/publications/mutualevaluations/more/more-about-mutual-evaluations.html?hf=10&b=0&s=desc(fatf_releasedate)>.

27. Following the adoption of the revised recommendations in 2012, the FATF issued the methodology for the 4th round of mutual evaluations.[43] The methodology contemplates a technical compliance assessment (as conducted in previous rounds) as well as an assessment of effectiveness. Effectiveness assessments are being conducted for the first time in the 4th round of evaluations. These assessments are described as follows:[44]

> The technical compliance assessment addresses the specific requirements of the FATF Recommendations, principally as they relate to the relevant legal and institutional framework of the country, and the powers and procedures of the competent authorities. These represent the fundamental building blocks of an AML/CFT system.
>
> The effectiveness assessment differs fundamentally from the assessment of technical compliance. It seeks to assess the adequacy of the implementation of the FATF Recommendations, and identifies the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system. The focus of the effectiveness assessment is therefore on the extent to which the legal and institutional framework is producing the expected results.

28. The mutual evaluation process and the results of recent evaluations of Canada are set out in the appendices identified below.

A. Documents Associated with the FATF Mutual Evaluation Process

29. The following documents, associated with the FATF mutual evaluation process, are attached as appendices to this overview report:

a. Appendix F:

   FATF, *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* (Paris: FATF, 2019).

[43] Financial Action Task Force, *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* (Paris: FATF, 2019) < https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf>.
[44] Financial Action Task Force, *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* (Paris: FATF, 2019) < https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> at 5.

b. Appendix G:

FATF, *Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations* (Paris: FATF, 2019).

c. Appendix H:

FATF, *Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up: "Universal Procedures"* (Paris: FATF, 2019).

d. Appendix I:

FATF, *Consolidated Table of Assessment Ratings* (Paris: FATF, 2020).

V. Mutual Evaluations of Canada

30. The following documents relate to mutual evaluations of Canada.

a. Appendix J:

FATF, *Financial Action Task Force on Money Laundering: Annual Report 1992-1993* (Paris: FATF, 1993).

b. Appendix K:

FATF, *Financial Action Task Force on Money Laundering: Annual Report 1997-1998* (Paris: FATF, 1998).

c. Appendix L:

FATF, *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism: Canada* (Paris: FATF, 2008).

d. Appendix M:

FATF, *6th Follow-Up Report: Mutual Evaluation of Canada* (Paris: FATF, 2014).

e. Appendix N:

FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016).

B. FATF Typology, Guidance and Best Practices Papers

31. The following typology, guidance and best practice documents have been created by the FATF and/or FSRBs:

a. Appendix O:

   APG & FATF, *FATF Report: Vulnerabilities of Casinos and Gaming Sector* (Paris: FATF, 2009).

b. Appendix P:

   FATF, *Money Laundering & Terrorist Financing Through the Real Estate Sector* (Paris: FATF, 2007).

c. Appendix Q:

   FATF, *Professional Money Laundering* (Paris: FATF, 2018).

d. Appendix R:

   FATF, *FATF Report: Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (Paris: FATF, 2013).

e. Appendix S:

   FATF, *Guidance for a Risk-Based Approach: Accounting Profession* (Paris: FATF, 2019).

f. Appendix T:

   FATF, *Guidance for a Risk-Based Approach: Legal Professionals* (Paris: FATF, 2019).

g. Appendix U:

   FATF, *Concealment of Beneficial Ownership* (Paris: FATF, 2018).

h. Appendix V:

   CFATF & FATF, *FATF Report: Money Laundering Using Trust and Company Service Providers* (Paris: FATF, 2010).

i. Appendix W:

FATF, *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* (Paris: FATF, 2006).

j. Appendix X:

FATF, *Best Practices on Beneficial Ownership for Legal Persons* (Paris: FATF, 2019).

k. Appendix Y:

FATF, *Guidance for a Risk-Based Approach: Securities Sector* (Paris: FATF, 2018).

l. Appendix Z:

APG, *APG Typology Report on Trade Based Money Laundering* (Paris: FATF, 2012).

m. Appendix AA:

FATF, *FATF Report: Virtual Currencies Key Definitions and Potential AML/CFT Risk* (Paris: FATF, 2014).

n. Appendix BB:

FATF, *FATF Report: The Role of Hawala and other Similar Service Providers in Money Laundering and Terrorist Financing* (Paris: FATF, 2013).

o. Appendix CC:

FATF, *Report on New Payment Methods* (Paris: FATF, 2005).

p. Appendix DD:

FATF, *FATF Report: Money Laundering Using New Payment Methods* (Paris: FATF, 2010).

q. Appendix EE:

FATF, *FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers* (Paris: FATF, 2010).

r. Appendix FF:

FATF, *FATF Report: Money Laundering and Terrorist Financing in the Securities Sector* (Paris: FATF, 2009).

s. Appendix GG:

FATF, *Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement* (Paris: FATF, 2015).

t. Appendix HH:

FATF, *Guidance for a Risk-Based Approach: Money or Value Transfer Services* (Paris: FATF, 2016).

u. Appendix II:

FATF, *FATF Guidance: Correspondent Banking Services* (Paris: FATF, 2016).

v. Appendix JJ:

FATF, *Guidance for a Risk-Based Approach: The Banking Sector* (Paris: FATF, 2014).

w. Appendix KK:

FATF, *FATF Report: Financial Flows from Human Trafficking* (Paris: FATF, 2018).

x. Appendix LL:

FATF, *FATF Report: Money Laundering Through the Physical Transportation of Cash* (Paris: FATF, 2015).

y. Appendix MM:

FATF, *FATF Report: Money Laundering through the Football Sector* (Paris: FATF, 2009).

z. Appendix NN:

FATF, *Proliferation on Financing Report* (Paris: FATF, 2008).

aa. Appendix OO:

FATF, *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (Paris: FATF, 2008).

bb. Appendix PP:

FATF, *FATF Report: Money Laundering and Terrorist Financing Related to Counterfeiting of Currency* (Paris: FATF, 2013).

cc. Appendix QQ:

FATF, *Guidance for a Risk-Based Approach: Trust and Company Service Providers* (Paris: FATF, 2019).

dd. Appendix RR:

FATF, *COVID-19-related Money Laundering and Terrorist Financing: Risks and Policy Responses* (Paris: FATF, 2020).

ee. Appendix SS:

FATF, *FATF Report: Illicit Tobacco Trade* (Paris: FATF, 2012).

ff. Appendix TT:

FATF, *FATF President's Paper: Anti-Money Laundering and Counter Terrorist Financing for Judges and Prosecutors* (Paris: FATF, 2018).

gg. Appendix UU:

FATF, *FATF Guidance: Private Sector Information Sharing* (Paris: FATF, 2017).

hh. Appendix VV:

FATF, *FATF Report: Operational Issues Financial Investigations Guidance* (Paris: FATF, 2012).

ii. Appendix WW:

FATF, *FATF Report: Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated with Gold* (Paris: FATF, 2015).

jj. Appendix XX:

FATF, *FATF Report: Money Laundering and Terrorist Financing Through Trade in Diamonds* (Paris: FATF, 2013).

Appendix A:

Financial Action Task Force, *The Forty Recommendations of the Financial Action Task Force on Money Laundering* (Paris: FATF, 1990)

THE FORTY RECOMMENDATIONS OF THE

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

1990

A. GENERAL FRAMEWORK OF THE RECOMMENDATIONS

1. Each country should, without further delay, take steps to fully implement the Vienna Convention, and proceed to ratify it.

2. Financial institution secrecy laws should be conceived so as not to inhibit implementation of the recommendations of this group.

3. An effective money laundering enforcement program should include increased multilateral cooperation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible.

B. IMPROVEMENT OF NATIONAL LEGAL SYSTEMS TO COMBAT MONEY LAUNDERING

Definition of the Criminal Offense of Money Laundering

4. Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalize drug money laundering as set forth in the Vienna Convention.

5. Each country should consider extending the offense of drug money laundering to any other crimes for which there is a link to narcotics; an alternative approach is to criminalize money laundering based on all serious offenses, and/or on all offenses that generate a significant amount of proceeds, or on certain serious offenses.

6. As provided in the Vienna Convention, the offense of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.

7. Where possible, corporations themselves - not only their employees - should be subject to criminal liability.

Provisional Measures and Confiscation

8. Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offense, or property of corresponding value.

Such measures should include the authority to : 1) identify, trace and evaluate property which is subject to confiscation; 2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and 3) take any appropriate investigative measures.

In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void contracts entered by parties, where parties knew or should have known that as a result of the contract, the State would be prejudiced in its ability to recover financial claims, e.g. through confiscation or collection of fines and penalties.

C. ENHANCEMENT OF THE ROLE OF THE FINANCIAL SYSTEM

Scope of the Following Recommendations

9. Recommendations 12 to 29 of this paper should apply not only to banks, but also to non-bank financial institutions.

10. The appropriate national authorities should take steps to ensure that these Recommendations are implemented on as broad a front as is practically possible.

11. A working group should further examine the possibility of establishing a common minimal list of non-bank financial institutions and other professions dealing with cash subject to these Recommendations.

Customer Identification and Record-keeping Rules

12. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

13. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are not acting on their own behalf, in particular, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

14. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

Increased Diligence of Financial Institutions

15. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

16. If financial institutions suspect that funds stem from a criminal activity, they should be permitted or required to report promptly their suspicions to the competent authorities. Accordingly, there should be legal provisions to protect financial institutions and their employees from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report in good faith, in disclosing suspected criminal activity to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

17. Financial institutions, their directors and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

18. In the case of a mandatory reporting system, or in the case of a voluntary reporting system where appropriate, financial institutions reporting their suspicions should comply with instructions from the competent authorities.

19. When a financial institution develops suspicions about the operations of a customer, and when no obligation of reporting these suspicious exists, makes no report to the competent authorities, it should deny assistance to this customer, sever relations with him and close his accounts.

20. Financial institutions should develop programs against money laundering. These programs should include, as a minimum :

(a) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

(b) an ongoing employee training programme;

(c) an audit function to test the system.

Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures

21. Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

22. Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the mother institution should be informed by the financial institutions that they cannot apply these Recommendations.

Other Measures to Avoid Currency Laundering

23. The feasibility of measures to detect or monitor cash at the border should be studied, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

24. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

25. Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to encourage the replacement of cash transfers.

Implementation, and Role of Regulatory and other Administrative Authorities

26. The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should cooperate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

27. Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.

28. The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behaviour by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

29. The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates.

D. STRENGTHENING OF INTERNATIONAL COOPERATION

Administrative Cooperation

(a) Exchange of general information

30. National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the IMF and BIS to facilitate international studies.

31. International competent authorities, perhaps Interpol and the Customs Cooperation Council, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques.

Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

(b) Exchange of information relating to suspicious transactions

32. Each country should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.

Cooperation Between Legal Authorities

(a) Basis and means for cooperation in confiscation, mutual assistance and extradition

33. Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions - i.e. different standards concerning the intentional element of the infraction - do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

34. International cooperation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.

35. Countries should encourage international conventions such as the draft Convention of the Council of Europe on Confiscation of the Proceeds from Offenses.

(b) Focus of improved mutual assistance on money laundering issues

36. Co-operative investigations among appropriate competent authorities of countries should be encouraged.

37. There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.

38. There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

39. To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

40. Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offense or related offenses. With respect to its national legal system, each

country should recognise money laundering as an extraditable offense. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Appendix B:

Financial Action Task Force, *The Forty Recommendations* (Paris: FATF, 1996)

Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

The Forty Recommendations

Introduction

The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering -- the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilised in future criminal activities and from affecting legitimate economic activities.

The FATF currently consists of 29 countries[1] and two international organisations[2]. Its membership includes the major financial centre countries of Europe, North and South America, and Asia. It is a multi-disciplinary body - as is essential in dealing with money laundering - bringing together the policy-making power of legal, financial and law enforcement experts.

This need to cover all relevant aspects of the fight against money laundering is reflected in the scope of the forty FATF Recommendations -- the measures which the Task Force have agreed to implement and which all countries are encouraged to adopt. The Recommendations were originally drawn up in 1990. In 1996 the forty Recommendations were revised to take into account the experience gained over the last six years and to reflect the changes which have occurred in the money laundering problem.[3]

These forty Recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application. They cover the criminal justice system and law enforcement; the financial system and its regulation, and international co-operation.

It was recognised from the outset of the FATF that countries have diverse legal and financial systems and so all cannot take identical measures. The Recommendations are therefore the principles for action in this field, for countries to implement according to their particular circumstances and constitutional frameworks allowing countries a measure of flexibility rather than prescribing every detail. The measures are not particularly complex or difficult, provided there is the political will to act. Nor do they compromise the freedom to engage in legitimate transactions or threaten economic development.

FATF countries are clearly committed to accept the discipline of being subjected to multilateral surveillance and peer review. All member countries have their implementation of the forty Recommendations monitored through a two-pronged approach: an annual self-assessment exercise and the more detailed mutual evaluation process under which each member country is subject to an on-site examination. In addition, the FATF carries out cross-country reviews of measures taken to implement particular Recommendations.

These measures are essential for the creation of an effective anti-money laundering framework.

---

[1] Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions". The twenty-nine FATF member countries and governments are: Argentina; Australia; Austria; Belgium; Brazil; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong, China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States.

[2] The two international organisations are: the European Commission and the Gulf Cooperation Council.

[3] During the period 1990 to 1995, the FATF also elaborated various Interpretative Notes which are designed to clarify the application of specific Recommendations. Some of these Interpretative Notes have been updated in the Stocktaking Review to reflect changes in the Recommendations. The FATF adopted a new Interpretative Note relating to Recommendation 15 on 2 July 1999.

THE FORTY RECOMMENDATIONS

A. GENERAL FRAMEWORK OF THE RECOMMENDATIONS

1. Each country should take immediate steps to ratify and to implement fully, the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention).

2. Financial institution secrecy laws should be conceived so as not to inhibit implementation of these recommendations.

3. An effective money laundering enforcement program should include increased multilateral co-operation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible.

B. ROLE OF NATIONAL LEGAL SYSTEMS IN COMBATING MONEY LAUNDERING

Scope of the Criminal Offence of Money Laundering

4. Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalise money laundering as set forth in the Vienna Convention. Each country should extend the offence of drug money laundering to one based on serious offences. Each country would determine which serious crimes would be designated as money laundering predicate offences.

5. As provided in the Vienna Convention, the offence of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.

6. Where possible, corporations themselves - not only their employees - should be subject to criminal liability.

Provisional Measures and Confiscation

7. Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offence, or property of corresponding value, without prejudicing the rights of bona fide third parties.

   Such measures should include the authority to : (1) identify, trace and evaluate property which is subject to confiscation; (2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and (3) take any appropriate investigative measures.

   In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void contracts entered into by parties, where parties knew or should have known that as a result of the contract, the State would be

prejudiced in its ability to recover financial claims, e.g. through confiscation or collection of fines and penalties.

C. ROLE OF THE FINANCIAL SYSTEM IN COMBATING MONEY LAUNDERING

8. Recommendations 10 to 29 should apply not only to banks, but also to non-bank financial institutions. Even for those non-bank financial institutions which are not subject to a formal prudential supervisory regime in all countries, for example bureaux de change, governments should ensure that these institutions are subject to the same anti-money laundering laws or regulations as all other financial institutions and that these laws or regulations are implemented effectively.

9. The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a commercial undertaking by businesses or professions which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the attached annex. It is left to each country to decide whether special situations should be defined where the application of anti-money laundering measures is not necessary, for example, when a financial activity is carried out on an occasional or limited basis.

Customer Identification and Record-keeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

    In order to fulfil identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

    (i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

    (ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

13. Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.

16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.

19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum :

    (i) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

    (ii) an ongoing employee training programme;

    (iii) an audit function to test the system.

Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures

20. Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the

country of the mother institution should be informed by the financial institutions that they cannot apply these Recommendations.

21. Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Other Measures to Avoid Money Laundering

22. Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

23. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

24. Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to encourage the replacement of cash transfers.

25. Countries should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities.

Implementation, and Role of Regulatory and other Administrative Authorities

26. The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should co-operate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

27. Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.

28. The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behaviour by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

29. The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates.

D. STRENGTHENING OF INTERNATIONAL CO-OPERATION

Administrative Co-operation

Exchange of general information

30. National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.

31. International competent authorities, perhaps Interpol and the World Customs Organisation, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques. Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

Exchange of information relating to suspicious transactions

32. Each country should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.

Other forms of Co-operation

Basis and means for co-operation in confiscation, mutual assistance and extradition

33. Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions - i.e. different standards concerning the intentional element of the infraction - do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

34. International co-operation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.

35. Countries should be encouraged to ratify and implement relevant international conventions on money laundering such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Focus of improved mutual assistance on money laundering issues

36. Co-operative investigations among countries' appropriate competent authorities should be encouraged. One valid and effective investigative technique in this respect is controlled delivery related to assets known or suspected to be the proceeds of crime. Countries are encouraged to support this technique, where possible.

37. There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by financial institutions and other persons, the search of

persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.

38. There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for co-ordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

39. To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for co-ordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

40. Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offence or related offences. With respect to its national legal system, each country should recognise money laundering as an extraditable offence. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Annex to Recommendation 9: List of Financial Activities undertaken by business or professions which are not financial institutions

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.*
3. Financial leasing.
4. Money transmission services.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques and bankers' drafts...).
6. Financial guarantees and commitments.
7. Trading for account of customers (spot, forward, swaps, futures, options...) in:
   (a) money market instruments (cheques, bills, CDs, etc.) ;
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of clients.
11. Life insurance and other investment related insurance.
12. Money changing.

* Including inter alia:
— consumer credit,
— mortgage credit,
— factoring, with or without recourse,
— finance of commercial transactions (including forfaiting).

INTERPRETATIVE NOTES[1] TO THE FORTY RECOMMENDATIONS

[1] During the period 1990 to 1995, the FATF elaborated various Interpretative Notes which are designed to clarify the application of specific Recommendations. Some of these Interpretative Notes have been updated in the Stocktaking Review to reflect changes in the Recommendations. The FATF adopted a new Interpretative Note relating to Recommendation 15 on 2 July 1999.

INTERPRETATIVE NOTES

Recommendation 4

Countries should consider introducing an offence of money laundering based on all serious offences and/or on all offences that generate a significant amount of proceeds.

Recommendation 8

The FATF Recommendations should be applied in particular to life insurance and other investment products offered by insurance companies, whereas Recommendation 29 applies to the whole of the insurance sector.

Recommendations 8 and 9 (Bureaux de Change)

Introduction

Bureaux de change are an important link in the money laundering chain since it is difficult to trace the origin of the money once it has been exchanged. Typologies exercises conducted by the FATF have indicated increasing use of bureaux de change in laundering operations. Hence it is important that there should be effective counter-measures in this area. This Interpretative Note clarifies the application of FATF Recommendations concerning the financial sector in relation to bureaux de change and, where appropriate, sets out options for their implementation.

Definition of Bureaux de Change

For the purpose of this Note, bureaux de change are defined as institutions which carry out retail foreign exchange operations (in cash, by cheque or credit card). Money changing operations which are conducted only as an ancillary to the main activity of a business have already been covered in Recommendation 9. Such operations are therefore excluded from the scope of this Note.

Necessary Counter-Measures Applicable to Bureaux de Change

To counter the use of bureaux de change for money laundering purposes, the relevant authorities should take measures to know the existence of all natural and legal persons who, in a professional capacity, perform foreign exchange transactions.

As a minimum requirement, FATF members should have an effective system whereby the bureaux de change are known or declared to the relevant authorities (whether regulatory or law enforcement). One method by which this could be achieved would be a requirement on bureaux de change to submit to a designated authority, a simple declaration containing adequate information on the institution itself and its management. The authority could either issue a receipt or give a tacit authorisation: failure to voice an objection being considered as approval.

FATF members could also consider the introduction of a formal authorisation procedure. Those wishing to establish bureaux de change would have to submit an application to a designated authority empowered to grant authorisation on a case-by-case basis. The request for authorisation would need to contain such information as laid down by the authorities but should at least provide details of the applicant institution and its management. Authorisation would be granted, subject to the bureau de change meeting the specified conditions relating to its management and the shareholders, including the application of a "fit and proper test".

Another option which could be considered would be a combination of declaration and authorisation procedures. Bureaux de change would have to notify their existence to a designated authority but would not need to be authorised before they could start business. It would be open to the authority to apply a 'fit and proper' test to the management of bureaux de change after the bureau had commenced its activity, and to prohibit the bureau de change from continuing its business, if appropriate.

Where bureaux are required to submit a declaration of activity or an application for registration, the designated authority (which could be either a public body or a self-regulatory organisation) could be empowered to publish the list of registered bureaux de change. As a minimum, it should maintain a (computerised) file of bureaux de change. There should also be powers to take action against bureaux de change conducting business without having made a declaration of activity or having been registered.

As envisaged under FATF Recommendations 8 and 9, bureaux de change should be subject to the same anti-money laundering regulations as any other financial institution. The FATF Recommendations on financial matters should therefore be applied to bureaux de change. Of particular importance are those on identification requirements, suspicious transactions reporting, due diligence and record-keeping.

To ensure effective implementation of anti-money laundering requirements by bureaux de change, compliance monitoring mechanisms should be established and maintained. Where there is a registration authority for bureaux de change or a body which receives declarations of activity by bureaux de change, it could carry out this function. But the monitoring could also be done by other designated authorities (whether directly or through the agency of third parties such as private audit firms). Appropriate steps would need to be taken against bureaux de change which failed to comply with the anti-laundering requirements.

The bureaux de change sector tends to be an unstructured one without (unlike banks) national representative bodies which can act as a channel of communication with the authorities. Hence it is important that FATF members should establish effective means to ensure that bureaux de change are aware of their anti-money laundering responsibilities and to relay information, such as guidelines on suspicious transactions, to the profession. In this respect it would be useful to encourage the development of professional associations.

Recommendations 11, 15 through 18

Whenever it is necessary in order to know the true identity of the customer and to ensure that legal entities cannot be used by natural persons as a method of operating in reality anonymous accounts, financial institutions should, if the information is not otherwise available through public registers or other reliable sources, request information - and update that information - from the customer concerning principal owners and beneficiaries. If the customer does not have such information, the financial institution should request information from the customer on whoever has actual control.

If adequate information is not obtainable, financial institutions should give special attention to business relations and transactions with the customer.

If, based on information supplied from the customer or from other sources, the financial institution has reason to believe that the customer's account is being utilised in money laundering transactions, the financial institution must comply with the relevant legislation, regulations, directives or agreements concerning reporting of suspicious transactions or termination of business with such customers.

Recommendation 11

A bank or other financial institution should know the identity of its own customers, even if these are represented by lawyers, in order to detect and prevent suspicious transactions as well as to enable it to comply swiftly to information or seizure requests by the competent authorities. Accordingly Recommendation 11 also applies to the situation where an attorney is acting as an intermediary for financial services.

Recommendation 14

(a) In the interpretation of this requirement, special attention is required not only to transactions between financial institutions and their clients, but also to transactions and/or shipments especially of currency and equivalent instruments between financial institutions themselves or even to transactions within financial groups. As the wording of Recommendation 14 suggests that indeed "all" transactions are covered, it must be read to incorporate these interbank transactions.

(b) The word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits.

Recommendation 15[2]

In implementing Recommendation 15, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.

Recommendation 22

(a) To facilitate detection and monitoring of cash transactions, without impeding in any way the freedom of capital movements, members could consider the feasibility of subjecting all cross-border transfers, above a given threshold, to verification, administrative monitoring, declaration or record keeping requirements.

(b) If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.

Recommendation 26

In respect of this requirement, it should be noted that it would be useful to actively detect money laundering if the competent authorities make relevant statistical information available to the investigative authorities, especially if this information contains specific indicators of money laundering activity. For instance, if the competent authorities' statistics show an imbalance between the development of the financial services industry in a certain geographical area within a country and the development of the local economy, this imbalance might be indicative of money laundering activity in the region. Another example would be manifest changes in domestic currency flows without an apparent legitimate economic cause. However, prudent analysis of these statistical data is warranted, especially as there is not necessarily a direct relationship between financial flows and economic activity (e.g. the financial flows in an international financial centre with a high proportion

[2] The FATF adopted this Interpretative Note on 2 July 1999.

of investment management services provided for foreign customers or a large interbank market not linked with local economic activity).

Recommendation 29

Recommendation 29 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view. Hence, where shareholder suitability (or "fit and proper") tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Recommendation 33

Subject to principles of domestic law, countries should endeavour to ensure that differences in the national definitions of the money laundering offences -- e.g., different standards concerning the intentional element of the infraction, differences in the predicate offences, differences with regard to charging the perpetrator of the underlying offence with money laundering -- do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

Recommendation 36 (Controlled delivery)

The controlled delivery of funds known or suspected to be the proceeds of crime is a valid and effective law enforcement technique for obtaining information and evidence in particular on international money laundering operations. In certain countries, controlled delivery techniques may also include the monitoring of funds. It can be of great value in pursuing particular criminal investigations and can also help in obtaining more general intelligence on money laundering activities. The use of these techniques should be strongly encouraged. The appropriate steps should therefore be taken so that no obstacles exist in legal systems preventing the use of controlled delivery techniques, subject to any legal requisites, including judicial authorisation for the conduct of such operations. The FATF welcomes and supports the undertakings by the World Customs Organisation and Interpol to encourage their members to take all appropriate steps to further the use of these techniques.

Recommendation 38

(a) Each country shall consider, when possible, establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

(b) Each country should consider, when possible, taking such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Deferred Arrest and Seizure

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

FATF Secretariat, OECD
2, rue André-Pascal
75775 Paris Cedex 16
FRANCE

T: 33 (0) 1 45 24 79 45
F: 33 (0) 1 45 24 17 60
E: fatf.contact@oecd.org

Appendix C:

Financial Action Task Force, *FATF Standards: FATF IX Special Recommendations* (Paris: FATF, 2008)

FATF GAFI

Financial Action Task Force | Groupe d'action financière

FATF Standards

FATF IX Special Recommendations

October 2001
(incorporating all subsequent amendments until February 2008)

The FATF revised the 40 and the IX Recommendations. The revision of the FATF Recommendation was adopted and published in February 2012. See www.fatf-gafi.org/recommendations for the 2012 FATF Recommendations.

FATF Special Recommendations on Terrorist Financing

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative Remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

(i) by terrorist organisations posing as legitimate entities;

(ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

(iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

IX. Cash Couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.

Interpretative Notes

Interpretative Note to

Special Recommendation II: Criminalising the financing of terrorism and associated money laundering

Objective

1. Special Recommendation II (SR II) was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and inter alia money laundering, another objective of SR II is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering. The basis for criminalising terrorist financing should be the United Nations International Convention for the Suppression of the Financing of Terrorism, 1999.[1]

Definitions

2. For the purposes of SR II and this Interpretative Note, the following definitions apply:

a) The term funds refers to assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.

b) The term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

[1] Although the UN Convention had not yet come into force at the time that SR II was originally issued in October 2001 – and thus is not cited in the SR itself – the intent of the FATF has been from the issuance of SR II to reiterate and reinforce the criminalisation standard as set forth in the Convention (in particular, Article 2). The Convention came into force in April 2003.

c) The term terrorist act includes:

i) An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and

ii) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

d) The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organisations.

e) The term terrorist organisation refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Characteristics of the Terrorist Financing Offence

3. Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.

4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with this Recommendation.

5. Terrorist financing offences should extend to any funds whether from a legitimate or illegitimate source.

6. Terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

7. It should also be an offence to attempt to commit the offence of terrorist financing.

8. It should also be an offence to engage in any of the following types of conduct:

a) Participating as an accomplice in an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;

b) Organising or directing others to commit an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;

c) Contributing to the commission of one or more offence(s) as set forth in paragraphs 3 or 7 of this Interpretative Note by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

9. Terrorist financing offences should be predicate offences for money laundering.

10. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

11. The law should permit the intentional element of the terrorist financing offence to be inferred from objective factual circumstances.

12. Criminal liability for terrorist financing should extend to legal persons. Where that is not possible (*i.e.* due to fundamental principles of domestic law), civil or administrative liability should apply.

13. Making legal persons subject to criminal liability for terrorist financing should not preclude the possibility of parallel criminal, civil or administrative proceedings in countries in which more than one form of liability is available.

14. Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil or administrative sanctions for terrorist financing.

Interpretative Note to

Special Recommendation III: Freezing and Confiscating Terrorist Assets

Objectives

1. FATF Special Recommendation III consists of two obligations. The first requires jurisdictions to implement measures that will freeze or, if appropriate, seize terrorist-related funds or other assets without delay in accordance with relevant United Nations resolutions. The second obligation of Special Recommendation III is to have measures in place that permit a jurisdiction to seize or confiscate terrorist funds or other assets on the basis of an order or mechanism issued by a competent authority or a court.

2. The objective of the first requirement is to freeze terrorist-related funds or other assets based on reasonable grounds, or a reasonable basis, to suspect or believe that such funds or other assets could be used to finance terrorist activity. The objective of the second requirement is to deprive terrorists of these funds or other assets if and when links have been adequately established between the funds or other assets and terrorists or terrorist activity. The intent of the first objective is preventative, while the intent of the second objective is mainly preventative and punitive. Both requirements are necessary to deprive terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations.

Scope

3. Special Recommendation III is intended, with regard to its first requirement, to complement the obligations in the context of the United Nations Security Council (UNSC) resolutions relating to the prevention and suppression of the financing of terrorist acts—S/RES/1267(1999) and its successor resolutions,[1] S/RES/1373(2001) and any prospective resolutions related to the freezing, or if appropriate seizure, of terrorist assets. It should be stressed that none of the obligations in Special Recommendation III is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding.[2] The focus of Special Recommendation III instead is on the preventative measures that

[1] When issued, S/RES/1267(1999) had a time limit of one year. A series of resolutions have been issued by the United Nations Security Council (UNSC) to extend and further refine provisions of S/RES/1267(1999). By successor resolutions are meant those resolutions that extend and are directly related to the original resolution S/RES/1267(1999). At the time of issue of this Interpretative Note, these resolutions included S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003). In this Interpretative Note, the term S/RES/1267(1999) refers to S/RES/1267(1999) and its successor resolutions.

[2] For instance, both the *UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)* and *UN Convention against Transnational Organised Crime (2000)* contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Those obligations exist separately and apart from obligations that are set forth in S/RES/1267(1999), S/RES/1373(2001) and Special Recommendation III.

are necessary and unique in the context of stopping the flow or use of funds or other assets to terrorist groups.

4. S/RES/1267(1999) and S/RES/1373(2001) differ in the persons and entities whose funds or other assets are to be frozen, the authorities responsible for making these designations, and the effect of these designations.

5. S/RES/1267(1999) and its successor resolutions obligate jurisdictions to freeze without delay the funds or other assets owned or controlled by Al-Qaida, the Taliban, Usama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267 (the Al-Qaida and Taliban Sanctions Committee), including funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons' benefit, by their nationals or by any person within their territory. The Al-Qaida and Taliban Sanctions Committee is the authority responsible for designating the persons and entities that should have their funds or other assets frozen under S/RES/1267(1999). All jurisdictions that are members of the United Nations are obligated by S/RES/1267(1999) to freeze the assets of persons and entities so designated by the Al-Qaida and Taliban Sanctions Committee.[3]

6. S/RES/1373(2001) obligates jurisdictions[4] to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual jurisdiction has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective co-operation is developed among jurisdictions, jurisdictions should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. When (i) a specific notification or communication is sent and (ii) the jurisdiction receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organisation, the jurisdiction receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.

Definitions

7. For the purposes of Special Recommendation III and this Interpretive Note, the following definitions apply:

a) The term *freeze* means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets

[3] When the UNSC acts under Chapter VII of the UN Charter, the resolutions it issues are mandatory for all UN members.

[4] The UNSC was acting under Chapter VII of the UN Charter in issuing S/RES/1373(2001) (see previous footnote).

remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism.

b) The term *seize* means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets.

c) The term *confiscate*, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets.[5]

d) The term *funds or other assets* means financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

e) The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts[6] by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts or terrorist financing; (iii) organises or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing by a group of persons acting with a common purpose where the

[5] Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

[6] A *terrorist act* includes an act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, International Convention against the Taking of Hostages, Convention on the Physical Protection of Nuclear Material, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, International Convention for the Suppression of Terrorist Bombings, and the International Convention for the Suppression of the Financing of Terrorism (1999).

contribution is made intentionally and with the aim of furthering the terrorist act or terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing.

f) The phrase *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.

g) The term *terrorist organisation* refers to any legal person, group, undertaking or other entity owned or controlled directly or indirectly by a terrorist(s).

h) The term *designated persons* refers to those persons or entities designated by the Al-Qaida and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001).

    i) The phrase *without delay*, for the purposes of S/RES/1267(1999), means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban Sanctions Committee. For the purposes of S/RES/1373(2001), the phrase *without delay* means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. The phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly.

Freezing without delay terrorist-related funds or other assets

8. In order to fulfil the preventive intent of Special Recommendation III, jurisdictions should establish the necessary authority and adopt the following standards and procedures to freeze the funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with both S/RES/1267(1999) and S/RES/1373(2001):

a) **Authority to freeze, unfreeze and prohibit dealing in funds or other assets of designated persons.** Jurisdictions should prohibit by enforceable means the transfer, conversion, disposition or movement of funds or other assets. Options for providing the authority to freeze and unfreeze terrorist funds or other assets include:

    i) empowering or designating a competent authority or a court to issue, administer and enforce freezing and unfreezing actions under relevant mechanisms, or

    ii) enacting legislation that places responsibility for freezing the funds or other assets of designated persons publicly identified by a competent authority or a court on the person or entity holding the funds or other assets and subjecting them to sanctions for non-compliance.

    The authority to freeze and unfreeze funds or other assets should also extend to funds or other assets derived or generated from funds or other assets owned or

controlled directly or indirectly by such terrorists, those who finance terrorism, or terrorist organisations.

Whatever option is chosen there should be clearly identifiable competent authorities responsible for enforcing the measures.

The competent authorities shall ensure that their nationals or any persons and entities within their territories are prohibited from making any funds or other assets, economic resources or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit of: designated persons, terrorists; those who finance terrorism; terrorist organisations; entities owned or controlled, directly or indirectly, by such persons or entities; and persons and entities acting on behalf of or at the direction of such persons or entities.

b) **Freezing procedures.** Jurisdictions should develop and implement procedures to freeze the funds or other assets specified in paragraph (c) below without delay and without giving prior notice to the persons or entities concerned. Persons or entities holding such funds or other assets should be required by law to freeze them and should furthermore be subject to sanctions for non-compliance with this requirement. Any delay between the official receipt of information provided in support of a designation and the actual freezing of the funds or other assets of designated persons undermines the effectiveness of designation by affording designated persons time to remove funds or other assets from identifiable accounts and places. Consequently, these procedures must ensure (i) the prompt determination whether reasonable grounds or a reasonable basis exists to initiate an action under a freezing mechanism and (ii) the subsequent freezing of funds or other assets without delay upon determination that such grounds or basis for freezing exist. Jurisdictions should develop efficient and effective systems for communicating actions taken under their freezing mechanisms to the financial sector immediately upon taking such action. As well, they should provide clear guidance, particularly financial institutions and other persons or entities that may be holding targeted funds or other assets on obligations in taking action under freezing mechanisms.

c) **Funds or other assets to be frozen or, if appropriate, seized.** Under Special Recommendation III, funds or other assets to be frozen include those subject to freezing under S/RES/1267(1999) and S/RES/1373(2001). Such funds or other assets would also include those wholly or jointly owned or controlled, directly or indirectly, by designated persons. In accordance with their obligations under the United Nations International Convention for the Suppression of the Financing of Terrorism (1999) (the Terrorist Financing Convention (1999)), jurisdictions should be able to freeze or, if appropriate, seize any funds or other assets that they identify, detect, and verify, in accordance with applicable legal principles, as being used by, allocated for, or being made available to terrorists, those who finance terrorists or terrorist organisations. Freezing or seizing under the Terrorist Financing Convention (1999) may be conducted by freezing or seizing in the context of a criminal investigation or proceeding. Freezing action taken under Special Recommendation III shall be without prejudice to the rights of third parties acting in good faith.

d) **De-listing and unfreezing procedures.** Jurisdictions should develop and implement publicly known procedures to consider de-listing requests upon satisfaction of certain criteria consistent with international obligations and applicable legal principles, and to unfreeze the funds or other assets of de-listed persons or entities in a timely manner. For persons and entities designated under S/RES/1267(1999), such procedures and criteria should be in

accordance with procedures adopted by the Al-Qaida and Taliban Sanctions Committee under S/RES/1267(1999).

e) **Unfreezing upon verification of identity.** For persons or entities with the same or similar name as designated persons, who are inadvertently affected by a freezing mechanism, jurisdictions should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner upon verification that the person or entity involved is not a designated person.

f) **Providing access to frozen funds or other assets in certain circumstances.** Where jurisdictions have determined that funds or other assets, which are otherwise subject to freezing pursuant to the obligations under S/RES/1267(1999), are necessary for basic expenses; for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses,[7] jurisdictions should authorise access to such funds or other assets in accordance with the procedures set out in S/RES/1452(2002) and subject to approval of the Al-Qaida and Taliban Sanctions Committee. On the same grounds, jurisdictions may authorise access to funds or other assets, if freezing measures are applied pursuant to S/RES/1373(2001).

g) **Remedies.** Jurisdictions should provide for a mechanism through which a person or an entity that is the target of a freezing mechanism in the context of terrorist financing can challenge that measure with a view to having it reviewed by a competent authority or a court.

h) **Sanctions.** Jurisdictions should adopt appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing freezing mechanisms by financial institutions and other persons or entities that may be holding funds or other assets as indicated in paragraph 8(c) above. Failure to comply with such legislation, rules or regulations should be subject to civil, administrative or criminal sanctions.

Seizure and Confiscation

9. Consistent with FATF Recommendation 3, jurisdictions should adopt measures similar to those set forth in Article V of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), Articles 12 to 14 of the United Nations Convention on Transnational Organised Crime (2000), and Article 8 of the Terrorist Financing Convention (1999), including legislative measures, to enable their courts or competent authorities to seize and confiscate terrorist funds or other assets.

[7] See Article 1, S/RES/1452(2002) for the specific types of expenses that are covered.

Interpretative Note to

Special Recommendation VI: Alternative Remittance

General

1. Money or value transfer systems have shown themselves vulnerable to misuse for money laundering and terrorist financing purposes. The objective of Special Recommendation VI is to increase the transparency of payment flows by ensuring that jurisdictions impose consistent anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector and not currently subject to the FATF Recommendations. This Recommendation and Interpretative Note underscore the need to bring all money or value transfer services, whether formal or informal, within the ambit of certain minimum legal and regulatory requirements in accordance with the relevant FATF Recommendations.

2. Special Recommendation VI consists of three core elements:

a) Jurisdictions should require licensing or registration of persons (natural or legal) that provide money/value transfer services, including through informal systems;

b) Jurisdictions should ensure that money/value transmission services, including informal systems (as described in paragraph 5 below), are subject to applicable FATF Forty Recommendations (2003) (in particular, Recommendations 4-16 and 21-25)[1] and the Eight Special Recommendations (in particular SR VII); and

c) Jurisdictions should be able to impose sanctions on money/value transfer services, including informal systems, that operate without a license or registration and that fail to comply with relevant FATF Recommendations.

Scope and Application

3. For the purposes of this Recommendation, the following definitions are used.

4. *Money or value transfer service* refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.

5. A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through non-bank financial institutions or other

[1] When this Interpretative Note was originally issued, these references were to the 1996 FATF Forty Recommendations. Subsequent to the publication of the revised FATF Forty Recommendations in June 2003, this text was updated accordingly. All references are now to the 2003 FATF Forty Recommendations.

business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or underground (or parallel) banking systems. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala, hundi, fei-chien,* and the *black market peso exchange*.[2]

6. Licensing means a requirement to obtain permission from a designated competent authority in order to operate a money/value transfer service legally.

7. Registration in this Recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.

8. The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents which must be made available to the designated competent authority. An agent is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).

Applicability of Special Recommendation VI

9. Special Recommendation VI should apply to all persons (natural or legal), which conduct for or on behalf of another person (natural or legal) the types of activity described in paragraphs 4 and 5 above as a primary or substantial part of their business or when such activity is undertaken on a regular or recurring basis, including as an ancillary part of a separate business enterprise.

10. Jurisdictions need not impose a separate licensing / registration system or designate another competent authority in respect to persons (natural or legal) already licensed or registered as financial institutions (as defined by the FATF Forty Recommendations (2003)) within a particular jurisdiction, which under such license or registration are permitted to perform activities indicated in paragraphs 4 and 5 above and which are already subject to the full range of applicable obligations under the FATF Forty Recommendations (2003) (in particular, Recommendations 4-16 and 21-25) and the Eight Special Recommendations (in particular SR VII).

Licensing or Registration and Compliance

11. Jurisdictions should designate an authority to grant licences and/or carry out registration and ensure that the requirement is observed. There should be an authority responsible for ensuring compliance by money/value transfer services with the FATF Recommendations (including the Eight Special Recommendations). There should also be effective systems in place for monitoring and ensuring such compliance. This interpretation of Special Recommendation VI (i.e., the need for designation of competent authorities) is consistent with FATF Recommendation 23.

[2] The inclusion of these examples does not suggest that such systems are legal in any particular jurisdiction.

Sanctions

12. Persons providing money/value transfer services without a license or registration should be subject to appropriate administrative, civil or criminal sanctions.[3] Licensed or registered money/value transfer services which fail to comply fully with the relevant measures called for in the FATF Forty Recommendations (2003) or the Eight Special Recommendations should also be subject to appropriate sanctions.

[3] Jurisdictions may authorise temporary or provisional operation of money / value transfer services that are already in existence at the time of implementing this Special Recommendation to permit such services to obtain a license or to register.

Revised[1] Interpretative Note to

Special Recommendation VII: Wire Transfers[2]

Objective

1. Special Recommendation VII (SR VII) was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator of wire transfers is immediately available (1) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals, (2) to financial intelligence units for analysing suspicious or unusual activity and disseminating it as necessary, and (3) to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions. Due to the potential terrorist financing threat posed by small wire transfers, countries should aim for the ability to trace all wire transfers and should minimise thresholds taking into account the risk of driving transactions underground. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system. The FATF will continue to monitor the impact of Special Recommendation VII and conduct an assessment of its operation within three years of full implementation.

Definitions

2. For the purposes of this interpretative note, the following definitions apply.

a) The terms *wire transfer* and *funds transfer* refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

b) *Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different countries. This term also refers to any chain of wire transfers that has at least one cross-border element.

c) *Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same country. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to

[1] This revision of the Interpretative Note to Special Recommendation VII was issued on 29 February 2008.

[2] It is recognised that countries will need time to make relevant legislative or regulatory changes and to allow financial institutions to make necessary adaptations to their systems and procedures. This period should not extend beyond December 2006.

effect the wire transfer may be located in another country. The term also refers to any chain of wire transfers that takes place entirely within the borders of the European Union[3].

d) The term *financial institution* is as defined by the FATF Forty Recommendations (2003).[4] The term does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds[5].

e) The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

Scope

3. SR VII applies, under the conditions set out below, to cross-border and domestic transfers between financial institutions.

Cross-border wire transfers

4. Cross-border wire transfers should be accompanied by accurate and meaningful originator information. However, countries may adopt a *de minimus* threshold (no higher than USD or EUR 1 000). For cross-border transfers below this threshold:

a) Countries are not obligated to require ordering financial institutions to identify, verify record, or transmit originator information.

b) Countries may nevertheless require that incoming cross-border wire transfers contain full and accurate originator information.

5. Information accompanying qualifying cross-border wire transfers[6] must always contain the name of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included.

---

[3] Having regard to the fact that:

The European Union constitutes an autonomous entity with its own sovereign rights and a legal order independent of the Member States, to which both the Member States themselves and their nationals are subject, within the European Union's areas of competence;

The European Union has enacted legislation binding upon its Member States, subject to control by a court of justice, which provides for the integration of payment services within an internal market in accordance with the principles of the free movement of capital and free provision of services; and

This legislation notably provides for the implementation of Special Recommendation VII as a single jurisdiction and requires that full information on the payer is made readily available, where appropriate upon request, to the beneficiary financial institution and relevant competent authorities. It is further noted that the European internal market and corresponding legal framework is extended to the members of the European Economic Area.

[4] When this Interpretative Note was originally issued, these references were to the 1996 FATF Forty Recommendations. Subsequent to the publication of the revised FATF Forty Recommendations in June 2003, this text was updated accordingly. All references are now to the 2003 FATF Forty Recommendations.

[5] However, these systems do have a role in providing the necessary means for the financial institutions to fulfil their obligations under SR VII and, in particular, in preserving the integrity of the information transmitted with a wire transfer.

6. Information accompanying qualifying wire transfers should also contain the address of the originator. However, countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth.

7. Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they shall be exempted from including full originator information, provided they include the originator's account number or unique reference number (as described in paragraph 8), and the batch file contains full originator information that is fully traceable within the recipient country.

Domestic wire transfers

8. Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless full originator information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, financial institutions need only include the account number or a unique identifier provided that this number or identifier will permit the transaction to be traced back to the originator.

9. The information must be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate authorities. Law enforcement authorities should be able to compel immediate production of such information.

Exemptions from SR VII

10. SR VII is not intended to cover the following types of payments:

a) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, and the necessary information should be included in the message.

b) Financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

Role of ordering, intermediary and beneficiary financial institutions

Ordering financial institution

11. The ordering financial institution must ensure that qualifying wire transfers contain complete originator information. The ordering financial institution must also verify this information for accuracy and maintain this information in accordance with the standards set out in the FATF Forty Recommendations (2003)[7].

[6] Throughout this Interpretative Note, the phrase "qualifying cross-border wire transfers" means those cross-border wire transfers above any applicable threshold as described in paragraph 4.

[7] See note 4.

Intermediary financial institution

12. For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.

13. Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

Beneficiary financial institution

14. Beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or other competent authorities. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet SRVII standards.

Enforcement mechanisms for financial institutions that do not comply with wire transfer rules and regulations

15. Countries should adopt appropriate measures to monitor effectively the compliance of financial institutions with rules and regulations governing wire transfers. Financial institutions that fail to comply with such rules and regulations should be subject to civil, administrative or criminal sanctions.

Interpretative Note to

Special Recommendation VIII: Non-Profit Organisations

Introduction

1. Non-profit organisations (NPOs) play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The ongoing international campaign against terrorist financing has unfortunately demonstrated however that terrorists and terrorist organisations exploit the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment or otherwise support terrorist organisations and operations. This misuse not only facilitates terrorist activity but also undermines donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting the NPO sector from terrorist abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs.

2. NPOs may be vulnerable to abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. Depending on the legal form of the NPO and the country, NPOs may often be subject to little or no governmental oversight (for example, registration, record keeping, reporting and monitoring), or few formalities may be required for their creation (for example, there may be no skills or starting capital required, no background checks necessary for employees). Terrorist organisations have taken advantage of these characteristics of NPOs to infiltrate the sector and misuse NPO funds and operations to cover for or support terrorist activity.

Objectives and General Principles

3. The objective of Special Recommendation VIII (SR VIII) is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes but diverted for terrorist purposes. In this Interpretative Note, the approach taken to achieve this objective is based on the following general principles:

a) Past and ongoing abuse of the NPO sector by terrorists and terrorist organisations requires countries to adopt measures both: (i) to protect the sector against such abuse, and (ii) to identify and take effective action against those NPOs that either are exploited by or actively support terrorists or terrorist organizations.

b) Measures adopted by countries to protect the NPO sector from terrorist abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote transparency and engender greater confidence in the sector, across the donor community and

with the general public that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of transparency, integrity and public confidence in the management and functioning of all NPOs are integral to ensuring the sector cannot be misused for terrorist financing.

c) Measures adopted by countries to identify and take effective action against NPOs that either are exploited by or actively support terrorists or terrorist organisations should aim to prevent and prosecute as appropriate terrorist financing and other forms of terrorist support. Where NPOs suspected of or implicated in terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should to the extent reasonably possible avoid any negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

d) Developing co-operative relationships among the public, private and NPO sector is critical to raising awareness and fostering capabilities to combat terrorist abuse within the sector. Countries should encourage the development of academic research on and information sharing in the NPO sector to address terrorist financing related issues.

e) A targeted approach in dealing with the terrorist threat to the NPO sector is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to misuse by terrorists, the need to ensure that legitimate charitable activity continues to flourish and the limited resources and authorities available to combat terrorist financing in each jurisdiction.

f) Flexibility in developing a national response to terrorist financing in the NPO sector is also essential in order to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

Definitions

4. For the purposes of SR VIII and this interpretative note, the following definitions apply:

a) The term *non-profit organisation* or *NPO* refers to a legal entity or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

b) The terms *FIU*, *legal arrangement and legal person* are as defined by the FATF Forty Recommendations (2003) (*the FATF Recommendations*).

c) The term *funds* is as defined by the Interpretative Note to FATF Special Recommendation II.

d) The terms *freezing*, *terrorist* and *terrorist organisation* are as defined by the Interpretative Note to FATF Special Recommendation III.

e) The term *appropriate authorities* refers to competent authorities, self-regulatory bodies, accrediting institutions and other administrative authorities.

f) The term *beneficiaries* refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.

Measures

5. Countries should undertake domestic reviews of their NPO sector or have the capacity to obtain timely information on its activities, size and other relevant features. In undertaking these assessments, countries should use all available sources of information in order to identify features and types of NPOs, which by virtue of their activities or characteristics, are at risk of being misused for terrorist financing.[1] Countries should also periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

6. There is a diverse range of approaches in identifying, preventing and combating terrorist misuse of NPOs. An effective approach, however, is one that involves all four of the following elements: (a) Outreach to the sector, (b) Supervision or monitoring, (c) Effective investigation and information gathering and (d) Effective mechanisms for international co-operation. The following measures represent specific actions that countries should take with respect to each of these elements in order to protect their NPO sector from terrorist financing abuse.

a. Outreach to the NPO sector concerning terrorist financing issues

(i) Countries should have clear policies to promote transparency, integrity and public confidence in the administration and management of all NPOs.

(ii) Countries should encourage or undertake outreach programmes to raise awareness in the NPO sector about the vulnerabilities of NPOs to terrorist abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.

(iii) Countries should work with the NPO sector to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect the sector from terrorist abuse.[2]

(iv) Countries should encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

b. Supervision or monitoring of the NPO sector

Countries should take steps to promote effective supervision or monitoring of their NPO sector. In practice, countries should be able to demonstrate that the following standards apply to NPOs which account for (1) a significant portion of the financial resources under control of the sector; and (2) a substantial share of the sector's international activities.

(i) NPOs should maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through appropriate authorities.

[1] For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

[2] The FATF's *Combating the Abuse of Non-Profit Organisations: International Best Practices* provides a useful reference document for such exercises.

(ii) NPOs should issue annual financial statements that provide detailed breakdowns of incomes and expenditures.

(iii) NPOs should be licensed or registered. This information should be available to competent authorities.[3]

(iv) NPOs should have appropriate controls in place to ensure that all funds are fully accounted for and are spent in a manner that is consistent with the purpose and objectives of the NPO's stated activities.

(v) NPOs should follow a "know your beneficiaries and associate NPOs[4]" rule, which means that the NPO should make best efforts to confirm the identity, credentials and good standing of their beneficiaries and associate NPOs. NPOs should also undertake best efforts to document the identity of their significant donors and to respect donor confidentiality.

(vi) NPOs should maintain, for a period of at least five years, and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation. This also applies to information mentioned in paragraphs (i) and (ii) above.

(vii) Appropriate authorities should monitor the compliance of NPOs with applicable rules and regulations.[5] Appropriate authorities should be able to properly sanction relevant violations by NPOs or persons acting on behalf of these NPOs.[6]

c. Effective information gathering and investigation

(i) Countries should ensure effective co-operation, co-ordination and information sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs.

(ii) Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by or actively supporting terrorist activity or terrorist organisations.

(iii) Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.

[3] Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

[4] The term *associate NPOs* includes foreign branches of international NPOs.

[5] In this context, rules and regulations may include rules and standards applied by self regulatory bodies and accrediting institutions.

[6] The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, de-licensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

(iv) Countries should establish appropriate mechanisms to ensure that when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, this information is promptly shared with all relevant competent authorities in order to take preventative or investigative action.

d. Effective capacity to respond to international requests for information about an NPO of concern

Consistent with Special Recommendation V, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or other forms of terrorist support.

Interpretative Note to

Special Recommendation IX: Cash Couriers

Objectives

1. FATF Special Recommendation IX was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures 1) to detect the physical cross-border transportation of currency and bearer negotiable instruments, 2) to stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, 3) to stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed, 4) to apply appropriate sanctions for making a false declaration or disclosure, and 5) to enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering. Countries should implement Special Recommendation IX subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.

Definitions

2. For the purposes of Special Recommendation IX and this Interpretative Note, the following definitions apply.

3. The term *bearer negotiable instruments* includes monetary instruments in bearer form such as: travellers cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.[1]

4. The term *currency* refers to banknotes and coins that are in circulation as a medium of exchange.

5. The term *physical cross-border transportation* refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person,

[1] For the purposes of this Interpretative Note, gold, precious metals and precious stones are not included despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should co-operate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.

or in that person's accompanying luggage or vehicle; (2) shipment of currency through containerised cargo or (3) the mailing of currency or bearer negotiable instruments by a natural or legal person.

6. The term *false declaration* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.

7. The term *false disclosure* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.

8. When the term *related to terrorist financing or money laundering* is used to describe currency or bearer negotiable instruments, it refers to currency or bearer negotiable instruments that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

The types of systems that may be implemented to address the issue of cash couriers

9. Countries may meet their obligations under Special Recommendation IX and this Interpretative Note by implementing one of the following types of systems; however, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

a) Declaration system: The key characteristics of a declaration system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments, which are of a value exceeding a pre-set, maximum threshold of EUR/USD 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries that implement a declaration system should ensure that the pre-set threshold is sufficiently low to meet the objectives of Special Recommendation IX.

b) Disclosure system: The key characteristics of a disclosure system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the designated competent authorities can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.

Additional elements applicable to both systems

10. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and bearer negotiable instruments.

b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use.

c) Information obtained through the declaration/disclosure process should be available to the financial intelligence unit (FIU) either through a system whereby the FIU is notified about suspicious cross-border transportation incidents or by making the declaration/disclosure information directly available to the FIU in some other way.

d) At the domestic level, countries should ensure that there is adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Special Recommendation IX.

e) In the following two cases, competent authorities should be able to stop or restrain cash or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

f) The declaration/disclosure system should allow for the greatest possible measure of international co-operation and assistance in accordance with Special Recommendation V and Recommendations 35 to 40. To facilitate such co-operation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of EUR/USD 15,000 is made, or (ii) where there is a false declaration or false disclosure, or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by the appropriate authorities. At a minimum, this information will cover: (i) the amount of currency or bearer negotiable instruments declared / disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

Sanctions

11. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or bearer negotiable instruments.

Appendix D:

Financial Action Task Force, *The Forty Recommendations* (Paris: FATF, 2004)

Financial Action Task Force Groupe d'action financière

FATF Standards

FATF 40 Recommendations

October 2003
(incorporating all subsequent amendments until October 2004)

The FATF revised the 40 and the IX Recommendations. The revision of the FATF Recommendation was adopted and published in February 2012. See www.fatf-gafi.org/recommendations for the 2012 FATF Recommendations.

INTRODUCTION

Money laundering methods and techniques change in response to developing counter-measures. In recent years, the Financial Action Task Force (FATF) [1] has noted increasingly sophisticated combinations of techniques, such as the increased use of legal persons to disguise the true ownership and control of illegal proceeds, and an increased use of professionals to provide advice and assistance in laundering criminal funds. These factors, combined with the experience gained through the FATF's Non-Cooperative Countries and Territories process, and a number of national and international initiatives, led the FATF to review and revise the Forty Recommendations into a new comprehensive framework for combating money laundering and terrorist financing. The FATF now calls upon all countries to take the necessary steps to bring their national systems for combating money laundering and terrorist financing into compliance with the new FATF Recommendations, and to effectively implement these measures.

The review process for revising the Forty Recommendations was an extensive one, open to FATF members, non-members, observers, financial and other affected sectors and interested parties. This consultation process provided a wide range of input, all of which was considered in the review process.

The revised Forty Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the Eight Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing. The FATF recognises that countries have diverse legal and financial systems and so all cannot take identical measures to achieve the common objective, especially over matters of detail. The Recommendations therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional frameworks. The Recommendations cover all the measures that national systems should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and certain other businesses and professions; and international co-operation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering typologies. The 1996 Forty Recommendations have been endorsed by more than 130 countries and are the international anti-money laundering standard.

In October 2001 the FATF expanded its mandate to deal with the issue of the financing of terrorism, and took the important step of creating the Eight Special Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organisations, and are complementary to the Forty Recommendations[2].

A key element in the fight against money laundering and the financing of terrorism is the need for countries systems to be monitored and evaluated, with respect to these international standards. The mutual evaluations conducted by the FATF and FATF-style regional bodies, as well as the assessments conducted by the IMF and World Bank, are a vital mechanism for ensuring that the FATF Recommendations are effectively implemented by all countries.

[1] The FATF is an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering and terrorist financing. It currently has 36 members: 34 countries and governments and two international organisations; and more than 20 observers: five FATF-style regional bodies and more than 15 other international organisations or bodies. A list of all members and observers can be found on the FATF website at www.fatf-gafi.org.

[2] The FATF Forty and Eight Special Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering and the financing of terrorism.

THE FORTY RECOMMENDATIONS

A. LEGAL SYSTEMS

Scope of the criminal offence of money laundering

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year's imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences[3].

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

2. Countries should ensure that:

a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

[3] See the definition of "designated categories of offences" in the Glossary.

b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisonal measures and confiscation

3. Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

4. Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Customer due diligence and record-keeping

5.* Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information[4].

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

6.* Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.

[4] Reliable, independent source documents, data or information will hereafter be referred to as "identification data".

* Recommendations marked with an asterisk should be read in conjunction with their Interpretative Note.

b) Obtain senior management approval for establishing business relationships with such customers.

c) Take reasonable measures to establish the source of wealth and source of funds.

d) Conduct enhanced ongoing monitoring of the business relationship.

7. Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

b) Assess the respondent institution's anti-money laundering and terrorist financing controls.

c) Obtain approval from senior management before establishing new correspondent relationships.

d) Document the respective responsibilities of each institution.

e) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

8. Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

9.* Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.

10.* Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

11.* Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

12.* The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance

13.* If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

14.* Financial institutions, their directors, officers and employees should be:

a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

15.* Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

b) An ongoing employee training programme.

c) An audit function to test the system.

16.* The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Other measures to deter money laundering and terrorist financing

17. Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

19. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

20. Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

21. Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

22. Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

Regulation and supervision

23.* Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent

authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

24. Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:

- casinos should be licensed;
- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino
- competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

25.* The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.

C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent authorities, their powers and resources

26.* Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding

potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

27.* Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries.

28. When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

29. Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

30. Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.

31. Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

32. Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of legal persons and arrangements

33. Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures.

Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

34. Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

D. INTERNATIONAL CO-OPERATION

35. Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Mutual legal assistance and extradition

36. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

a) Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.

b) Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.

c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

37. Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within

the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

38.* There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.

39. Countries should recognise money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other forms of co-operation

40.* Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

GLOSSARY

In these Recommendations the following abbreviations and references are used:

"**Beneficial owner**" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

"**Core Principles**" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

"**Designated categories of offences**" means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

"**Designated non-financial businesses and professions**" means:

a) Casinos (which also includes internet casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

"**Designated threshold**" refers to the amount set out in the Interpretative Notes.

"**Financial institutions**" means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[5]
2. Lending.[6]
3. Financial leasing.[7]
4. The transfer of money or value.[8]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:

   (a) money market instruments (cheques, bills, CDs, derivatives etc.);

   (b) foreign exchange;

[5] This also captures private banking.

[6] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).

[7] This does not extend to financial leasing arrangements in relation to consumer products.

[8] This applies to financial activity in both the formal or informal sector *e.g.* alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

(c) exchange, interest rate and index instruments;

(d) transferable securities;

(e) commodity futures trading.

8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance[9].
13. Money and currency changing.

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

"**FIU**" means financial intelligence unit.

"**Legal arrangements**" refers to express trusts or other similar legal arrangements.

"**Legal persons**" refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

"**Payable-through accounts**" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

"**Politically Exposed Persons**" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

"**Shell bank**" means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

"**STR**" refers to suspicious transaction reports.

"**Supervisors**" refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

"**the FATF Recommendations**" refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing.

[9] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

INTERPRETATIVE NOTES

General

1. Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions".

2. Recommendations 5-16 and 21-22 state that financial institutions or designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige financial institutions or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.

3. Where reference is made to a financial institution being satisfied as to a matter, that institution must be able to justify its assessment to competent authorities.

4. To comply with Recommendations 12 and 16, countries do not need to issue laws or regulations that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws or regulations covering the underlying activities.

5. The Interpretative Notes that apply to financial institutions are also relevant to designated non-financial businesses and professions, where applicable.

Recommendations 5, 12 and 16

The designated thresholds for transactions (under Recommendations 5 and 12) are as follows:

- Financial institutions (for occasional customers under Recommendation 5) - USD/EUR 15 000.
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3 000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15 000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Recommendation 5

Customer due diligence and tipping off

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

   a) Normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.

   b) Make a STR to the FIU in accordance with Recommendation 13.

2. Recommendation 14 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

CDD for legal persons and arrangements

4. When performing elements (a) and (b) of the CDD process in relation to legal persons or arrangements, financial institutions should:

   a) Verify that any person purporting to act on behalf of the customer is so authorised, and identify that person.

   b) Identify the customer and verify its identity - the types of measures that would be normally needed to satisfactorily perform this function would require obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the customer's name, the names of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.

   c) Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons. The types of measures that would be normally needed to satisfactorily perform this function would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.

The relevant information or data may be obtained from a public register, from the customer or from other reliable sources.

Reliance on identification and verification already performed

5. The CDD measures set out in Recommendation 5 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile.

Timing of verification

6. Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include:

   - Non face-to-face business.
   - Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
   - Life insurance business. In relation to life insurance business, countries may permit the identification and verification of the beneficiary under the policy to take place after having established the business relationship with the policyholder. However, in all such cases, identification and verification should occur at or before the time of payout or the time where the beneficiary intends to exercise vested rights under the policy.

7. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. Financial institutions should refer to the Basel CDD paper[10] (section 2.2.6.) for specific guidance on examples of risk management measures for non-face to face business.

Requirement to identify existing customers

8. The principles set out in the Basel CDD paper concerning the identification of existing customers should serve as guidance when applying customer due diligence processes to institutions engaged in banking activity, and could apply to other financial institutions where relevant.

[10] "Basel CDD paper" refers to the guidance paper on Customer Due Diligence for Banks issued by the Basel Committee on Banking Supervision in October 2001.

Simplified or reduced CDD measures

9. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

10. Examples of customers where simplified or reduced CDD measures could apply are:

- Financial institutions – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.
- Public companies that are subject to regulatory disclosure requirements.
- Government administrations or enterprises.

11. Simplified or reduced CDD measures could also apply to the beneficial owners of pooled accounts held by designated non financial businesses or professions provided that those businesses or professions are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring their compliance with those requirements. Banks should also refer to the Basel CDD paper (section 2.2.4.), which provides specific guidance concerning situations where an account holding institution may rely on a customer that is a professional financial intermediary to perform the customer due diligence on his or its own customers (*i.e.* the beneficial owners of the bank account). Where relevant, the CDD Paper could also provide guidance in relation to similar accounts held by other types of financial institutions.

12. Simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

- Life insurance policies where the annual premium is no more than USD/EUR 1 000 or a single premium of no more than USD/EUR 2 500.
- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

13. Countries could also decide whether financial institutions could apply these simplified measures only to customers in its own jurisdiction or allow them to do for customers from any other jurisdiction that the original country is satisfied is in compliance with and has effectively implemented the FATF Recommendations.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

Recommendation 6

Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.

Recommendation 9

This Recommendation does not apply to outsourcing or agency relationships.

This Recommendation also does not apply to relationships, accounts or transactions between financial institutions for their clients. Those relationships are addressed by Recommendations 5 and 7.

Recommendations 10 and 11

In relation to insurance business, the word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits.

Recommendation 13

1. The reference to criminal activity in Recommendation 13 refers to:

   a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or

   b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

   Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

2. In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.

Recommendation 14 (tipping off)

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.

Recommendation 15

The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.

Recommendation 16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.

Recommendation 23

Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view. Hence, where shareholder suitability (or "fit and proper") tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Recommendation 25

When considering the feedback that should be provided, countries should have regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

Recommendation 26

Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

Recommendation 27

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

Recommendation 38

Countries should consider:

a) Establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

b) Taking such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Recommendation 40

1. For the purposes of this Recommendation:

   - "Counterparts" refers to authorities that exercise similar responsibilities and functions.
   - "Competent authority" refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

2. Depending on the type of competent authority involved and the nature and purpose of the co-operation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.

3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

   - Searching its own databases, which would include information related to suspicious transaction reports.
   - Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

   Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information.

Appendix E:

Financial Action Task Force, *The FATF Recommendations* (Paris: FATF, 2019)

INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING OF
TERRORISM & PROLIFERATION

The FATF Recommendations

Updated June 2019

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2012-2019), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France, www.fatf-gafi.org/recommendations.html

INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING
OF TERRORISM & PROLIFERATION

THE FATF RECOMMENDATIONS

ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012

Updated June 2019

CONTENTS

THE FATF RECOMMENDATIONS

Number	Old Number[1]	
		A – AML/CFT POLICIES AND COORDINATION
1	-	Assessing risks & applying a risk-based approach *
2	R.31	National cooperation and coordination
		B – MONEY LAUNDERING AND CONFISCATION
3	R.1 & R.2	Money laundering offence *
4	R.3	Confiscation and provisional measures *
		C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	SRII	Terrorist financing offence *
6	SRIII	Targeted financial sanctions related to terrorism & terrorist financing *
7		Targeted financial sanctions related to proliferation *
8	SRVIII	Non-profit organisations *
		D – PREVENTIVE MEASURES
9	R.4	Financial institution secrecy laws
		Customer due diligence and record keeping
10	R.5	Customer due diligence *
11	R.10	Record keeping
		Additional measures for specific customers and activities
12	R.6	Politically exposed persons *
13	R.7	Correspondent banking *
14	SRVI	Money or value transfer services *
15	R.8	New technologies
16	SRVII	Wire transfers *
		Reliance, Controls and Financial Groups
17	R.9	Reliance on third parties *
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries *
19	R.21	Higher-risk countries *
		Reporting of suspicious transactions
20	R.13 & SRIV	Reporting of suspicious transactions *
21	R.14	Tipping-off and confidentiality
		Designated non-financial Businesses and Professions (DNFBPs)
22	R.12	DNFBPs: Customer due diligence *
23	R.16	DNFBPs: Other measures *

		E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
24	R.33	Transparency and beneficial ownership of legal persons *
25	R.34	Transparency and beneficial ownership of legal arrangements *
		F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
		Regulation and Supervision
26	R.23	Regulation and supervision of financial institutions *
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs
		Operational and Law Enforcement
29	R.26	Financial intelligence units *
30	R.27	Responsibilities of law enforcement and investigative authorities *
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers *
		General Requirements
33	R.32	Statistics
34	R.25	Guidance and feedback
		Sanctions
35	R.17	Sanctions
		G – INTERNATIONAL COOPERATION
36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation *
39	R.39	Extradition
40	R.40	Other forms of international cooperation *

1. The 'old number' column refers to the corresponding 2003 FATF Recommendation.

** Recommendations marked with an asterisk have interpretive notes, which should be read in conjunction with the Recommendation.*

Version as adopted on 15 February 2012.

INTRODUCTION

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:

- identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;
- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- facilitate international cooperation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

Following the conclusion of the third round of mutual evaluations of its members, the FATF has reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (FSRBs) and the observer organisations, including the International Monetary Fund, the World Bank and the United Nations. The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations.

The FATF Standards have also been revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced. Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk. The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.

Combating terrorist financing is a very significant challenge. An effective AML/CFT system, in general, is important for addressing terrorist financing, and most measures previously focused on terrorist financing are now integrated throughout the Recommendations, therefore obviating the need for the Special Recommendations. However, there are some Recommendations that are unique to terrorist financing, which are set out in Section C of the FATF Recommendations. These are: Recommendation 5 (the criminalisation of terrorist financing); Recommendation 6 (targeted financial sanctions related to terrorism & terrorist financing); and Recommendation 8 (measures to prevent the misuse of non-profit organisations). The proliferation of weapons of mass destruction is also a significant security concern, and in 2008 the FATF's mandate was expanded to include dealing with the financing of proliferation of weapons of mass destruction. To combat this threat, the FATF has adopted a new Recommendation (Recommendation 7) aimed at ensuring consistent and effective implementation of targeted financial sanctions when these are called for by the UN Security Council.

The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. The measures set out in the FATF Standards should be implemented by all members of the FATF and the FSRBs, and their implementation is assessed rigorously through Mutual Evaluation processes, and through the assessment processes of the International Monetary Fund and the World Bank – on the basis of the FATF's common assessment methodology. Some Interpretive Notes and definitions in the glossary include examples which illustrate how the requirements could be applied. These examples are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

The FATF also produces Guidance, Best Practice Papers, and other advice to assist countries with the implementation of the FATF standards. These other documents are not mandatory for assessing compliance with the Standards, but countries may find it valuable to have regard to them when considering how best to implement the FATF Standards. A list of current FATF Guidance and Best

Practice Papers, which are available on the FATF website, is included as an annex to the Recommendations.

The FATF is committed to maintaining a close and constructive dialogue with the private sector, civil society and other interested parties, as important partners in ensuring the integrity of the financial system. The revision of the Recommendations has involved extensive consultation, and has benefited from comments and suggestions from these stakeholders. Going forward and in accordance with its mandate, the FATF will continue to consider changes to the standards, as appropriate, in light of new information regarding emerging threats and vulnerabilities to the global financial system.

The FATF calls upon all countries to implement effective measures to bring their national systems for combating money laundering, terrorist financing and the financing of proliferation into compliance with the revised FATF Recommendations.

THE FATF RECOMMENDATIONS

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach *

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence *

Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures *

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of *bona fide* third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence *

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing *

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation *

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organisations *

Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

(a) by terrorist organisations posing as legitimate entities;

(b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

(c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence *

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons *

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

(b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and source of funds; and

(d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking *

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships;

(d) clearly understand the respective responsibilities of each institution; and

(e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services *

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

16. Wire transfers *

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

RELIANCE, CONTROLS AND FINANCIAL GROUPS

17. Reliance on third parties *

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries *

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-

wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

19. Higher-risk countries *

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions *

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence *

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

(a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

(b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures *

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d)

of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

(b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons *

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements *

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions *

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs *

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- casinos should be licensed;

- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units *

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities *

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary,

cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers *

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

(a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.

(b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

(c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

(d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).

(e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

(a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation *

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

(a) ensure money laundering and terrorist financing are extraditable offences;

(b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;

(c) not place unreasonable or unduly restrictive conditions on the execution of requests; and

(d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation *

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing

cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

INTERPRETIVE NOTES TO THE FATF RECOMMENDATIONS

INTERPRETIVE NOTE TO RECOMMENDATION 1 (ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH)

1. The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also, in strictly limited circumstances and where there is a proven low risk of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from money laundering and terrorist financing, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors.

A. Obligations and decisions for countries

3. **Assessing risk** - Countries[1] should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

4. **Higher risk** - Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks, and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.

5. **Lower risk** - Countries may decide to allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its money laundering and terrorist financing risks, as referred to in paragraph 3.

   Independent of any decision to specify certain lower risk categories in line with the previous paragraph, countries may also allow financial institutions and DNFBPs to apply simplified customer due diligence (CDD) measures, provided that the requirements set out in section B below ("Obligations and decisions for financial institutions and DNFBPs"), and in paragraph 7 below, are met.

6. **Exemptions** - Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided:

   (a) there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

   (b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.

[1] Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

While the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered.

7. **Supervision and monitoring of risk** - Supervisors (or SRBs for relevant DNFBPs sectors) should ensure that financial institutions and DNFBPs are effectively implementing the obligations set out below. When carrying out this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration.

B. Obligations and decisions for financial institutions and DNFBPs

8. **Assessing risk** - Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their money laundering and terrorist financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

9. **Risk management and mitigation** - Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs.

10. **Higher risk** - Where higher risks are identified financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks.

11. **Lower risk** - Where lower risks are identified, countries may allow financial institutions and DNFBPs to take simplified measures to manage and mitigate those risks.

12. When assessing risk, financial institutions and DNFBPs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBPs may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

INTERPRETIVE NOTE TO RECOMMENDATION 3 (MONEY LAUNDERING OFFENCE)

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

2. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches.

3. Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment.

4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

5. Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically.

6. Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

7. Countries should ensure that:

   (a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances.

   (b) Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering.

   (c) Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of

liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

(d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

INTERPRETIVE NOTE TO RECOMMENDATIONS 4 AND 38 (CONFISCATION AND PROVISIONAL MEASURES)

Countries should establish mechanisms that will enable their competent authorities to effectively manage and, when necessary, dispose of, property that is frozen or seized, or has been confiscated. These mechanisms should be applicable both in the context of domestic proceedings, and pursuant to requests by foreign countries.

INTERPRETIVE NOTE TO RECOMMENDATION 5 (TERRORIST FINANCING OFFENCE)

A. Objectives

1. Recommendation 5 was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and, *inter alia*, money laundering, another objective of Recommendation 5 is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering.

B. Characteristics of the terrorist financing offence

2. Terrorist financing offences should extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.

3. Terrorist financing includes financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with this Recommendation.

5. Terrorist financing offences should extend to any funds or other assets, whether from a legitimate or illegitimate source.

6. Terrorist financing offences should not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

7. Countries should ensure that the intent and knowledge required to prove the offence of terrorist financing may be inferred from objective factual circumstances.

8. Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of terrorist financing.

9. Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

10. It should also be an offence to attempt to commit the offence of terrorist financing.

11. It should also be an offence to engage in any of the following types of conduct:

    (a) Participating as an accomplice in an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(b) Organising or directing others to commit an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(c) Contributing to the commission of one or more offence(s), as set forth in paragraphs 2 or 9 of this Interpretive Note, by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

12. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

INTERPRETIVE NOTE TO RECOMMENDATION 6 (TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING)

A. OBJECTIVE

1. Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person[2] or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions[3]; or (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

2. It should be stressed that none of the obligations in Recommendation 6 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 4 (confiscation and provisional measures)[4]. Measures under Recommendation 6 may complement criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not conditional upon the existence of such proceedings. Instead, the focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups. In determining the limits of, or fostering widespread support for, an effective counter-terrorist financing regime, countries must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

---

2 Natural or legal person.

3 Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

4 Based on requirements set, for instance, in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)(the Vienna Convention)* and the *United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention),* which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the *International Convention for the Suppression of the Financing of Terrorism (1999)(the Terrorist Financing Convention)* contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Recommendation 6 and the United Nations Security Council Resolutions related to terrorist financing.

B. IDENTIFYING AND DESIGNATING PERSONS AND ENTITIES FINANCING OR SUPPORTING TERRORIST ACTIVITIES

3. For resolution 1267 (1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), designations are made, at the national or supranational level, by a country or countries acting on their own motion, or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

4. Countries need to have the authority, and effective procedures or mechanisms, to identify and initiate proposals for designations of persons and entities targeted by resolution 1267 (1999) and its successor resolutions, consistent with the obligations set out in those Security Council resolutions[5]. Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council list-based programmes, pursuant to those Security Council resolutions. Countries also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373 (2001), consistent with the obligations set out in that Security Council resolution. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in resolution 1373 (2001), described in Section E. A country's regime to implement resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), should include the following necessary elements:

   (a) Countries should identify a competent authority or a court as having responsibility for:

      (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1989 (2011) (on Al-Qaida) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;

      (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1988 (2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and

[5] The relevant Security Council resolutions do not require countries to identify persons or entities and submit these to the relevant United Nations Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

(iii) designating persons or entities that meet the specific criteria for designation, as set forth in resolution 1373 (2001), as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

(b) Countries should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1988 (2011) and resolution 1989 (2011) and related resolutions, and resolution 1373 (2001) (see Section E for the specific designation criteria of relevant Security Council resolutions). This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to resolution 1373 (2001). To ensure that effective cooperation is developed among countries, countries should ensure that, when receiving a request, they make a prompt determination whether they are satisfied, according to applicable (supra-) national principles, that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2011), as set forth in Section E.

(c) The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) When deciding whether or not to make a (proposal for) designation, countries should apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis". For designations under resolutions 1373 (2001), the competent authority of each country will apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.

(e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to resolution 1267 (1999) and its successor resolutions, countries should:

(i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice;

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and

(iv) specify whether their status as a designating state may be made known.

(f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to resolution 1988 (2011) and its successor resolutions, countries should:

(i) follow the procedures for listing, as adopted by the 1988 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice; and

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.

(g) When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(h) Countries should have procedures to be able to operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of resolution 1267 (1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), the obligation for countries to take freezing action and prohibit the dealing in funds or other assets of designated persons and entities, without delay, is triggered by a designation at the (supra-)national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

6. Countries should establish the necessary legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries[6] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(b) Countries should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or

[6] In the case of the European Union (EU), which is a supra-national jurisdiction under Recommendation 6, the EU law applies as follows. The assets of designated persons and entities are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(d) Countries should require financial institutions and DNFBPs[7] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities.

(e) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions that, in the view of the country, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988 Committee has de-listed a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), and any successor resolutions. In the case of de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and any successor resolutions.

8. For persons and entities designated pursuant to resolution 1373 (2001), countries should have appropriate legal authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons and entities that no longer meet the criteria for designation. Countries should also have procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.

9. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of

[7] Security Council resolutions apply to all natural and legal persons within the country.

such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

10. Where countries have determined that funds or other assets of persons and entities designated by the Security Council, or one of its relevant sanctions committees, are necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, countries should authorise access to such funds or other assets in accordance with the procedures set out in Security Council resolution 1452 (2002) and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to resolution 1373 (2001) and as set out in resolution 1963 (2010).

11. Countries should provide for a mechanism through which a designated person or entity can challenge their designation, with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions.

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions**[8]:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof[9]; or

[8] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999). At the time of issuance of this Interpretive Note, (February 2012) , the successor resolutions to resolution 1267 (1999) are: resolutions 1333 (2000), 1367 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

[9] OP2 of resolution 1617 (2005) further defines the criteria for being "associated with" Al-Qaida or Usama bin Laden.

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i), or by persons acting on their behalf or at their direction.

(b) **Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions**:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(b)(i) of this subparagraph, or by persons acting on their behalf or at their direction.

(c) **Security Council resolution 1373 (2001)**:

(i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;

(ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(c) (i) of this subparagraph; or

(iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection 13(c) (i) of this subparagraph.

INTERPRETIVE NOTE TO RECOMMENDATION 7 (TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION)

A. OBJECTIVE

1. Recommendation 7 requires countries to implement targeted financial sanctions[10] to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person[11] or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.[12]

2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation.[13] The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

---

10 Recommendation 7 is focused on targeted financial sanctions. These include the specific restrictions set out in Security Council resolution 2231 (2015) (see Annex B paragraphs 6(c) and (d)). However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions, category-based sanctions and vigilance measures). With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction and other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

11 Natural or legal person.

12 Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Interpretive Note (June 2017), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017). Resolution 2231 (2015), endorsing the Joint Comprehensive Plan of Action, terminated all provisions of resolutions relating to Iran and proliferation financing, including 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010), but established specific restrictions including targeted financial sanctions. This lifts sanctions as part of a step by step approach with reciprocal commitments endorsed by the Security Council. Implementation day of the JCPOA was on 16 January 2016.

13 Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty*, the *Biological and Toxin Weapons Convention*, the *Chemical Weapons Convention*, and Security Council resolutions 1540 (2004) and 2235 (2016). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

B. DESIGNATIONS

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations to the Security Council or the relevant Security Council Committee(s). However, in practice, the Security Council or the relevant Committee(s) primarily depends upon requests for designation by Member States. Security Council resolution 1718 (2006) provides that the relevant Committee shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by this resolution and its successor resolutions. Resolution 2231 (2015) provides that the Security Council shall make the necessary practical arrangements to undertake directly tasks related to the implementation of the resolution.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:

   (a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:

      (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006) and its successor resolutions[14], if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and

      (ii) proposing to the Security Council, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 2231 (2015) and any future successor resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions).

   (b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 2231 (2015), and their successor and any future successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.

[14] Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note (June 2017), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009), resolution 2087 (2013), resolution 2094 (2013), resolution 2270 (2016), resolution 2321 (2016) and resolution 2356 (2017).

(c) having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.

(e) when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the Security Council, pursuant to resolution 2231 (2015) and any future successor resolutions, providing as much detail as possible on:

(i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and

(ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(f) having procedures to be able, where necessary, to operate ex parte against a person or entity who has been identified and whose proposal for designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:

(a) in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council[15]; and

(b) in the case of resolution 2231 (2015) and any future successor resolutions by the Security Council,

when acting under the authority of Chapter VII of the Charter of the United Nations.

15 As noted in resolution 2270 (2016) (OP32) this also applies to entities of the Government of the Democratic People's Republic of Korea or the Worker's Party of Korea that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

6. Countries should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries[16] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

(b) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(d) Countries should require financial institutions and DNFBPs[17] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.

(e) Countries should adopt effective measures which protect the rights of bona fide third parties acting in good faith when implementing the obligations under Recommendation 7.

(f) Countries should adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions and DNFBPs with the relevant laws or

16 In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU Common Foreign and Security Policy (CFSP) Council decisions and Council regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

17 Security Council resolutions apply to all natural and legal persons within the country.

enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities, that, in the view of the country, do not or no longer meet the criteria for designation. Once the Security Council or the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer exists. In the case of resolution 1718 (2006) and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

8. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e., a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

9. Where countries have determined that the exemption conditions set out in resolution 1718(2006) and resolution 2231 (2015) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.

10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 2231 (2015) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

11. Freezing action taken pursuant to resolution 1737 (2006) and continued by resolution 2231 (2015), or taken pursuant to resolution 2231 (2015), shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:

    (a) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in resolution 2231 (2015) and any future successor resolutions;

    (b) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity subject to the measures in paragraph 6 of Annex B to resolution 2231 (2015); and

(c) the relevant countries have submitted prior notification to the Security Council of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.[18]

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **On DPRK - Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016)**:

(i) any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programmes;

(ii) any person or entity providing support for DPRK's nuclear-related, other WMD-related and ballistic missile-related programmes, including through illicit means;

(iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[19];

(iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[20];

(v) any person or entity that has assisted in the evasion of sanctions or in violating the provisions of resolutions 1718 (2006) and 1874 (2009);

(vi) any person or entity that has contributed to DPRK's prohibited programmes, activities prohibited by the DPRK-related resolutions, or to the evasion of provisions; or

---

18 In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, adopted in June 2013.*

19 The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee. Further, resolution 2270 (2016) OP23 expanded the scope of targeted financial sanctions obligations under resolution 1718 (2006), by applying these to the Ocean Maritime Management Company vessels specified in Annex III of resolution 2270 (2016).

20 Ibid.

(vii) any entity of the Government of the DPRK or the Worker's Party of Korea, or person or entity acting on their behalf or at their direction, or by any entity owned or controlled by them, that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

(b) **On Iran - Resolution 2231 (2015)**:

(i) any person or entity having engaged in, directly associated with or provided support for Iran's proliferation sensitive nuclear activities contrary to Iran's commitments in the Joint Comprehensive Plan of Action (JCPOA) or the development of nuclear weapon delivery systems, including through the involvement in procurement of prohibited items, goods, equipment, materials and technology specified in Annex B to resolution 2231 (2015);

(ii) any person or entity assisting designated persons or entities in evading or acting inconsistently with the JCPOA or resolution 2231 (2015); and

(iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i), subsection 13(b)(ii) and/or subsection 13(b)(iii), or by any entities owned or controlled by them.

INTERPRETIVE NOTE TO RECOMMENDATION 8 (NON-PROFIT ORGANISATIONS)

A. INTRODUCTION

1. Given the variety of legal forms that non-profit organisations (NPOs) can have, depending on the country, the FATF has adopted a functional definition of NPO. This definition is based on those activities and characteristics of an organisation which put it at risk of terrorist financing abuse, rather than on the simple fact that it is operating on a non-profit basis. For the purposes of this Recommendation, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". Without prejudice to Recommendation 1, this Recommendation only applies to those NPOs which fall within the FATF definition of an NPO. It does not apply to the entire universe of NPOs.

2. NPOs play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The FATF recognises the vital importance of NPOs in providing these important charitable services, as well as the difficulty of providing assistance to those in need, often in high risk areas and conflict zones, and applauds the efforts of NPOs to meet such needs. The FATF also recognises the intent and efforts to date of NPOs to promote transparency within their operations and to prevent terrorist financing abuse, including through the development of programmes aimed at discouraging radicalisation and violent extremism. The ongoing international campaign against terrorist financing has identified cases in which terrorists and terrorist organisations exploit some NPOs in the sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. As well, there have been cases where terrorists create sham charities or engage in fraudulent fundraising for these purposes. This misuse not only facilitates terrorist activity, but also undermines donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting NPOs from terrorist financing abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs and the donor community. Measures to protect NPOs from potential terrorist financing abuse should be targeted and in line with the risk-based approach. It is also important for such measures to be implemented in a manner which respects countries' obligations under the Charter of the United Nations and international human rights law.

3. Some NPOs may be vulnerable to terrorist financing abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. In some cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate some NPOs and misuse funds and operations to cover for, or support, terrorist activity.

B. OBJECTIVES AND GENERAL PRINCIPLES

4. The objective of Recommendation 8 is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes. In this Interpretive Note, the approach taken to achieve this objective is based on the following general principles:

   (a) A risk-based approach applying focused measures in dealing with identified threats of terrorist financing abuse to NPOs is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to terrorist financing abuse, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.

   (b) Flexibility in developing a national response to terrorist financing abuse of NPOs is essential, in order to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

   (c) Past and ongoing terrorist financing abuse of NPOs requires countries to adopt effective and proportionate measures, which should be commensurate to the risks identified through a risk-based approach.

   (d) Focused measures adopted by countries to protect NPOs from terrorist financing abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote accountability and engender greater confidence among NPOs, across the donor community and with the general public, that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of accountability, integrity and public confidence in the management and functioning of NPOs are integral to ensuring they cannot be abused for terrorist financing.

   (e) Countries are required to identify and take effective and proportionate action against NPOs that either are exploited by, or knowingly supporting, terrorists or terrorist organisations taking into account the specifics of the case. Countries should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should, to the extent reasonably possible, minimise negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

   (f) Developing cooperative relationships among the public and private sectors and with NPOs is critical to understanding NPOs' risks and risk mitigation strategies, raising awareness, increasing effectiveness and fostering capabilities to combat terrorist

financing abuse within NPOs. Countries should encourage the development of academic research on, and information-sharing in, NPOs to address terrorist financing related issues.

C. MEASURES

5. Without prejudice to the requirements of Recommendation 1, since not all NPOs are inherently high risk (and some may represent little or no risk at all), countries should identify which subset of organisations fall within the FATF definition of NPO. In undertaking this exercise, countries should use all relevant sources of information in order to identify features and types of NPOs, which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse.[21] It is also crucial to identify the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs. Countries should review the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for terrorism financing support in order to be able to take proportionate and effective actions to address the risks identified. These exercises could take a variety of forms and may or may not be a written product. Countries should also periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities to ensure effective implementation of measures.

6. There is a diverse range of approaches in identifying, preventing and combating terrorist financing abuse of NPOs. An effective approach should involve all four of the following elements: (a) sustained outreach, (b) targeted risk-based supervision or monitoring, (c) effective investigation and information gathering and (d) effective mechanisms for international cooperation. The following measures represent examples of specific actions that countries should take with respect to each of these elements, in order to protect NPOs from potential terrorist financing abuse.

   (a) Sustained outreach concerning terrorist financing issues

      (i) Countries should have clear policies to promote accountability, integrity and public confidence in the administration and management of NPOs.

      (ii) Countries should encourage and undertake outreach and educational programmes to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.

      (iii) Countries should work with NPOs to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect them from terrorist financing abuse.

[21] For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

(iv) Countries should encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

(b) Targeted risk-based supervision or monitoring of NPOs

Countries should take steps to promote effective supervision or monitoring. A "one-size-fits-all" approach would be inconsistent with the proper implementation of a risk-based approach as stipulated under Recommendation 1 of the FATF Standards. In practice, countries should be able to demonstrate that risk-based measures apply to NPOs at risk of terrorist financing abuse. It is also possible that existing regulatory or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a jurisdiction, although terrorist financing risks to the sector should be periodically reviewed. Appropriate authorities should monitor the compliance of NPOs with the requirements of this Recommendation, including the risk-based measures being applied to them.[22] Appropriate authorities should be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[23] The following are some examples of measures that could be applied to NPOs, in whole or in part, depending on the risks identified:

(i) NPOs could be required to license or register. This information should be available to competent authorities and encouraged to be available to the public.[24]

(ii) NPOs could be required to maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information could be publicly available either directly from the NPO or through appropriate authorities.

(iii) NPOs could be required to issue annual financial statements that provide detailed breakdowns of incomes and expenditures.

(iv) NPOs could be required to have appropriate controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the NPO's stated activities.

(v) NPOs could be required to take reasonable measures to confirm the identity, credentials and good standing of beneficiaries[25] and associate NPOs and that

22 In this context, rules and regulations may include rules and standards applied by self-regulatory organisations and accrediting institutions.

23 The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, de-licensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

24 Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

they are not involved with and/or using the charitable funds to support terrorists or terrorist organisations[26]. However, NPOs should not be required to conduct customer due diligence. NPOs could be required to take reasonable measures to document the identity of their significant donors and to respect donor confidentiality. The ultimate objective of this requirement is to prevent charitable funds from being used to finance and support terrorists and terrorist organisations.

(vi) NPOs could be required to maintain, for a period of at least five years, records of domestic and international transactions that are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the organisation, and could be required to make these available to competent authorities upon appropriate authority. This also applies to information mentioned in paragraphs (ii) and (iii) above. Where appropriate, records of charitable activities and financial operations by NPOs could also be made available to the public.

(c) Effective information gathering and investigation

(i) Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs.

(ii) Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.

(iii) Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.

(iv) Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is involved in terrorist financing abuse and/or is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, that this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action.

---

25 The term beneficiaries refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.

26 This does not mean that NPOs are expected to identify each specific individual, as such a requirement would not always be possible and would, in some instances, impede the ability of NPOs to provide much-needed services

(d) Effective capacity to respond to international requests for information about an NPO of concern. Consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support.

D. RESOURCES FOR SUPERVISION, MONITORING, AND INVESTIGATION

7. Countries should provide their appropriate authorities, which are responsible for supervision, monitoring and investigation of their NPO sector, with adequate financial, human and technical resources.

Glossary of specific terms used in this Recommendation	
Appropriate authorities	refers to competent authorities, including regulators, tax authorities, FIUs, law enforcement, intelligence authorities, accrediting institutions, and potentially self-regulatory organisations in some jurisdictions.
Associate NPOs	includes foreign branches of international NPOs, and NPOs with which partnerships have been arranged.
Beneficiaries	refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.
Non-profit organisation or NPO	refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".
Terrorist financing abuse	refers to the exploitation by terrorists and terrorist organisations of NPOs to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support terrorists or terrorist organisations and operations.

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

A. CUSTOMER DUE DILIGENCE AND TIPPING-OFF

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

   (a) normally seek to identify and verify the identity[27] of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and

   (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.

2. Recommendation 21 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements[28], financial institutions should be required to identify and verify the identity of

---

27 Reliable, independent source documents, data or information will hereafter be referred to as "identification data."

28 In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue

the customer, and understand the nature of its business, and its ownership and control structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

(a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

  (i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

  (ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

  (iii) The address of the registered office, and, if different, a principal place of business.

(b) Identify the beneficial owners of the customer and take reasonable measures[29] to verify the identity of such persons, through the following information:

  (i) For legal persons[30]:

    (i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest[31] in a legal person; and

---

to apply, including paragraph 4 of INR.10, but the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

29 In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

30 Measures (i.i) to (i.iii) are not alternative options, but are cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

31 A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

(i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(ii) For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries[32], and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the

[32] For beneficiary(ies) of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

10. The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

F. TIMING OF VERIFICATION

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

G. EXISTING CUSTOMERS

13. Financial institutions should be required to apply CDD measures to existing customers[33] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

H. RISK BASED APPROACH[34]

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:[35]

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.

---

33 Existing customers as at the date that the national requirements are brought into force.

34 The RBA does not apply to the circumstances when CDD should be required but may be used to determine the extent of such measures.

35 Under Recommendation 19 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties

Lower risks

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

(a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.

(b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Risk variables

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

    - Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
    - Reducing the frequency of customer identification updates.
    - Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
    - Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

    Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Thresholds

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Ongoing due diligence

23. Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

INTERPRETIVE NOTE TO RECOMMENDATION 12 (POLITICALLY EXPOSED PERSONS)

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the payout. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

a) inform senior management before the payout of the policy proceeds; and

b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

INTERPRETIVE NOTE TO RECOMMENDATION 13 (CORRESPONDENT BANKING)

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

The term *payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

INTERPRETIVE NOTE TO RECOMMENDATION 14 (MONEY OR VALUE TRANSFER SERVICES)

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

INTERPRETIVE NOTE TO RECOMMENDATION 15

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)

2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created[36]. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.

4. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk- based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

[36] References to creating a legal person include incorporation of companies or any other mechanism that is used.

6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

7. With respect to the preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:

(a) R. 10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.
(b) R. 16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information[37] on virtual asset transfers, submit[38] the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

8. Countries should rapidly, constructively, and effectively provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

[37] As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context.

[38] The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers.

INTERPRETIVE NOTE TO RECOMMENDATION 16 (WIRE TRANSFERS)

A. OBJECTIVE

1. Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:

   (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;

   (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and

   (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.

2. To accomplish these objectives, countries should have the ability to trace all wire transfers. Due to the potential terrorist financing threat posed by small wire transfers, countries should minimise thresholds taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

B. SCOPE

3. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers , including serial payments, and cover payments.

4. Recommendation 16 is not intended to cover the following types of payments:

   (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.

   (b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

5. Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

   (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.

   (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

C. CROSS-BORDER QUALIFYING WIRE TRANSFERS

6. Information accompanying all qualifying wire transfers should always contain:

   (a) the name of the originator;

   (b) the originator account number where such an account is used to process the transaction;

   (c) the originator's address, or national identity number, or customer identification number[39], or date and place of birth;

   (d) the name of the beneficiary; and

   (e) the beneficiary account number where such an account is used to process the transaction.

7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

8. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraph 6 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 7 above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

D. DOMESTIC WIRE TRANSFERS

9. Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter

[39] The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

10. The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

E. RESPONSIBILITIES OF ORDERING, INTERMEDIARY AND BENEFICIARY FINANCIAL INSTITUTIONS

Ordering financial institution

11. The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information.

12. The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.

13. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

14. The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above.

Intermediary financial institution

15. For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it

16. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

17. An intermediary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

18. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

Beneficiary financial institution

19. A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

20. For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

21. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

    (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

    (b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Glossary of specific terms used in this Recommendation	
Accurate	is used to describe information that has been verified for accuracy.
Batch transfer	is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficiary	refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
Beneficiary Financial Institution	refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.
Cover Payment	refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution

Glossary of specific terms used in this Recommendation

	through one or more intermediary financial institutions.
Cross-border wire transfer	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of *wire transfer* in which at least one of the financial institutions involved is located in a different country.
Domestic wire transfers	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of *wire transfer* that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of *wire transfer* that takes place entirely within the borders of the European Economic Area (EEA)[40].
Intermediary financial institution	refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
Ordering financial institution	refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
Originator	refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
Qualifying wire transfers	means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.
Required	is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the *required originator information.* Subparagraphs 6(d) and 6(e) set out the *required beneficiary information.*

40 An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

Glossary of specific terms used in this Recommendation	
Serial Payment	refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g. correspondent banks).
Straight-through processing	refers to payment transactions that are conducted electronically without the need for manual intervention.
Unique transaction reference number	refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
Wire transfer	refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.[41]

[41] It is understood that the settlement of wire transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).

INTERPRETIVE NOTE TO RECOMMENDATION 17 (RELIANCE ON THIRD PARTIES)

1. This Recommendation does not apply to outsourcing or agency relationships. In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity.

2. For the purposes of Recommendation 17, the term *relevant competent authorities* means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.

3. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

INTERPRETIVE NOTE TO RECOMMENDATION 18 (INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES)

1. Financial institutions' programmes against money laundering and terrorist financing should include:

   (a) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;

   (b) an ongoing employee training programme; and

   (c) an independent audit function to test the system.

2. The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

3. Compliance management arrangements should include the appointment of a compliance officer at the management level.

4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial

group, including, as appropriate, requesting the financial group to close down its operations in the host country.

INTERPRETIVE NOTE TO RECOMMENDATION 19 (HIGHER-RISK COUNTRIES)

1. The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.

2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:

   (a) Requiring financial institutions to apply specific elements of enhanced due diligence.

   (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.

   (c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.

   (d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.

   (e) Limiting business relationships or financial transactions with the identified country or persons in that country.

   (f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.

   (g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.

   (h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.

   (i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

   There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries

INTERPRETIVE NOTE TO RECOMMENDATION 20 (REPORTING OF SUSPICIOUS TRANSACTIONS)

1. The reference to criminal activity in Recommendation 20 refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3. Countries are strongly encouraged to adopt the first of these alternatives.
2. The reference to terrorist financing in Recommendation 20 refers to: the financing of terrorist acts and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.
3. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.
4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called "indirect reporting"), is not acceptable.

INTERPRETIVE NOTE TO RECOMMENDATIONS 22 AND 23 (DNFBPS)

1. The designated thresholds for transactions are as follows:

   - Casinos (under Recommendation 22) - USD/EUR 3,000
   - For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 22 and 23) - USD/EUR 15,000.

   Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

2. The Interpretive Notes that apply to financial institutions are also relevant to DNFBPs, where applicable. To comply with Recommendations 22 and 23, countries do not need to issue laws or enforceable means that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions, so long as these businesses or professions are included in laws or enforceable means covering the underlying activities.

INTERPRETIVE NOTE TO RECOMMENDATION 22 (DNFBPS – CUSTOMER DUE DILIGENCE)

1. Real estate agents should comply with the requirements of Recommendation 10 with respect to both the purchasers and vendors of the property.

2. Casinos should implement Recommendation 10, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/EUR 3,000. Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

INTERPRETIVE NOTE TO RECOMMENDATION 23 (DNFBPS – OTHER MEASURES)

1. Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

2. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.

3. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU.

4. Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

INTERPRETIVE NOTE TO RECOMMENDATION 24 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS)

1. Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information[42]) that are created[43] in the country. Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. It is also very likely that countries will need to utilise a combination of mechanisms to achieve the objective.

2. As part of the process of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:

   (a) identify and describe the different types, forms and basic features of legal persons in the country.

   (b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information;

   (c) make the above information publicly available; and

   (d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country.

A. BASIC INFORMATION

3. In order to determine who the beneficial owners of a company are, competent authorities will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.

4. All companies created in a country should be registered in a company registry.[44] Whichever combination of mechanisms is used to obtain and record beneficial ownership information (see section B), there is a set of basic information on a company that needs to be obtained and recorded by the company[45] as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be:

---

42 Beneficial ownership information for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (e.g. 25%).

43 References to creating a legal person, include incorporation of companies or any other mechanism that is used.

44 "Company registry" refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

45 The information can be recorded by the company itself or by a third person under the company's responsibility.

(a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors; and

(b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder[46] and categories of shares (including the nature of the associated voting rights).

5. The company registry should record all the basic information set out in paragraph 4(a) above.

6. The company should maintain the basic information set out in paragraph 4(b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request.

B. BENEFICIAL OWNERSHIP INFORMATION

7. Countries should ensure that either: (a) information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or (b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority.

8. In order to meet the requirements in paragraph 7, countries should use one or more of the following mechanisms:

(a) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

(b) Requiring companies to take reasonable measures[47] to obtain and hold up-to-date information on the companies' beneficial ownership;

(c) Using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22[48]; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (e.g. company registries, tax authorities or financial or other regulators); (iii) information held by the company as required above in Section A; and (iv) available information on companies listed on a stock exchange, where disclosure requirements (either by stock exchange rules or through law or enforceable means) impose requirements to ensure adequate transparency of beneficial ownership.

46 This is applicable to the nominal owner of all registered shares.

47 Measures taken should be proportionate to the level of risk or complexity induced by the ownership structure of the company or the nature of the controlling shareholders.

48 Countries should be able to determine in a timely manner whether a company has an account with a financial institution within the country.

9. Regardless of which of the above mechanisms are used, countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner. This should include:

   (a) Requiring that one or more natural persons resident in the country is authorised by the company[49], and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

   (b) Requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

   (c) Other comparable measures, specifically identified by the country, which can effectively ensure cooperation.

10. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

C. TIMELY ACCESS TO CURRENT AND ACCURATE INFORMATION

11. Countries should have mechanisms that ensure that basic information, including information provided to the company registry, is accurate and updated on a timely basis. Countries should require that any available information referred to in paragraph 7 is accurate and is kept as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.

12. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

13. Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in paragraph 4(a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in paragraph 4(b) above.

D. OBSTACLES TO TRANSPARENCY

14. Countries should take measures to prevent the misuse of bearer shares and bearer share warrants, for example by applying one or more of the following mechanisms: (a) prohibiting

[49] Members of the company's board or senior management may not require specific authorisation by the company.

them; (b) converting them into registered shares or share warrants (for example through dematerialisation); (c) immobilising them by requiring them to be held with a regulated financial institution or professional intermediary; or (d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity.

15. Countries should take measures to prevent the misuse of nominee shares and nominee directors, for example by applying one or more of the following mechanisms: (a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register; or (b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request.

E. OTHER LEGAL PERSONS

16. In relation to foundations, Anstalt, and limited liability partnerships, countries should take similar measures and impose similar requirements, as those required for companies, taking into account their different forms and structures.

17. As regards other types of legal persons, countries should take into account the different forms and structures of those other legal persons, and the levels of money laundering and terrorist financing risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and current by such legal persons, and that such information is accessible in a timely way by competent authorities. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and current beneficial ownership information for such legal persons.

F. LIABILITY AND SANCTIONS

18. There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability and effective, proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

G. INTERNATIONAL COOPERATION

19. Countries should rapidly, constructively and effectively provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries should monitor

the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

INTERPRETIVE NOTE TO RECOMMENDATION 25 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS)

1. Countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust. This should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. Countries should also require trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors.

2. All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when, as a trustee, forming a business relationship or carrying out an occasional transaction above the threshold. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust[50]; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

3. Countries are encouraged to ensure that other relevant authorities, persons and entities hold information on all trusts with which they have a relationship. Potential sources of information on trusts, trustees, and trust assets are:

   (a) Registries (e.g. a central registry of trusts or trust assets), or asset registries for land, property, vehicles, shares or other assets.

   (b) Other competent authorities that hold information on trusts and trustees (e.g. tax authorities which collect information on assets and income relating to trusts).

   (c) Other agents and service providers to the trust, including investment advisors or managers, lawyers, or trust and company service providers.

4. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the information held by trustees and other parties, in particular information held by financial institutions and DNFBPs on: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

5. Professional trustees should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust ceases. Countries are encouraged to require non-professional trustees and the other authorities, persons and entities mentioned in paragraph 3 above to maintain the information for at least five years.

---

50 Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

6. Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and be as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.

7. Countries should consider measures to facilitate access to any information on trusts that is held by the other authorities, persons and entities referred to in paragraph 3, by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

8. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 2 and 6 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

Other Legal Arrangements

9. As regards other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified above in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities.

International Cooperation

10. Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.

Liability and Sanctions

11. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretive Note; and that trustees are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 2, 6 and (where applicable) 5; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.[51] Countries should ensure that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to

[51] This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

grant to competent authorities timely access to information regarding the trust referred to in paragraphs 1 and 5.

INTERPRETIVE NOTE TO RECOMMENDATION 26 (REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS)

Risk-based approach to Supervision

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.

2. Adopting a risk-based approach to supervising financial institutions' AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result, supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the money laundering and terrorist financing risks present in a country; and (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group (or groups, when applicable for Core Principles institutions). The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the money laundering and terrorist financing risks, and the policies, internal controls and procedures associated with the institution/group, as identified by the supervisor's assessment of the institution/group's risk profile, and on the money laundering and terrorist financing risks present in the country.

3. The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country's established practices for ongoing supervision. This assessment should not be static: it will change depending on how circumstances develop and how threats evolve.

4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under the RBA to the financial institution/group, and encompass, in an appropriate manner, a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.

5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions, and the degree of discretion allowed to them under the RBA.

Resources of supervisors

6. Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and

autonomy to ensure freedom from undue influence or interference. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 28 (REGULATION AND SUPERVISION OF DNFBPS)

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor or SRB, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring DNFBPs that apply an AML/CFT risk-based approach.

2. Supervisors or SRBs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the money laundering and terrorist financing risks, and taking into consideration the characteristics of the DNFBPs, in particular their diversity and number, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the money laundering and terrorist financing risks: (a) present in the country; and (b) associated with the type of DNFBP and their customers, products and services.

3. Supervisors or SRBs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the money laundering and terrorist financing risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA.

4. Supervisors or SRBs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 29 (FINANCIAL INTELLIGENCE UNITS)

A. GENERAL

1. This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities. Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

B. FUNCTIONS

(a) Receipt

2. The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

(b) Analysis

3. FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and on the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. However, such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing.
- Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns. This information is then also used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

(c) Dissemination

4. The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities. Dedicated, secure and protected channels should be used for the dissemination.

- **Spontaneous dissemination**: The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
- **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU.

C. ACCESS TO INFORMATION

(a) Obtaining Additional Information from Reporting Entities

5. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).

(b) Access to Information from other sources

6. In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

D. INFORMATION SECURITY AND CONFIDENTIALITY

7. Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems.

E. OPERATIONAL INDEPENDENCE

8. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities.

9. An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.

10. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

11. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

F. UNDUE INFLUENCE OR INTERFERENCE

12. The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

G. EGMONT GROUP

13. Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs). The FIU should apply for membership in the Egmont Group.

H. LARGE CASH TRANSACTION REPORTING

14. Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

INTERPRETIVE NOTE TO RECOMMENDATION 30 (RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES)

1. There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation.

2. A 'financial investigation' means an enquiry into the financial affairs related to a criminal activity, with a view to:

   - identifying the extent of criminal networks and/or the scale of criminality;
   - identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and
   - developing evidence which can be used in criminal proceedings.

3. A 'parallel financial investigation' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.

4. Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering and terrorist financing cases to postpone or waive the arrest of suspected persons and/or the seizure of the money, for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

5. Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

6. Anti-corruption enforcement authorities with enforcement powers may be designated to investigate money laundering and terrorist financing offences arising from, or related to, corruption offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

7. The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when countries make use of multi-disciplinary groups in financial investigations.

8. Law enforcement authorities and prosecutorial authorities should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the

staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 32 (CASH COURIERS)

A. OBJECTIVES

1. Recommendation 32 was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (a) detect the physical cross-border transportation of currency and bearer negotiable instruments; (b) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (c) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (d) apply appropriate sanctions for making a false declaration or disclosure; and (e) enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

B. THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

2. Countries may meet their obligations under Recommendation 32 and this Interpretive Note by implementing one of the following types of systems. However, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

Declaration system

3. All persons making a physical cross-border transportation of currency or bearer negotiable instruments (BNIs), which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system: (i) a written declaration system for all travellers; (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above a threshold; and (iii) an oral declaration system. These three systems are described below in their pure form. However, it is not uncommon for countries to opt for a mixed system.

(a) *Written declaration system for all travellers*: In this system, all travellers are required to complete a written declaration before entering the country. This would include questions contained on common or customs declaration forms. In practice, travellers have to make a declaration whether or not they are carrying currency or BNIs (e.g. ticking a “yes” or “no” box).

(b) *Written declaration system for travellers carrying amounts above a threshold:* In this system, all travellers carrying an amount of currency or BNIs above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNIs over the designated threshold.

(c) *Oral declaration system for all travellers:* In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. Usually, this is done at customs entry points by requiring travellers to choose between the "red channel" (goods to declare) and the "green channel" (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

Disclosure system

4. Countries may opt for a system whereby travellers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

C. ADDITIONAL ELEMENTS APPLICABLE TO BOTH SYSTEMS

5. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

(a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and BNIs.

(b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs and their intended use.

(c) Information obtained through the declaration/disclosure process should be available to the FIU, either through a system whereby the FIU is notified about suspicious cross-border transportation incidents, or by making the declaration/disclosure information directly available to the FIU in some other way.

(d) At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

(e) In the following two cases, competent authorities should be able to stop or restrain cash or BNIs for a reasonable time, in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

(f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of

money laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

(g) Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

D. SANCTIONS

6. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or BNIs that is related to terrorist financing, money laundering or predicate offences should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, consistent with Recommendation 4, which would enable the confiscation of such currency or BNIs.

7. Authorities responsible for implementation of Recommendation 32 should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

E. GOLD, PRECIOUS METALS AND PRECIOUS STONES

8. For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action.

Glossary of specific terms used in this Recommendation

False declaration	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is

Glossary of specific terms used in this Recommendation

	asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
Physical cross-border transportation	refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.
Related to terrorist financing or money laundering	when used to describe currency or BNIs, refers to currency or BNIs that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

INTERPRETIVE NOTE TO RECOMMENDATION 38 (MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION)

1. Countries should consider establishing an asset forfeiture fund into which all, or a portion of, confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes. Countries should take such measures as may be necessary to enable them to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions.

2. With regard to requests for cooperation made on the basis of non-conviction based confiscation proceedings, countries need not have the authority to act on the basis of all such requests, but should be able to do so, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.

INTERPRETIVE NOTE TO RECOMMENDATION 40 (OTHER FORMS OF INTERNATIONAL COOPERATION)

A. PRINCIPLES APPLICABLE TO ALL FORMS OF INTERNATIONAL COOPERATION

Obligations on requesting authorities

1. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained.

Unduly restrictive measures

2. Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:

   (a) the request is also considered to involve fiscal matters; and/or

   (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or

   (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

   (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

Safeguards on information exchanged

3. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority.

4. Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry[52], consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of

[52] Information may be disclosed if such disclosure is required to carry out the request for cooperation.

information should take place in a secure way, and through reliable channels or mechanisms. Requested competent authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively.

Power to search for information

5. Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

B. PRINCIPLES APPLICABLE TO SPECIFIC FORMS OF INTERNATIONAL COOPERATION

6. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.

Exchange of information between FIUs

7. FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.

8. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

9. FIUs should have the power to exchange:

   (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and

   (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

Exchange of information between financial supervisors[53]

10. Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

---

53 This refers to financial supervisors which are competent authorities.

11. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group:

    (a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors.

    (b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness.

    (c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

12. Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

13. Any dissemination of information exchanged or use of that information for supervisory and non- supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding.

Exchange of information between law enforcement authorities

14. Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

15. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

16. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or

multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

Exchange of information between non-counterparts

17. Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

18. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS

1. All requirements for financial institutions or DNFBPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).

2. In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.

3. The term "*Enforceable means*" refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).

4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:

   (a) There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:

      (i) if particular measures use the word *shall* or *must*, this should be considered mandatory;

      (ii) if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).

   (b) The document/mechanism must be issued or approved by a competent authority.

   (c) There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:

      (i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

(ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and

(iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.

5. In all cases it should be apparent that financial institutions and DNFBPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

GENERAL GLOSSARY

Terms	Definitions
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Please refer to the IN to Recommendation 16.
Agent	For the purposes of Recommendations 14 and 16, *agent* means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.
Appropriate authorities	Please refer to the IN to Recommendation 8.
Associate NPOs	Please refer to the IN to Recommendation 8.
Batch transfer	Please refer to the IN to Recommendation 16.
Bearer negotiable instruments	*Bearer negotiable instruments (BNIs)* includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
Beneficial owner	*Beneficial owner* refers to the natural person(s) who ultimately[54] owns or controls a customer[55] and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiaries	Please refer to the IN to Recommendation 8.
Beneficiary	The meaning of the term *beneficiary* in the FATF Recommendations depends on the context: ■ In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or

54 Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

55 This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Terms	Definitions
	statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. Please also refer to the Interpretive Notes to Recommendation 16.
Beneficiary Financial Institution	Please refer to the IN to Recommendation 16.
Competent authorities	*Competent authorities* refers to all public authorities[56] with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.
Confiscation	The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or

[56] This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
	forfeited property is determined to have been derived from or intended for use in a violation of the law.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to *country* or *countries* apply equally to territories or jurisdictions.
Cover Payment	Please refer to the IN. to Recommendation 16.
Criminal activity	*Criminal activity* refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Cross-border Wire Transfer	Please refer to the IN to Recommendation 16.
Currency	*Currency* refers to banknotes and coins that are in circulation as a medium of exchange.
Designated categories of offences	*Designated categories of offences* means: ■ participation in an organised criminal group and racketeering; ■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking; ■ illicit trafficking in stolen and other goods;

Terms	Definitions
	■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime; ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos[57] b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses,

[57] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

Terms	Definitions
	nor to professionals working for government agencies, who may already be subject to AML/CFT measures. f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; ■ acting as (or arranging for another person to act as) a nominee shareholder for another person.
Designated person or entity	The term designated person or entity refers to: (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any individual, natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council

Terms	Definitions
	resolution 1718 (2006) and any future successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to resolution 1718 (2006) (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and (v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 2231 (2015) and any future successor resolutions by the Security Council.
Designation	The term *designation* refers to the identification of a person[58], individual or entity that is subject to targeted financial sanctions pursuant to: ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution 1718 (2006) and any future successor resolutions; ■ Security Council resolution 2231 (2015) and any future successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. As far as Security Council resolution 2231 (2015) and any future successor resolutions are concerned, references to "designations" apply equally to "listing".
Domestic Wire Transfer	Please refer to the IN to Recommendation 16.
Enforceable means	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Ex Parte	The term *ex parte* means proceeding without prior notification and participation of the affected party.
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts

58 Natural or legal.

Terms	Definitions
	which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
False declaration	Please refer to the IN to Recommendation 32.
False disclosure	Please refer to the IN to Recommendation 32.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[59] 2. Lending.[60] 3. Financial leasing.[61] 4. Money or value transfer services.[62] 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading.

59 This also captures private banking.

60 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

61 This does not extend to financial leasing arrangements in relation to consumer products.

62 It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

Terms	Definitions
	8. Participation in securities issues and the provision of financial services related to such issues. 9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[63]. 13. Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).
Freeze	In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court. In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.

63 This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Terms	Definitions
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	The term *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.
Funds or other assets	The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.
Identification data	The term *identification data* refers to reliable, independent source documents, data or information.
Intermediary financial institution	Please refer to the IN to Recommendation 16.
International organisations	International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

Terms	Definitions
Law	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Legal arrangements	*Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
Legal persons	*Legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a *money laundering offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.
Non-conviction based confiscation	*Non-conviction based confiscation* means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.
Non-profit organisations	Please refer to the IN to Recommendation 8.
Originator	Please refer to the IN to Recommendation 16.
Ordering financial institution	Please refer to the IN to Recommendation 16.
Payable-through accounts	Please refer to the IN to Recommendation 13.
Physical cross-border transportation	Please refer to the IN. to Recommendation 32.

Terms	Definitions
Politically Exposed Persons (PEPs)	*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Persons who are or have been entrusted with a prominent function by an international organisation* refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Qualifying wire transfers	Please refer to the IN to Recommendation 16.
Reasonable measures	The term *Reasonable Measures* means: appropriate measures which are commensurate with the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	Please refer to the IN. to Recommendation 32.
Required	Please refer to the IN to Recommendation 16.
Risk	All references to *risk* refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent

Terms	Definitions
	authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
Serial Payment	Please refer to the IN. to Recommendation 16.
Settlor	*Settlors* are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
Straight-through processing	Please refer to the IN. to Recommendation 16.
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*" [64]) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

64 Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

Terms	Definitions
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
Terrorist	The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A *terrorist act* includes: (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	*Terrorist financing* is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist financing abuse	Please refer to the IN to Recommendation 8.
Terrorist financing offence	References (except in Recommendation 4) to a *terrorist financing offence* refer not only to the primary offence or offences, but also to ancillary offences.

Terms	Definitions
Terrorist organisation	The term *terrorist organisation* refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term *third parties* includes, but is not limited to, financial institutions and DNFBPs. Please also refer to the IN to Recommendation 17.
Trustee	The terms *trust* and *trustee* should be understood as described in and consistent with Article 2 of the *Hague Convention on the law applicable to trusts and their recognition*[65]. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family).
Unique transaction reference number	Please refer to the IN. to Recommendation 16.
Virtual Asset	A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

65 Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

a) the assets constitute a separate fund and are not a part of the trustee's own estate;

b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;

c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

Terms	Definitions
Virtual Asset Service Providers	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer[66] of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Without delay	The phrase without delay means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

66 In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IN	Interpretive Note
ML	Money Laundering
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-Based Approach
SR.	Special Recommendation
SRB	Self-Regulatory Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
UN	United Nations
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

ANNEX I: FATF GUIDANCE DOCUMENTS

The FATF has published a large body of Guidance and Best Practices papers which can be found at: www.fatf-gafi.org/documents/guidance/.

ANNEX II: INFORMATION ON UPDATES MADE TO THE FATF RECOMMENDATIONS

The following amendments have been made to the FATF Recommendations since the text was adopted in February 2012.

Date	Type of amendments	Sections subject to amendments
Feb 2013	Alignment of the Standards between R.37 and R.40	■ R.37(d) – page 27 Insertion of the reference that DNFBP secrecy or confidentiality laws should not affect the provision of mutual legal assistance, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.
Oct 2015	Revision of the Interpretive Note to R. 5 to address the foreign terrorist fighters threat	■ INR.5 (B.3) – page 37 Insertion of B.3 to incorporate the relevant element of UNSCR 2178 which addresses the threat posed by foreign terrorist fighters. This clarifies that Recommendation 5 requires countries to criminalise financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. Existing B.3-11 became B.4-12.
Jun 2016	Revision of R. 8 and the Interpretive Note to R. 8	■ R.8 and INR.8 – pages 13 and 54-59 Revision of the standard on non-profit organisation (NPO) to clarify the subset of NPOs which should be made subject to supervision and monitoring. This brings INR.8 into line with the FATF Typologies Report on Risk of Terrorist Abuse of NPOs (June 2014) and the FATF Best Practices on Combatting the Abuse of NPOs (June 2015) which clarify that not all NPOs are high risk and intended to be addressed by R.8, and better align the implementation of R.8/INR.8 with the risk-based approach.

Date	Type of amendments	Sections subject to amendments
Oct 2016	Revision of the Interpretive Note to R. 5 and the Glossary definition of 'Funds or other assets'	■ INR. 5 and Glossary – pages 37 and 121 Revision of the INR.5 to replace "*funds*" with "*funds or other assets*" throughout INR.5, in order to have the same scope as R.6. Revision of the Glossary definition of "*funds or other assets*" by adding references to oil and other natural resources, and to other assets which may potentially be used to obtain funds.
Jun 2017	Revision of the Interpretive Note to R.7 and the Glossary definitions of "Designated person or entity", "Designation" and "Without delay"	■ INR. 7 and Glossary – pages 45-51, 114-115 and 123 Revision of the INR.7 and consequential revisions of the Glossary definitions of *"Designated person or entity"*, *"Designation"* and *"Without delay"* to bring the text in line with the requirements of recent United Nations Security Council Resolutions and to clarify the implementation of targeted financial sanctions relating to proliferation financing.
Nov 2017	Revision of the Interpretive Note to Recommendation 18	■ INR.18 – page 77 Revision of INR.18 to clarify the requirements on sharing of information related to unusual or suspicious transactions within financial groups. It also includes providing this information to branches and subsidiaries when necessary for AML/CFT risk management.
Nov 2017	Revision of Recommendation 21	■ R. 21 – page 17 Revision of R. 21 to clarify the interaction of these requirements with tipping-off provisions.
Feb 2018	Revision of Recommendation 2	■ R. 2 – page 9 Revision of R. 2 to ensure compatibility of AML/CFT requirements and data protection and privacy rules, and to promote domestic inter-agency information sharing among competent authorities.

Date	Type of amendments	Sections subject to amendments
Oct 2018	Revision of Recommendation 15 and addition of two new definitions in the Glossary	■ R. 15 and Glossary – pages 15 and 126-127 Revision of R.15 and addition of new definitions "virtual asset" and "virtual asset service provider" in order to clarify how AML/CFT requirements apply in the context of virtual assets.
June 2019	Addition of Interpretive Note to R. 15	■ INR. 15 – page 70-71 Insertion of a new interpretive note that sets out the application of the FATF Standards to virtual asset activities and service providers.

www.fatf-gafi.org

Appendix F:

FATF, *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* (Paris: FATF, 2019).

Methodology

FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS

Updated October 2019

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2013-2019), *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*, updated October 2019, FATF, Paris, France, http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

METHODOLOGY

FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS

ADOPTED IN FEBRUARY 2013

Updated October 2019

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
CFT	Countering the financing of terrorism
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IO	Immediate Outcome
IN	Interpretive Note
ML	Money Laundering
MOU	Memorandum of Understanding
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-Based Approach
SRB	Self-Regulating Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
TF	Terrorist Financing
UN	United Nations
UNSCR	United Nations Security Council Resolutions
VASP	Virtual Asset Service Provider
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

INTRODUCTION

1. This document provides the basis for undertaking assessments of technical compliance with the revised FATF Recommendations, adopted in February 2012, and for reviewing the level of effectiveness of a country's Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) system. It consists of three sections. This first section is an introduction, giving an overview of the assessment Methodology[1], its background, and how it will be used in evaluations/assessments. The second section sets out the criteria for assessing technical compliance with each of the FATF Recommendations. The third section sets out the outcomes, indicators, data and other factors used to assess the effectiveness of the implementation of the FATF Recommendations. The processes and procedures for Mutual Evaluations are set out in a separate document.

2. For its 4th round of mutual evaluations, the FATF has adopted complementary approaches for assessing technical compliance with the FATF Recommendations, and for assessing whether and how the AML/CFT system is effective. Therefore, the Methodology comprises two components:

- The technical compliance assessment addresses the specific requirements of the FATF Recommendations, principally as they relate to the relevant legal and institutional framework of the country, and the powers and procedures of the competent authorities. These represent the fundamental building blocks of an AML/CFT system.
- The effectiveness assessment differs fundamentally from the assessment of technical compliance. It seeks to assess the adequacy of the implementation of the FATF Recommendations, and identifies the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system. The focus of the effectiveness assessment is therefore on the extent to which the legal and institutional framework is producing the expected results.

3. Together, the assessments of both technical compliance and effectiveness will present an integrated analysis of the extent to which the country is compliant with the FATF Standards and how successful it is in maintaining a strong AML/CFT system, as required by the FATF Recommendations.

4. This Methodology is designed to assist assessors when they are conducting an assessment of a country's compliance with the international AML/CFT standards. It reflects the requirements set out in the FATF Recommendations and Interpretive Notes, which constitute the international standard to combat money laundering and the financing of terrorism and proliferation, but does not amend or override them. It will assist assessors in identifying the systems and mechanisms developed by countries with diverse legal, regulatory and financial frameworks in order to implement effective AML/CFT systems; and is also useful for countries that are reviewing their own systems, including in

[1] The terms "assessment", "evaluation" and their derivatives are used throughout this document, and refer to both mutual evaluations undertaken by the FATF and FSRBs and third-party assessments (*i.e.* assessments undertaken by the IMF and World Bank).

relation to technical assistance needs. This Methodology is also informed by the experience of the FATF, the FATF-style regional bodies (FSRBs), the International Monetary Fund and the World Bank in conducting assessments of compliance with earlier versions of the FATF Recommendations.

RISK AND CONTEXT

5. The starting point for every assessment is the assessors' initial understanding of the country's risks and context, in the widest sense, and elements which contribute to them. This includes:

- the nature and extent of the money laundering and terrorist financing risks ;
- the circumstances of the country, which affect the *materiality* of different Recommendations (*e.g.,* the makeup of its economy and its financial sector);
- *structural elements* which underpin the AML/CFT system; and
- *other contextual factors* which could influence the way AML/CFT measures are implemented and how effective they are.

6. The ML/TF *risks* are critically relevant to evaluating technical compliance with Recommendation 1 and the risk-based elements of other Recommendations, and to assess effectiveness. Assessors should consider the nature and extent of the money laundering and terrorist financing risk factors to the country at the outset of the assessment, and throughout the assessment process. Relevant factors can include the level and type of proceeds-generating crime in the country; the terrorist groups active or raising funds in the country; exposure to cross-border flows of criminal or illicit assets.

7. Assessors should use the country's own assessment(s) of its risks as an initial basis for understanding the risks, but should not uncritically accept a country's risk assessment as correct, and need not follow all its conclusions. Assessors should also note the guidance in paragraph 16, below on how to evaluate risk assessments in the context of Recommendation 1 and Immediate Outcome 1. There may be cases where assessors cannot conclude that the country's assessment is reasonable, or where the country's assessment is insufficient or non-existent. In such situations, they should consult closely with the national authorities to try to reach a common understanding of what are the key risks within the jurisdiction. If there is no agreement, or if they cannot conclude that the country's assessment is reasonable, then assessors should clearly explain any differences of understanding, and their reasoning on these, in the Mutual Evaluation Report (MER); and should use their understanding of the risks as a basis for assessing the other risk-based elements (e.g. risk-based supervision).

8. Assessors should also consider issues of *materiality*, including, for example, the relative importance of different parts of the financial sector and different DNFBPs; the size, integration and make-up of the financial sector; the relative importance of different types of financial products or institutions; the amount of business which is domestic or cross-border; the extent to which the economy is cash-based; and estimates of the size of the informal sector and/or shadow economy. Assessors should also be aware of population size, the country's level of development, geographical factors, and trading or cultural links. Assessors should consider the relative importance of different sectors and issues in the assessment of both technical compliance and of effectiveness. The most important and relevant issues to the country should be given more weight when determining ratings

for technical compliance, and more attention should be given to the most important areas when assessing effectiveness, as set out below.

9. An effective AML/CFT system normally requires certain *structural elements* to be in place, for example: political stability; a high-level commitment to address AML/CFT issues; stable institutions with accountability, integrity, and transparency; the rule of law; and a capable, independent and efficient judicial system. The lack of such structural elements, or significant weaknesses and shortcomings in the general framework, may significantly hinder the implementation of an effective AML/CFT framework; and, where assessors identify a lack of compliance or effectiveness, missing structural elements may be a reason for this and should be identified in the MER, where relevant.

10. *Other contextual factors* that might significantly influence the effectiveness of a country's AML/CFT measures include the maturity and sophistication of the regulatory and supervisory regime in the country; the level of corruption and the impact of measures to combat corruption; or the level of financial exclusion. Such factors may affect the ML/FT risks and increase or reduce the effectiveness of AML/CFT measures.

11. Assessors should consider the contextual factors above, including the risks, issues of materiality, structural elements, and other contextual factors, to reach a general understanding of the context in which the country's AML/CFT system operates. These factors may influence which issues assessors consider to be material or higher-risk, and consequently will help assessors determine where to focus their attention in the course of an assessment. Some particularly relevant contextual factors are noted in the context of individual immediate outcomes addressed in the effectiveness component of this Methodology. Assessors should be cautious regarding the information used when considering how these risk and contextual factors might affect a country's evaluation, particularly in cases where they materially affect the conclusions. Assessors should take the country's views into account, but should review them critically, and should also refer to other credible or reliable sources of information (e.g. from international institutions or major authoritative publications), preferably using multiple sources. Based on these elements the assessors should make their own judgement of the context in which the country's AML/CFT system operates, and should make this analysis clear and explicit in the MER.

12. Risk, materiality, and structural or contextual factors may in some cases explain why a country is compliant or non-compliant, or why a country's level of effectiveness is higher or lower than might be expected, on the basis of the country's level of technical compliance. These factors may be an important part of the explanation why the country is performing well or poorly, and an important element of assessors' recommendations about how effectiveness can be improved. Ratings of both technical compliance and effectiveness are judged on a universal standard applied to all countries. An unfavourable context (*e.g.,* where there are missing structural elements), may undermine compliance and effectiveness. However, risks and materiality, and structural or other contextual factors should not be an excuse for poor or uneven implementation of the FATF standards. Assessors should make clear in the MER which factors they have taken into account; why and how they have done so, and the information sources used when considering them.

GENERAL INTERPRETATION AND GUIDANCE

13. A full set of definitions from the FATF Recommendations are included in the Glossary which accompanies the Recommendations. Assessors should also take note of the following guidance on other points of general interpretation, which is important to ensure consistency of approach.

14. **Financial Institutions** –Assessors should have a thorough understanding of the types of entities that engage in the financial activities referred to in the glossary definition of *financial institutions*. It is important to note that such activities may be undertaken by institutions with different generic names (*e.g.,* "bank") in different countries, and that assessors should focus on the activity, not the names attached to the institutions.

15. **VASPs and virtual assets** - Assessors should also have a thorough understanding of the financial institutions, DNFBPs and VASPs that engage in covered activities under the Glossary definition of *virtual asset service provider*. In particular, assessors should note that the requirements of the FATF Standards relating to virtual assets and associated providers are applied by Recommendation 15 ("New Technologies"). INR.15 explicitly confirms that the FATF Definitions of *property, proceeds, funds, funds or other assets* or *other corresponding value* in the Glossary include Virtual Assets. Assessors should bear this in mind when assessing any Recommendations (for technical compliance) or related Immediate Outcomes (for effectiveness) using those terms.[2] See the Note to Assessors in R.15 for more detailed guidance.

16. **Evaluating the country's Assessment of risk** – Assessors are not expected to conduct an independent risk assessment of their own when assessing Recommendation1 and Immediate Outcome 1, but on the other hand should not necessarily accept a country's risk assessment as correct. In reviewing the country's risk assessment, assessors should consider the rigour of the processes and procedures employed; and the internal consistency of the assessment (*i.e.* whether the conclusions are reasonable given the information and analysis used). Assessors should focus on high-level issues, not fine details, and should take a common-sense approach to whether the results are reasonable. Where relevant and appropriate, assessors should also consider other credible or reliable sources of information on the country's risks, in order to identify whether there might be any material differences that should be explored further. Where the assessment team considers the country's assessment of the risks to be reasonable the risk-based elements of the Methodology could be considered on the basis of it.

17. When assessing Recommendation 1, assessors should concentrate their analysis on the following elements: (1) processes and mechanisms in place to produce and coordinate the risk assessment(s); (2) the reasonableness of the risk assessment(s); and, (3) the alignment of risk-based measures with the risks identified (*e.g.,* exemptions, higher or lower risks situations).

---

[2] The terms property, proceeds, funds, funds or other assets and/or corresponding value are used in R.3 (criteria 3.4 and 3.5), R.4 (criteria 4.1, 4.2 and 4.4), R.5 (criteria 5.2, 5.3 and 5.4), R.6 (criteria 6.5, 6.6 and 6.7), R.7 (criteria 7.2, 7.4 and 7.5), R.8 (criteria 8.1 and 8.5), R.10 (criteria 10.7), R.12 (criterion 12.1), R.20 (criterion 20.1), R.29 (criterion 29.4), R.30 (criteria 30.2, 30.3 and 30.5), R.33 (criterion 33.1), R.38 (criteria 38.1, 38.3 and 38.4) and R.40 (criterion 40.17). The words virtual assets need not appear or be explicitly included in legislation referring or defining those terms, provided that there is nothing on the face of the legislation or in case law that would preclude virtual assets from falling within the definition of these terms.

18. When assessing Immediate Outcome 1, assessors, based on their views of the reasonableness of the assessment(s) of risks, should focus on how well the competent authorities use their understanding of the risks in practice to inform policy development and activities to mitigate the risks.

19. **Risk-based requirements** - For each Recommendation where financial institutions and Designated Non-Financial Businesses or Professions (DNFBPs) should be required to take certain actions, assessors should normally assess compliance on the basis that all financial institutions and DNFBPs should have to meet all the specified requirements. However, an important consideration underlying the FATF Recommendations is the degree of risk of money laundering or terrorist financing for particular types of institutions, businesses or professions, or for particular customers, products, transactions, or countries. A country may, therefore, take risk into account in the application of the Recommendations (*e.g.,* in the application of simplified measures), and assessors will need to take the risks, and the flexibility allowed by the risk-based approach, into account when determining whether there are deficiencies in a country's preventive measures, and their importance. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.

20. **Exemptions for low-risk situations** – Where there is a low risk of money laundering and terrorist financing, countries may decide not to apply some of the Recommendations requiring financial institutions and DNFBPs to take certain actions. In such cases, countries should provide assessors with the evidence and analysis which was the basis for the decision not to apply the Recommendations.

21. **Requirements for financial institutions, DNFBPs, VASPs and countries** - The FATF Recommendations state that financial institutions, DNFBPs and VASPs "*should*" or "*should be required to*" take certain actions, or that countries "*should ensure*" that certain actions are taken by financial institutions, DNFBPs, VASPs or other entities or persons. In order to use one consistent phrase, the relevant criteria in this Methodology use the phrase "*Financial institutions (DNFBPs and VASPs) should be required*".

22. **Law or enforceable means** – The note on the *Legal basis of requirements on financial institutions, DNFBPs and VASPs* (at the end of the Interpretive Notes to the FATF Recommendations) sets out the required legal basis for enacting the relevant requirements. Assessors should consider whether the mechanisms used to implement a given requirement qualify as an *enforceable means* on the basis set out in that note. Assessors should be aware that Recommendations 10, 11, and 20 contain requirements which must be set out in law, while other requirements may be set out in either law or enforceable means. It is possible that types of documents or measures which are not considered to be enforceable means may nevertheless help contribute to effectiveness, and may, therefore, be considered in the context of effectiveness analysis, without counting towards meeting requirements of technical compliance (*e.g.,* voluntary codes of conduct issued by private sector bodies or non-binding guidance by a supervisory authority).

23. **Assessment for DNFBPs** – Under Recommendations 22, 23 and 28 (and specific elements of Recommendations 6 and 7), DNFBPs and the relevant supervisory (or self-regulatory) bodies are required to take certain actions. Technical compliance with these requirements should only be

assessed under these specific Recommendations and should not be carried forward into other Recommendations relating to financial institutions. However, the assessment of effectiveness should take account of both financial institutions and DNFBPs when examining the relevant outcomes.

24. **Financing of Proliferation** – The requirements of the FATF Standard relating to the financing of proliferation are limited to Recommendation 7 ("Targeted Financial Sanctions"), Recommendation 15 ("New Technologies") and Recommendation 2 ("National Co-operation and Co-ordination"). In the context of the effectiveness assessment, all requirements relating to the financing of proliferation are included within Outcome 11, except those on national co-operation and co-ordination, which are included in Immediate Outcome 1. Issues relating to the financing of proliferation should be considered in those places only, and not in other parts of the assessment.

25. **National, supra-national and sub-national measures** - In some countries, AML/CFT issues are addressed not just at the level of the national government, but also at state/province or local levels. When assessments are being conducted, appropriate steps should be taken to ensure that AML/CFT measures at the state/provincial level are also adequately considered. Equally, assessors should take into account and refer to supra-national laws or regulations that apply to a country. Annex I sets out the specific Recommendations that may be assessed on a supra-national basis.

26. **Financial Supervision** – Laws and enforceable means that impose preventive AML/CFT requirements upon the banking, insurance, and securities sectors should be implemented and enforced through the supervisory process. In these sectors, the relevant core supervisory principles issued by the Basel Committee, IAIS, and IOSCO should also be adhered to. For certain issues, these supervisory principles will overlap with or be complementary to the requirements set out in the FATF standards. Assessors should be aware of, and have regard to, any assessments or findings made with respect to the Core Principles, or to other relevant principles or standards issued by the supervisory standard-setting bodies. For other types of financial institutions, it will vary from country to country as to whether these laws and obligations are implemented and enforced through a regulatory or supervisory framework, or by other means.

27. **Sanctions** – Several Recommendations require countries to have "*effective, proportionate, and dissuasive sanctions*" for failure to comply with AML/CFT requirements. Different elements of these requirements are assessed in the context of technical compliance and of effectiveness. In the technical compliance assessment, assessors should consider whether the country's framework of laws and enforceable means includes a sufficient range of sanctions that they can be applied *proportionately* to greater or lesser breaches of the requirements[3]. In the effectiveness assessment, assessors should consider whether the sanctions applied in practice are *effective* at ensuring future compliance by the sanctioned institution; and *dissuasive* of non-compliance by others.

28. **International Co-operation** – In this Methodology, international co-operation is assessed in specific Recommendations and Immediate Outcomes (principally Recommendations 36-40 and

[3] Examples of types of sanctions include: written warnings; orders to comply with specific instructions (possibly accompanied with daily fines for non-compliance); ordering regular reports from the institution on the measures it is taking; fines for non-compliance; barring individuals from employment within that sector; replacing or restricting the powers of managers, directors, and controlling owners; imposing conservatorship or suspension or withdrawal of the license; or criminal penalties where permitted.

Immediate Outcome 2). Assessors should also be aware of the impact that a country's ability and willingness to engage in international co-operation may have on other Recommendations and Immediate Outcomes (*e.g.,* on the investigation of crimes with a cross-border element or the supervision of international groups), and set out clearly any instances where compliance or effectiveness is positively or negatively affected by international co-operation.

29. **Draft legislation and proposals** – Assessors should only take into account relevant laws, regulations or other AML/CFT measures that are in force and effect by the end of the on-site visit to the country. Where bills or other specific proposals to amend the system are made available to assessors, these may be referred to in the report, but should not be taken into account in the conclusions of the assessment or for ratings purposes.

30. **FATF Guidance** - assessors may also consider FATF Guidance as background information on how countries can implement specific requirements. A full list of FATF Guidance is included as an annex to this document. Such guidance may help assessors understand the practicalities of implementing the FATF Recommendations, but the application of the guidance should not form part of the assessment.

TECHNICAL COMPLIANCE

31. The technical compliance component of the Methodology refers to the implementation of the specific requirements of the FATF Recommendations, including the framework of laws and enforceable means; and the existence, powers and procedures of competent authorities. For the most part, it does not include the specific requirements of the standards that relate principally to effectiveness. These are assessed separately, through the effectiveness component of the Methodology.

32. The FATF Recommendations, being the recognised international standards, are applicable to all countries. However, assessors should be aware that the legislative, institutional and supervisory framework for AML/CFT may differ from one country to the next. Provided the FATF Recommendations are complied with, countries are entitled to implement the FATF Standards[4] in a manner consistent with their national legislative and institutional systems, even though the methods by which compliance is achieved may differ. In this regard, assessors should be aware of the risks, and the structural or contextual factors for the country.

33. The technical compliance component of the Methodology sets out the specific requirements of each Recommendation as a list of criteria, which represent those elements that should be present in order to demonstrate full compliance with the mandatory elements of the Recommendations. Criteria to be assessed are numbered sequentially for each Recommendation, but the sequence of criteria does not represent any priority or order of importance. In some cases, elaboration (indented below the criteria) is provided in order to assist in identifying important aspects of the assessment of the criteria. For criteria with such elaboration, assessors should review whether each of the elements is present, in order to judge whether the criterion as a whole is met.

COMPLIANCE RATINGS

34. For each Recommendation assessors should reach a conclusion about the extent to which a country complies (or not) with the standard. There are four possible levels of compliance: compliant, largely compliant, partially compliant, and non-compliant. In exceptional circumstances, a Recommendation may also be rated as not applicable. These ratings are based only on the criteria specified in the technical compliance assessment, and are as follows:

[4] The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

Technical compliance ratings		
Compliant	C	There are no shortcomings.
Largely compliant	LC	There are only minor shortcomings.
Partially compliant	PC	There are moderate shortcomings.
Non-compliant	NC	There are major shortcomings.
Not applicable	NA	A requirement does not apply, due to the structural, legal or institutional features of a country.
When deciding on the level of shortcomings for any Recommendation, assessors should consider, having regard to the country context, the number and the relative importance of the criteria met or not met.		

35. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT system is compliant with the Recommendations. In determining the level of compliance for each Recommendation, the assessor should not only assess whether laws and enforceable means are compliant with the FATF Recommendations, but should also assess whether the institutional framework is in place.

36. **Weighting** – The individual criteria used to assess each Recommendation do not all have equal importance, and the number of criteria met is not always an indication of the overall level of compliance with each Recommendation. When deciding on the rating for each Recommendation, assessors should consider the relative importance of the criteria in the context of the country. Assessors should consider how significant any deficiencies are given the country's risk profile and other structural and contextual information (*e.g.,* for a higher risk area or a large part of the financial sector). In some cases a single deficiency may be sufficiently important to justify an NC rating, even if other criteria are met. Conversely a deficiency in relation to a low risk or little used types of financial activity may have only a minor effect on the overall rating for a Recommendation.

37. **Overlaps between Recommendations** – In many cases the same underlying deficiency will have a cascading effect on the assessment of several different Recommendations. For example: a deficient risk assessment could undermine risk-based measures throughout the AML/CFT system; or a failure to apply AML/CFT regulations to a particular type of financial institution or DNFBP could affect the assessment of all Recommendations which apply to financial institutions or DNFBPs. When considering ratings in such cases, assessors should reflect the deficiency in the factors underlying the rating for each applicable Recommendation, and, if appropriate, mark the rating accordingly. They should also clearly indicate in the MER that the same underlying cause is involved in all relevant Recommendations.

38. **Comparison with previous ratings** - Due to the revision and consolidation of the FATF Recommendations and Special Recommendations in 2012, and the introduction of separate

assessments for technical compliance and effectiveness, the ratings given under this Methodology will not be directly comparable with ratings given under the 2004 Methodology.

EFFECTIVENESS

39. The assessment of the effectiveness of a country's AML/CFT system is equally as important as the assessment of technical compliance with the FATF standards. Assessing effectiveness is intended to: (a) improve the FATF's focus on outcomes; (b) identify the extent to which the national AML/CFT system is achieving the objectives of the FATF standards, and identify any systemic weaknesses; and (c) enable countries to prioritise measures to improve their system. For the purposes of this Methodology, effectiveness is defined as "*The extent to which the defined outcomes are achieved*".

40. In the AML/CFT context, effectiveness is the extent to which financial systems and economies mitigate the risks and threats of money laundering, and financing of terrorism and proliferation. This could be in relation to the intended result of a given (a) policy, law, or enforceable means; (b) programme of law enforcement, supervision, or intelligence activity; or (c) implementation of a specific set of measures to mitigate the money laundering and financing of terrorism risks, and combat the financing of proliferation.

41. The goal of an assessment of effectiveness is to provide an appreciation of the whole of the country's AML/CFT system and how well it works. Assessing effectiveness is based on a fundamentally different approach to assessing technical compliance with the Recommendations. It does not involve checking whether specific requirements are met, or that all elements of a given Recommendation are in place. Instead, it requires a judgement as to whether, or to what extent defined outcomes are being achieved, *i.e.* whether the key objectives of an AML/CFT system, in line with the FATF Standards, are being effectively met in practice The assessment process is reliant on the judgement of assessors, who will work in consultation with the assessed country.

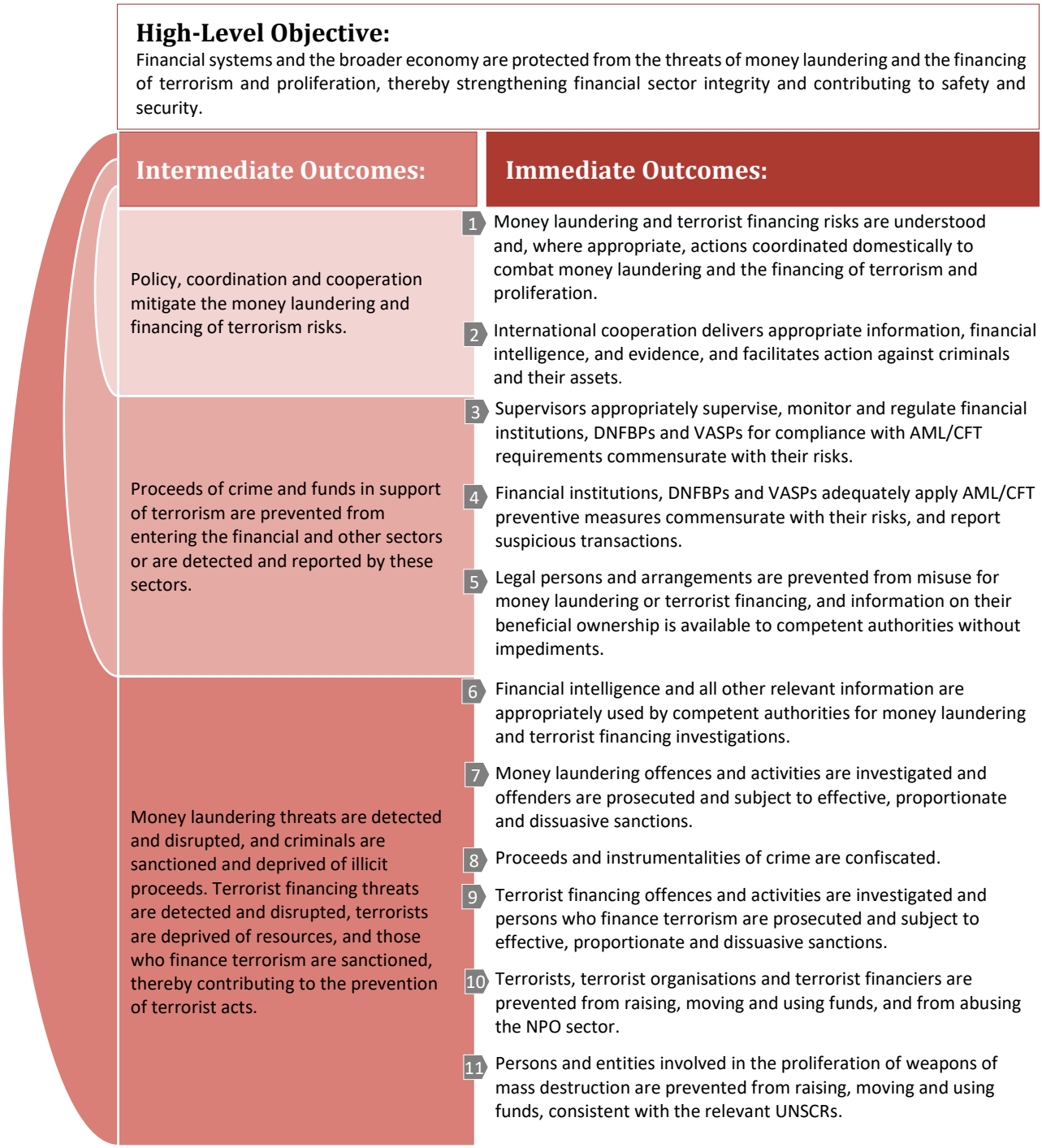
42. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT system is effective. If the evidence is not made available, assessors can only conclude that the system is not effective.

THE FRAMEWORK FOR ASSESSING EFFECTIVENESS

43. For its assessment of effectiveness, the FATF has adopted an approach focusing on a hierarchy of defined outcomes. At the highest level, the objective in implementing AML/CFT measures is that "*Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security*". In order to give the right balance between an overall understanding of the effectiveness of a country's AML/CFT system, and a detailed appreciation of how well its component parts are operating, the FATF assesses effectiveness primarily on the basis of *eleven Immediate Outcomes*. Each of these represents one of the key goals which an effective AML/CFT system should achieve, and they feed into three Intermediate Outcomes which represent the major thematic goals of AML/CFT measures. This approach does not seek to assess directly the effectiveness with which a country is implementing individual Recommendations; or the performance of specific organisations, or institutions. Assessors are not expected to evaluate directly the High-Level Objective

or Intermediate Outcomes, though these could be relevant when preparing the written MER and summarising the country's overall effectiveness in general terms.

44. The relation between the High-Level Objective, the Intermediate Outcomes, and the Immediate Outcomes, is set out in the diagram below:



SCOPING

45. Assessors must assess all eleven of the Immediate Outcomes. However, prior to the on-site visit, assessors should conduct a scoping exercise, in consultation with the assessed country, which should take account of the risks and other factors set out in paragraphs 5 to 10 above. Assessors should, in consultation with the assessed country, identify the higher risk issues, which should be examined in more detail in the course of the assessment and reflected in the final report. They should also seek to identify areas of lower/low risk, which may not need to be examined in the same level of detail. As the assessment continues, assessors should continue to engage the country and review their scoping based on their initial findings about effectiveness, with a view to focusing their attention on the areas where there is greatest scope to improve effectiveness in addressing the key ML/TF risks.

LINKS TO TECHNICAL COMPLIANCE

46. The country's level of technical compliance contributes to the assessment of effectiveness. Assessors should consider the level of technical compliance as part of their scoping exercise. The assessment of technical compliance reviews whether the legal and institutional foundations of an effective AML/CFT system are present. It is unlikely that a country that is assessed to have a low level of compliance with the technical aspects of the FATF Recommendations will have an effective AML/CFT system (though it cannot be taken for granted that a technically compliant country will also be effective). In many cases, the main reason for poor effectiveness will be serious deficiencies in implementing the technical elements of the Recommendations.

47. In the course of assessing effectiveness, assessors should also consider the impact of technical compliance with the relevant Recommendations when explaining why the country is (or is not) effective and making recommendations to improve effectiveness. There may in exceptional circumstances be situations in which assessors conclude that there is a low level of technical compliance but nevertheless a certain level of effectiveness (*e.g.,* as a result of specific country circumstances, including low risks or other structural, material or contextual factors; particularities of the country's laws and institutions; or if the country applies compensatory AML/CFT measures which are not required by the FATF Recommendations). Assessors should pay particular attention to such cases in the MER, and must fully justify their decision, explaining in detail the basis and the specific reasons for their conclusions on effectiveness, despite lower levels of technical compliance.

USING THE EFFECTIVENESS METHODOLOGY

48. An assessment of effectiveness should consider each of the eleven Immediate Outcomes individually, but does not directly focus on the Intermediate or High-Level Outcomes. For each of the Immediate Outcomes, there are two overarching questions which assessors should try to answer:

- ***To what extent is the outcome being achieved?*** Assessors should assess whether the country is effective in relation to that outcome (*i.e.* whether the country is achieving the results expected of a well-performing AML/CFT system). They should base their conclusions principally on the *Core Issues*, supported by the *examples of information* and the *examples of specific*

factors; and taking into account the level of technical compliance, and contextual factors.

- ***What can be done to improve effectiveness?*** Assessors should understand the reasons why the country may not have reached a high level of effectiveness and, where possible, make recommendations to improve its ability to achieve the specific outcome. They should base their analysis and recommendations on their consideration of the *core issues* and on the *examples of specific factors that could support the conclusions on core issues*, including activities, processes, resources and infrastructure. They should also consider the effect of technical deficiencies on effectiveness, and the relevance of contextual factors. If assessors are satisfied that the outcome is being achieved to a high degree, they would not need to consider in detail *what can be done to improve effectiveness* (though there may still be value in identifying good practises or potential further improvements, or ongoing efforts needed to sustain a high level of effectiveness).

Characteristics of an Effective System

49. The boxed text at the top of each of the Immediate Outcomes describes the main features and outcomes of an effective system. This sets out the situation in which a country is effective at achieving the outcome, and provides the benchmark for the assessment.

Core Issues to be considered in determining whether the Outcome is being achieved

50. The second section sets out the basis for assessors to judge if, and to what extent, the outcome is being achieved. The *core issues* are the mandatory questions which assessors should seek to answer, in order to get an overview about how effective a country is under each outcome. Assessors' conclusions about how effective a country is should be based on an overview of each outcome, informed by the assessment of the *core issues*.

51. Assessors should examine all the *core issues* listed for each outcome. However, they may vary the degree of detail with which they examine each in order to reflect the degree of risk and materiality associated with that issue in the country. In exceptional circumstances, assessors may also consider additional issues which they consider, in the specific circumstances, to be core to the effectiveness outcome (*e.g.,* alternative measures which reflect the specificities of the country's AML/CFT system, but which are not included in the *core issues* or as additional *information* or *specific factors*). They should make clear when, and why, any additional issues have been used which are considered to be core.

Examples of information that could support the conclusions on Core Issues

52. The *Examples of Information* sets out the types and sources of information which are most relevant to understanding the extent to which the outcome is achieved, including particular data points which assessors might look for when assessing the *core issues*. The supporting information and

other data can test or validate assessors' understanding of the core issues, and can provide a quantitative element to complete the assessors' picture of how well the outcome is achieved.

53. The supporting information and data listed are not exhaustive and not mandatory. The data, statistics, and other material which are available will vary considerably from country to country, and assessors should make use of whatever information the country can provide in order to assist in reaching their judgement.

54. Assessment of effectiveness is not a statistical exercise. Assessors should use data and statistics, as well as other qualitative information, when reaching an informed judgement about how well the outcome is being achieved, but should interpret the available data critically, in the context of the country's circumstances. The focus should not be on raw data (which can be interpreted in a wide variety of ways and even with contradictory conclusions), but on information and analysis which indicates, in the context of the country being assessed, whether the objective is achieved. Assessors should be particularly cautious about using data relating to other countries as a comparison point in judging effectiveness, given the significant differences in country circumstances, AML/CFT systems, and data collection practices. Assessors should also be aware that a high level of outputs does not always contribute positively towards achieving the desired outcome.

Examples of specific factors that could support the conclusions on core issues

55. The *factors* section of the Methodology sets out examples of the elements which are normally involved in delivering each outcome. These are not an exhaustive list of the possible factors, but are provided as an aid to assessors when considering the reasons why a country may (or may not) be achieving a particular outcome (*e.g.,* through a breakdown in one of the factors). In most cases, assessors will need to refer to the *factors* in order to reach a firm conclusion about the extent to which a particular outcome is being achieved. It should be noted that the activities and processes listed in this section do not imply a single mandatory model for organising AML/CFT functions, but only represent the most commonly implemented administrative arrangements, and that the reasons why a country may not be effective are not limited to the factors listed. It should be noted that assessors need to focus on the qualitative aspects of these *factors*, not on the mere underlying process or procedure.

56. Assessors are not required to review all the *factors* in every case. When a country is demonstrably effective in an area, assessors should set out succinctly why this is the case, and highlight any areas of particular good practice, but they do not need to examine every individual factor in this section of the Methodology. There may also be cases in which a country is demonstrably not effective and where the reasons for this are fundamental (*e.g.,* where there are major technical deficiencies). In such cases, there is also no need for assessors to undertake further detailed examination of why the outcome is not being achieved.

57. Assessors should be aware of outcomes which depend on a sequence of different steps, or a *value-chain* to achieve the outcome (*e.g.,* Immediate Outcome 7, which includes investigation, prosecution and sanctioning, in order). In these cases, it is possible that an outcome may not be achieved because of a failure at one stage of the process, even though the other stages are themselves effective.

58. Assessors should also consider contextual factors, which may influence the issues assessors consider to be material or higher risk, and consequently, where they focus their attention. These factors may be an important part of the explanation why the country is performing well or poorly, and an important element of assessors' recommendations about how effectiveness can be improved. However, they should not be an excuse for poor or uneven implementation of the FATF standards.

CROSS-CUTTING ISSUES

59. The Immediate Outcomes are not independent of each other. In many cases an issue considered specifically under one Immediate Outcome will also contribute to the achievement of other outcomes. In particular, the factors assessed under Immediate Outcomes 1 and 2, which consider (a) the country's assessment of risks and implementation of the risk-based approach; and (b) its engagement in international co-operation, may have far-reaching effects on other outcomes (*e.g.,* risk assessment affects the application of risk-based measures under Immediate Outcome 4, and the deployment of competent authorities' resources relative to all outcomes; international co-operation includes seeking co-operation to support domestic ML investigations and confiscation proceedings under Immediate Outcomes 7 and 8). Therefore, assessors should take into consideration how their findings for Immediate Outcomes 1 and 2 may have a positive or negative impact on the level of effectiveness for other Immediate Outcomes. These cross-cutting issues are reflected in the *notes to assessors* under each Immediate Outcome.

CONCLUSIONS ON EFFECTIVENESS

60. For each individual Immediate Outcome, assessors should reach conclusions about the extent to which a country is (or is not) effective. In cases where the country has not reached a high level of effectiveness, assessors should also make recommendations about the reasons why this is the case, and the measures which the country should take to improve its ability to achieve the outcome.

61. ***Effectiveness is assessed in a fundamentally different way to technical compliance***. Assessors' conclusions about the extent to which a country is more or less effective should be based on an overall understanding of the degree to which the country is achieving the outcome. ***The Core Issues should <u>not</u> be considered as a checklist of criteria***, but as a set of questions which help assessors achieve an appropriate understanding of the country's effectiveness for each of the Immediate Outcomes. The core issues are not equally important, and their significance will vary according to the specific situation of each country, taking into account the ML/TF risks and relevant structural factors. Therefore, assessors need to be flexible and to use their judgement and experience when reaching conclusions.

62. Assessors' conclusions should reflect only *whether the outcome is being achieved*. Assessors should set-aside their own preferences about the best way to achieve effectiveness, and should not be unduly influenced by their own national approach. They should also avoid basing their conclusions on the number of problems or deficiencies identified, as it is possible that a country may have several weaknesses which are not material in nature or are offset by strengths in other areas, and is therefore able to achieve a high overall level of effectiveness.

63. ***Assessors' conclusions on the level of effectiveness should be primarily descriptive***. Assessors should set out clearly the extent to which they consider the outcome to be achieved overall, noting any variation, such as particular areas where effectiveness is higher or lower. They should also clearly explain the basis for their judgement, *e.g.,* problems or weaknesses which they believe are responsible for a lack of effectiveness; the *core issues* and the information which they considered to be most significant; the way in which they understood data and other indicators; and the weight they gave to different aspects of the assessment. Assessors should also identify any areas of particular strength or examples of good practice.

64. In order to ensure clear and comparable decisions, assessors should also summarise their conclusion in the form of a rating. For each Immediate Outcome there are four possible ratings for effectiveness, based on the extent to which the *core issues* and *characteristics* are addressed: *High level of effectiveness; Substantial level of effectiveness; Moderate level of effectiveness; and Low level of effectiveness.* These ratings should be decided on the basis of the following:

Effectiveness ratings	
High level of effectiveness	The Immediate Outcome is achieved to a very large extent. Minor improvements needed.
Substantial level of effectiveness	The Immediate Outcome is achieved to a large extent. Moderate improvements needed.
Moderate level of effectiveness	The Immediate Outcome is achieved to some extent. Major improvements needed.
Low level of effectiveness	The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements needed.

RECOMMENDATIONS ON HOW TO IMPROVE THE AML/CFT SYSTEM

65. Assessors' recommendations to a country are a vitally important part of the evaluation. On the basis of their conclusions, assessors should make recommendations of measures that the country should take in order to improve its AML/CFT system, including both the level of effectiveness and the level of technical compliance. The report should prioritise these recommendations for remedial measures, taking into account the country's circumstances and capacity, its level of effectiveness, and any weaknesses and problems identified. Assessors' recommendations should not simply be to address each of the deficiencies or weaknesses identified, but should add value by identifying and prioritising specific measures in order to most effectively mitigate the risks the country faces. This could be on the basis that they offer the greatest and most rapid practical improvements, have the widest-reaching effects, or are easiest to achieve.

66. Assessors should be careful to consider the circumstances and context of the country, and its legal and institutional system when making recommendations, noting that there are several different ways to achieve an effective AML/CFT system, and that their own preferred model may not be appropriate in the context of the country assessed.

67. In order to facilitate the development of an action plan by the assessed country, assessors should clearly indicate in their recommendations where a specific action is required, and where there may be some flexibility about how a given priority objective is to be achieved. Assessors should avoid making unnecessarily rigid recommendations (*e.g.,* on the scheduling of certain measures), so as not to hinder countries efforts to fully adapt the recommendations to fit local circumstances.

68. Even if a country has a high level of effectiveness, this does not imply that there is no further room for improvement. There may also be a need for action in order to sustain a high level of effectiveness in the face of evolving risks. If assessors are able to identify further actions in areas where there is a high degree of effectiveness, then they should also include these in their recommendations.

POINT OF REFERENCE

69. If assessors have any doubts about how to apply this Methodology, or about the interpretation of the FATF Standards, they should consult the FATF Secretariat or the Secretariat of their FSRB.

TECHNICAL COMPLIANCE ASSESSMENT

RECOMMENDATION 1 ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH[5]

OBLIGATIONS AND DECISIONS FOR COUNTRIES

Risk assessment

1.1 Countries[6] should identify and assess the ML/TF risks for the country,

1.2 Countries should designate an authority or mechanism to co-ordinate actions to assess risks.

1.3 Countries should keep the risk assessments up-to-date.

1.4 Countries should have mechanisms to provide information on the results of the risk assessment(s) to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

Risk mitigation

1.5 Based on their understanding of their risks, countries should apply a risk-based approach to allocating resources and implementing measures to prevent or mitigate ML/TF.

1.6 Countries which decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, should demonstrate that:

(a) there is a proven low risk of ML/TF; the exemption occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

(b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is a low risk of ML/TF.

---

5 The requirements in this recommendation should be assessed taking into account the more specific risk based requirements in other Recommendations. Under Recommendation 1 assessors should come to an overall view of risk assessment and risk mitigation by countries and financial institutions/DNFBPs as required in other Recommendations, but should not duplicate the detailed assessments of risk-based measures required under other Recommendations. Assessors are not expected to conduct an in-depth review of the country's assessment(s) of risks. Assessors should focus on the process, mechanism, and information sources adopted by the country, as well as the contextual factors, and should consider the reasonableness of the conclusions of the country's assessment(s) of risks.

6 Where appropriate, ML/TF risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

1.7 Where countries identify higher risks, they should ensure that their AML/CFT regime addresses such risks, including through: (a) requiring financial institutions and DNFBPs to take enhanced measures to manage and mitigate the risks; or (b) requiring financial institutions and DNFBPs to ensure that this information is incorporated into their risk assessments.

1.8 Countries may allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its ML/TF risks[7].

1.9 Supervisors and SRBs should ensure that financial institutions and DNFBPs are implementing their obligations under Recommendation 1[8].

OBLIGATIONS AND DECISIONS FOR FINANCIAL INSTITUTIONS AND DNFBPS

Risk assessment

1.10 Financial institutions and DNFBPs should be required to take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels)[9]. This includes being required to:

(a) document their risk assessments;

(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) keep these assessments up to date; and

(d) have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs.

Risk mitigation

1.11 Financial institutions and DNFBPs should be required to:

(a) have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the country or by the financial institution or DNFBP);

(b) monitor the implementation of those controls and to enhance them if necessary; and

---

7 Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, countries should ensure that all such measures are applied, although the extent of such measures may vary according to the specific level of risk.

8 The requirements in this criterion should be assessed taking into account the findings in relation to Recommendations 26 and 28.

9 The nature and extent of any assessment of ML/TF risks should be appropriate to the nature and size of the business. Competent authorities or SRBs may determine that individual documented risk assessments are not required, provided that the specific risks inherent to the sector are clearly identified and understood, and that individual financial institutions and DNFBPs understand their ML/TF risks.

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

1.12 Countries may only permit financial institutions and DNFBPs to take simplified measures to manage and mitigate risks, if lower risks have been identified, and criteria 1.9 to 1.11 are met. Simplified measures should not be permitted whenever there is a suspicion of ML/TF.

RECOMMENDATION 2 NATIONAL CO-OPERATION AND CO-ORDINATION

2.1 Countries should have national AML/CFT policies which are informed by the risks identified, and are regularly reviewed.

2.2 Countries should designate an authority or have a co-ordination or other mechanism that is responsible for national AML/CFT policies.

2.3 Mechanisms should be in place to enable policy makers, the Financial Intelligence Unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities to co-operate, and where appropriate, co-ordinate and exchange information domestically with each other concerning the development and implementation of AML/CFT policies and activities. Such mechanisms should apply at both policymaking and operational levels.

2.4 Competent authorities should have similar co-operation and, where appropriate, co-ordination mechanisms to combat the financing of proliferation of weapons of mass destruction.

2.5 Countries should have cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).[10]

[10] For purposes of technical compliance, the assessment should be limited to whether there is co-operation and, where appropriate, co-ordination, whether formal or informal, between the relevant authorities.

RECOMMENDATION 3 MONEY LAUNDERING OFFENCE

3.1 ML should be criminalised on the basis of the Vienna Convention and the Palermo Convention (see Article 3(1)(b)&(c) Vienna Convention and Article 6(1) Palermo Convention)[11].

3.2 The predicate offences for ML should cover all serious offences, with a view to including the widest range of predicate offences. At a minimum, predicate offences should include a range of offences in each of the designated categories of offences[12].

3.3 Where countries apply a threshold approach or a combined approach that includes a threshold approach[13], predicate offences should, at a minimum, comprise all offences that:

(a) fall within the category of serious offences under their national law; or

(b) are punishable by a maximum penalty of more than one year's imprisonment; or

(c) are punished by a minimum penalty of more than six months' imprisonment (for countries that have a minimum threshold for offences in their legal system).

3.4 The ML offence should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime.

3.5 When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

3.6 Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically.

3.7 The ML offence should apply to persons who commit the predicate offence, unless this is contrary to fundamental principles of domestic law.

3.8 It should be possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances.

3.9 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of ML.

---

11 Note in particular the physical and material elements of the offence.

12 Recommendation 3 does not require countries to create a separate offence of "participation in an organised criminal group and racketeering". In order to cover this category of "designated offence", it is sufficient if a country meets either of the two options set out in the Palermo Convention, *i.e.* either a separate offence or an offence based on conspiracy.

13 Countries determine the underlying predicate offences for ML by reference to (a) all offences; or (b) to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or (c) to a list of predicate offences; or (d) a combination of these approaches.

3.10 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures are without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

3.11 Unless it is not permitted by fundamental principles of domestic law, there should be appropriate ancillary offences to the ML offence, including: participation in; association with or conspiracy to commit; attempt; aiding and abetting; facilitating; and counselling the commission.

RECOMMENDATION 4 CONFISCATION AND PROVISIONAL MEASURES

4.1 Countries should have measures, including legislative measures, that enable the confiscation of the following, whether held by criminal defendants or by third parties:

(a) property laundered;

(b) proceeds of (including income or other benefits derived from such proceeds), or instrumentalities used or intended for use in, ML or predicate offences;

(c) property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations; or

(d) property of corresponding value.

4.2 Countries should have measures, including legislative measures, that enable their competent authorities to:

(a) identify, trace and evaluate property that is subject to confiscation;

(b) carry out provisional measures, such as freezing or seizing, to prevent any dealing, transfer or disposal of property subject to confiscation[14];

(c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and

(d) take any appropriate investigative measures.

4.3 Laws and other measures should provide protection for the rights of *bona fide* third parties.

4.4 Countries should have mechanisms for managing and, when necessary, disposing of property frozen, seized or confiscated.

[14] Measures should allow the initial application to freeze or seize property subject to confiscation to be made *ex-parte* or without prior notice, unless this is inconsistent with fundamental principles of domestic law.

RECOMMENDATION 5 TERRORIST FINANCING OFFENCE

5.1 Countries should criminalise TF on the basis of the Terrorist Financing Convention[15].

5.2 TF offences should extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts).[16]

5.2bis TF offences should include financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

5.3 TF offences should extend to any funds or other assets whether from a legitimate or illegitimate source.

5.4 TF offences should not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

5.5 It should be possible for the intent and knowledge required to prove the offence to be inferred from objective factual circumstances.

5.6 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of TF.

5.7 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

5.8 It should also be an offence to:

(a) attempt to commit the TF offence;

(b) participate as an accomplice in a TF offence or attempted offence;

(c) organise or direct others to commit a TF offence or attempted offence; and

15 Criminalisation should be consistent with Article 2 of the International Convention for the Suppression of the Financing of Terrorism.

16 Criminalising TF solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with the Recommendation.

(d) contribute to the commission of one or more TF offence(s) or attempted offence(s), by a group of persons acting with a common purpose[17].

5.9 TF offences should be designated as ML predicate offences.

5.10 TF offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

[17] Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a TF offence; or (ii) be made in the knowledge of the intention of the group to commit a TF offence.

RECOMMENDATION 6 TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING

Identifying and designating

6.1 In relation to designations pursuant to United Nations Security Council 1267/1989 (Al Qaida) and 1988 sanctions regimes (Referred to below as "UN Sanctions Regimes"), countries should:

(a) identify a competent authority or a court as having responsibility for proposing persons or entities to the 1267/1989 Committee for designation; and for proposing persons or entities to the 1988 Committee for designation;

(b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in the relevant United Nations Security Council resolutions (UNSCRs);

(c) apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether or not to make a proposal for designation. Such proposals for designations should not be conditional upon the existence of a criminal proceeding;

(d) follow the procedures and (in the case of UN Sanctions Regimes) standard forms for listing, as adopted by the relevant committee (the 1267/1989 Committee or 1988 Committee); and

(e) provide as much relevant information as possible on the proposed name[18]; a statement of case[19] which contains as much detail as possible on the basis for the listing[20]; and (in the case of proposing names to the 1267/1989 Committee), specify whether their status as a designating state may be made known.

6.2 In relation to designations pursuant to UNSCR 1373, countries should:

(a) identify a competent authority or a court as having responsibility for designating persons or entities that meet the specific criteria for designation, as set forth in UNSCR 1373; as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country.

---

18 In particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice

19 This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the relevant committee (the 1267/1989 Committee or 1988 Committee).

20 Including: specific information supporting a determination that the person or entity meets the relevant designation; the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity

(b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in UNSCR 1373[21];

(c) when receiving a request, make a prompt determination of whether they are satisfied, according to applicable (supra-) national principles that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373;

(d) apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether or not to make a designation[22]. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding; and

(e) when requesting another country to give effect to the actions initiated under the freezing mechanisms, provide as much identifying information, and specific information supporting the designation, as possible.

6.3 The competent authority(ies) should have legal authorities and procedures or mechanisms to:

(a) collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation; and

(b) operate *ex parte* against a person or entity who has been identified and whose (proposal for) designation is being considered.

Freezing

6.4 Countries should implement targeted financial sanctions without delay[23].

6.5 Countries should have the legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

---

21 This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to UNSCR 1373 (2001)

22 A country should apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country.

23 For UNSCR 1373, the obligation to take action without delay is triggered by a designation at the (supra-) national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373.

(a) Countries should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

(b) The obligation to freeze should extend to: (i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; (ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as (iv) funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(c) Countries should prohibit their nationals, or[24] any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant UNSCRs.

(d) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(e) Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

(f) Countries should adopt measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

De-listing, unfreezing and providing access to frozen funds or other assets

6.6 Countries should have publicly known procedures to de-list and unfreeze the funds or other assets of persons and entities which do not, or no longer, meet the criteria for designation. These should include:

(a) procedures to submit de-listing requests to the relevant UN sanctions Committee in the case of persons and entities designated pursuant to the UN Sanctions Regimes , in the view of the country, do not or no longer meet the criteria for designation. Such

[24] "or", in this particular case means that countries must both prohibit their own nationals and prohibit any persons/entities in their jurisdiction.

procedures and criteria should be in accordance with procedures adopted by the *1267/1989 Committee* or the *1988 Committee*, as appropriate[25];

(b) legal authorities and procedures or mechanisms to de-list and unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373, that no longer meet the criteria for designation;

(c) with regard to designations pursuant to UNSCR 1373, procedures to allow, upon request, review of the designation decision before a court or other independent competent authority;

(d) with regard to designations pursuant to UNSCR 1988, procedures to facilitate review by the *1988 Committee* in accordance with any applicable guidelines or procedures adopted by the *1988 Committee*, including those of the Focal Point mechanism established under UNSCR 1730;

(e) with respect to designations on the *Al-Qaida Sanctions List*, procedures for informing designated persons and entities of the availability of the *United Nations Office of the Ombudsperson*, pursuant to UNSCRs 1904, 1989, and 2083 to accept de-listing petitions;

(f) publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (*i.e.* a false positive), upon verification that the person or entity involved is not a designated person or entity; and

(g) mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing guidance to financial institutions and other persons or entities, including DNFBPs, that may by holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

6.7 Countries should authorise access to frozen funds or other assets which have been determined to be necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, in accordance with the procedures set out in UNSCR 1452 and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to UNSCR 1373.

[25] The procedures of the *1267/1989 Committee* are set out in UNSCRs 1730; 1735; 1822; 1904; 1989; 2083 and any successor resolutions. The procedures of the *1988 Committee* are set out in UNSCRs 1730; 1735; 1822; 1904; 1988; 2082; and any successor resolutions.

RECOMMENDATION 7 TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION

7.1 Countries should implement targeted financial sanctions without delay to comply with United Nations Security Council Resolutions, adopted under Chapter VII of the Charter of the United Nations, relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.[26].

7.2 Countries should establish the necessary legal authority and identify competent authorities responsible for implementing and enforcing targeted financial sanctions, and should do so in accordance with the following standards and procedures.

(a) Countries should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

(b) The freezing obligation should extend to: (i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; (ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as (iv) funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

(c) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant United Nations Security Council Resolutions.

(d) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs,

26 Recommendation 7 is applicable to all current UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future UNSCRs which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of the FATF Standards to which this Methodology corresponds (June 2017), the UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: UNSCR 1718(2006) on DPRK and its successor resolutions 1874(2009), 2087(2013), 2094(2013), 2270(2016), 2321(2016) and 2356(2017). UNSCR 2231(2015), endorsing the Joint Comprehensive Plan of Action (JCPOA), terminated all provisions of UNSCRs relating to Iran and proliferation financing, including 1737(2006), 1747(2007), 1803(2008) and 1929(2010), but established specific restrictions including targeted financial sanctions. This lifts sanctions as part of a step by step approach with reciprocal commitments endorsed by the Security Council. Implementation day of the JCPOA was on 16 January 2016.

that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(e) Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

(f) Countries should adopt measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 7.

7.3 Countries should adopt measures for monitoring and ensuring compliance by financial institutions and DNFBPs with the relevant laws or enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws or enforceable means should be subject to civil, administrative or criminal sanctions.

7.4 Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities that, in the view of the country, do not or no longer meet the criteria for designation[27]. These should include:

(a) enabling listed persons and entities to petition a request for de-listing at the Focal Point for de-listing established pursuant to UNSCR 1730, or informing designated persons or entities to petition the Focal Point directly;

(b) publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (*i.e.* a false positive), upon verification that the person or entity involved is not a designated person or entity;

(c) authorising access to funds or other assets, where countries have determined that the exemption conditions set out in UNSCRs 1718 and 2231 are met, in accordance with the procedures set out in those resolutions; and

(d) mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

7.5 With regard to contracts, agreements or obligations that arose prior to the date on which accounts became subject to targeted financial sanctions:

(a) countries should permit the addition to the accounts frozen pursuant to UNSCRs 1718 or 2231 of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which

[27] In the case of UNSCR 1718 and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the United Nations Security Council pursuant to UNSCR 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution.

those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen; and

(b) freezing action taken pursuant to UNSCR 1737 and continued by UNSCR 2231, or taken pursuant to UNSCR 2231 should not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that: (i) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in UNSCR 2231 and any future successor resolutions; (ii) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity subject to the measures in paragraph 6 of Annex B to UNSCR 2231; and (iii) the relevant countries have submitted prior notification to the Security Council of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.

RECOMMENDATION 8 NON-PROFIT ORGANISATIONS (NPOS)

Taking a risk-based approach

8.1 Countries should:

(a) Without prejudice to the requirements of Recommendation 1, since not all NPOs are inherently high risk (and some may represent little or no risk at all), identify which subset of organizations fall within the FATF definition[28] of NPO, and use all relevant sources of information, in order to identify the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse[29];

(b) identify the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs;

(c) review the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for terrorism financing support in order to be able to take proportionate and effective actions to address the risks identified; and

(d) periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities to ensure effective implementation of measures.

Sustained outreach concerning terrorist financing issues

8.2 Countries should:

(a) have clear policies to promote accountability, integrity, and public confidence in the administration and management of NPOs;

(b) encourage and undertake outreach and educational programmes to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse;

(c) work with NPOs to develop and refine best practices to address terrorist financing risk and vulnerabilities and thus protect them from terrorist financing abuse; and

---

28 For the purposes of this Recommendation, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

29 For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

(d) encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

Targeted risk-based supervision or monitoring of NPOs

8.3 Countries should take steps to promote effective supervision or monitoring such that they are able to demonstrate that risk based measures apply to NPOs at risk of terrorist financing abuse.[30]

8.4 Appropriate authorities should:

(a) monitor the compliance of NPOs with the requirements of this Recommendation, including the risk-based measures being applied to them under criterion 8.3[31]; and

(b) be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[32]

Effective information gathering and investigation

8.5 Countries should:

(a) ensure effective co-operation, co-ordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs;

(b) have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations;

(c) ensure that full access to information on the administration and management of particular NPOs (including financial and programmatic information) may be obtained during the course of an investigation; and

(d) establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is involved in terrorist financing abuse and/or is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, that

30 Some examples of measures that could be applied to NPOs, in whole or in part, depending on the risks identified are detailed in sub-paragraph 6(b) of INR.8. It is also possible that existing regulatory or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a jurisdiction, although terrorist financing risks to the sector should be periodically re-assessed.

31 In this context, rules and regulations may include rules and standards applied by self-regulatory organisations and accrediting institutions.

32 The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, delicensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

this information is promptly shared with competent authorities, in order to take preventive or investigative action.

Effective capacity to respond to international requests for information about an NPO of concern

8.6 Countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support.

RECOMMENDATION 9 FINANCIAL INSTITUTION SECRECY LAWS

9.1 Financial institution secrecy laws should not inhibit the implementation of the FATF Recommendations[33].

[33] Areas where this may be of particular concern are the ability of competent authorities to access information they require to properly perform their functions in combating ML or FT; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions where this is required by Recommendations 13, 16 or 17.

RECOMMENDATION 10 CUSTOMER DUE DILIGENCE[34] (CDD)

10.1 Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

When CDD is required

10.2 Financial institutions should be required to undertake CDD measures when:

(a) establishing business relations;

(b) carrying out occasional transactions above the applicable designated threshold (USD/EUR 15 000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;

(c) carrying out occasional transactions that are wire transfers in the circumstances covered by Recommendation 16 and its Interpretive Note;

(d) there is a suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or

(e) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Required CDD measures for all customers

10.3 Financial institutions should be required to identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data).

10.4 Financial institutions should be required to verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person.

10.5 Financial institutions should be required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the financial institution is satisfied that it knows who the beneficial owner is.

10.6 Financial institutions should be required to understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.

[34] The principle that financial institutions conduct CDD should be set out in law, though specific requirements may be set out in enforceable means.

10.7 Financial institutions should be required to conduct ongoing due diligence on the business relationship, including:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

Specific CDD measures required for legal persons and legal arrangements

10.8 For customers that are legal persons or legal arrangements, the financial institution should be required to understand the nature of the customer's business and its ownership and control structure.

10.9 For customers that are legal persons or legal arrangements, the financial institution should be required to identify the customer and verify its identity through the following information:

(a) name, legal form and proof of existence;

(b) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and

(c) the address of the registered office and, if different, a principal place of business.

10.10 For customers that are legal persons[35], the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) the identity of the natural person(s) (if any[36]) who ultimately has a controlling ownership interest[37] in a legal person; and

---

35 Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

36 Ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership.

37 A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

(b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and

(c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

10.11 For customers that are legal arrangements, the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries[38], and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

CDD for Beneficiaries of Life Insurance Policies

10.12 In addition to the CDD measures required for the customer and the beneficial owner, financial institutions should be required to conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated:

(a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout;

(c) for both the above cases – the verification of the identity of the beneficiary should occur at the time of the payout.

10.13 Financial institutions should be required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it should be required to take enhanced measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

---

38 For beneficiaries of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

Timing of verification

10.14 Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:

(a) this occurs as soon as reasonably practicable;

(b) this is essential not to interrupt the normal conduct of business; and

(c) the ML/TF risks are effectively managed.

10.15 Financial institutions should be required to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification.

Existing customers

10.16 Financial institutions should be required to apply CDD requirements to existing customers[39] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Risk-Based Approach

10.17 Financial institutions should be required to perform enhanced due diligence where the ML/TF risks are higher.

10.18 Financial institutions may only be permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the financial institution. The simplified measures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

Failure to satisfactorily complete CDD

10.19 Where a financial institution is unable to comply with relevant CDD measures:

(a) it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and

(b) it should be required to consider making a suspicious transaction report (STR) in relation to the customer.

[39] Existing customers as at the date that the new national requirements are brought into force.

CDD and tipping-off

10.20 In cases where financial institutions form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process, and instead should be required to file an STR.

RECOMMENDATION 11 RECORD KEEPING[40]

11.1 Financial institutions should be required to maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction.

11.2 Financial institutions should be required to keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction.

11.3 Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

11.4 Financial institutions should be required to ensure that all CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority.

40 The principle that financial institutions should maintain records on transactions and information obtained through CDD measures should be set out in law.

RECOMMENDATION 12 POLITICALLY EXPOSED PERSONS (PEPS)

12.1 In relation to foreign PEPs, in addition to performing the CDD measures required under Recommendation 10, financial institutions should be required to:

(a) put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;

(b) obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(d) conduct enhanced ongoing monitoring on that relationship.

12.2 In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required under Recommendation10, financial institutions should be required to:

(a) take reasonable measures to determine whether a customer or the beneficial owner is such a person; and

(b) in cases when there is higher risk business relationship with such a person, adopt the measures in criterion 12.1 (b) to (d).

12.3 Financial institutions should be required to apply the relevant requirements of criteria 12.1 and 12.2 to family members or close associates of all types of PEP.

12.4 In relation to life insurance policies, financial institutions should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

RECOMMENDATION 13 CORRESPONDENT BANKING

13.1 In relation to cross-border correspondent banking and other similar relationships, financial institutions should be required to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships; and

(d) clearly understand the respective AML/CFT responsibilities of each institution.

13.2 With respect to "payable-through accounts", financial institutions should be required to satisfy themselves that the respondent bank:

(a) has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank; and

(b) is able to provide relevant CDD information upon request to the correspondent bank.

13.3 Financial institutions should be prohibited from entering into, or continuing, correspondent banking relationships with shell banks. They should be required to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.

RECOMMENDATION 14 MONEY OR VALUE TRANSFER SERVICES (MVTS)

14.1 Natural or legal persons that provide MVTS (MVTS providers) should be required to be licensed or registered[41].

14.2. Countries should take action, with a view to identifying natural or legal persons that carry out MVTS without a licence or registration, and applying proportionate and dissuasive sanctions to them.

14.3 MVTS providers should be subject to monitoring for AML/CFT compliance.

14.4 Agents for MVTS providers should be required to be licensed or registered by a competent authority, or the MVTS provider should be required to maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate.

14.5 MVTS providers that use agents should be required to include them in their AML/CFT programmes and monitor them for compliance with these programmes.

41 Countries need not impose a separate licensing or registration system with respect to licensed or registered financial institutions which are authorised to perform MVTS.

RECOMMENDATION 15 NEW TECHNOLOGIES

Note to Assessors:
For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property", "proceeds", "funds", "funds or other assets", or other "corresponding value". When assessing any Recommendation(s) using these terms[42], the words virtual assets do not have to appear or be explicitly included in legislation referring to or defining those terms.

Assessors should satisfy themselves that the country has demonstrated that nothing in the text of the legislation or in case law precludes virtual assets from falling within the definition of these terms. Where these terms do not cover virtual assets, the deficiency should be noted in the relevant Recommendation(s) that use the term.

Assessors should also satisfy themselves that VASPs may be considered as existing sources of information on beneficial ownership for the purposes of c.24.6(c)(i) and 25.5; and are empowered to obtain relevant information from trustees for the purposes of c.25.3 and 25.4.[43]

Paragraph 1 of INR.15 also requires countries to apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs):

a) Where these are preventive measures under Recommendations 10 to 21 and implementation of TFS in R.6 (sub-criteria 6.5(d) and (e), and 6.6(g)) and R.7 (sub-criteria 7.2(d) and (e), criterion 7.3, and sub-criterion 7.4(d)), their application to VASPs should be assessed under Recommendation 15, as should compliance with relevant aspects of R.1, 26, 27, 34, 35 and 37 to 40.

b) Where these are other relevant measures relating to virtual assets and VASPs under Recommendations 2 to 5, R.6 (sub-criteria 6.5(a) to (c), 6.6(a) to (f), and criterion 6.7), R.7 (sub-criteria 7.2(a) to (c), 7.4(b) and 7.4(c), and criterion 7.5)), R.8 to 9, and R.29 to 33, their application to virtual assets and VASPs should be assessed in those Recommendations (not in R.15).

Assessors should refer to paragraph 15 of the Introduction section of the Methodology for more guidance on how to assess the FATF Standards relating to virtual assets and VASPs.

New technologies

15.1 Countries and financial institutions should identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including

42 The terms property, proceeds, funds, funds or other assets and/or corresponding value are used in R.3 (criteria 3.4 and 3.5), R.4 (criteria 4.1, 4.2 and 4.4), R.5 (criteria 5.2, 5.3 and 5.4), R.6 (criteria 6.5, 6.6 and 6.7), R.7 (criteria 7.2, 7.4 and 7.5), R.8 (criteria 8.1 and 8.5), R.10 (criteria 10.7), R.12 (criterion 12.1), R.20 (criterion 20.1), R.29 (criterion 29.4), R.30 (criteria 30.2, 30.3 and 30.5), R.33 (criterion 33.1), R.38 (criteria 38.1, 38.3 and 38.4) and R.40 (criterion 40.17). See additional guidance in paragraph 15 of the Introduction to the Methodology.

43 Consideration of VASPs in the context of these criteria is meant to ensure availability of beneficial ownership information. Assessors should not consider these criteria to impose obligations on VASPs.

new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

15.2 Financial institutions should be required to:

(a) undertake the risk assessments prior to the launch or use of such products, practices and technologies; and
(b) take appropriate measures to manage and mitigate the risks.

Virtual assets and virtual asset service providers[44]

15.3 In accordance with Recommendation 1, countries should:

(a) identify and assess the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs;

(b) based on their understanding of their risks, apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified; and

(c) require VASPs to take appropriate steps to identify, assess, manage and mitigate their money laundering and terrorist financing risks, as required by criteria 1.10 and 1.11.

15.4 Countries should ensure that:

(a) VASPs are required to be licensed or registered[45] at a minimum[46]:

(i) when the VASP is a legal person, in the jurisdiction(s) where it is created[47]; and

---

44 Note to assessors: Countries that have decided to prohibit virtual assets should only be assessed under criteria 15.1, 15.2, 15.3(a) and 15.3(b), 15.5 and 15.11, as the remaining criteria are not applicable in such cases.

45 A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

46 Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction.

47 References to creating a legal person include incorporation of companies or any other mechanism that is used. To clarify, the requirement in criterion 15.4(a)(i) is that a country must ensure that a VASP created within the country is licenced or registered, but not that any VASP licenced or registered in the country is also registered in any third country where it was created.

(ii) when the VASP is a natural person, in the jurisdiction where its place of business is located[48]; and

(b) competent authorities take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP.

15.5 Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions to them.[49]

15.6 Consistent with the applicable provisions of Recommendations 26 and 27, countries should ensure that:

(a) VASPs are subject to adequate regulation and risk-based supervision or monitoring by a competent authority[50], including systems for ensuring their compliance with national AML/CFT requirements;

(b) supervisors have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections, compel the production of information and impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

15.7 In line with Recommendation 34, competent authorities and supervisors should establish guidelines, and provide feedback, which will assist VASPs in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

15.8 In line with Recommendation 35, countries should ensure that:

(a) there is a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements; and

(b) sanctions should be applicable not only to VASPs, but also to their directors and senior management.

15.9 With respect to the preventive measures, VASPs should be required to comply with the requirements set out in Recommendations 10 to 21, subject to the following qualifications:

(a) R.10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.

---

48 To clarify, criterion 15.4(a)(ii) requires that a country ensure that a VASP that is a natural person located in their country is licensed or registered in their country; not that any VASP that is a natural person with a place of business located in the country is registered in any third country where it also has a place of business.

49 Note to assessors: Criterion 15.5 applies to all countries, regardless of whether they have chosen to license, register or prohibit virtual assets or VASPs.

50 In this context, a "competent authority" cannot include a SRB.

(b) R.16 – For virtual asset transfers[51], countries should ensure that:

(i) originating VASPs obtain and hold required and accurate originator information and required beneficiary information[52] on virtual asset transfers, submit[53] the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities;

(ii) beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities[54];

(iii) other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16; and

(iv) the same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

15.10 With respect to targeted financial sanctions, countries should ensure that the communication mechanisms, reporting obligations and monitoring referred to in criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) apply to VASPs.

15.11 Countries should rapidly provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should have a legal basis for exchanging information with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.[55]

---

51 For the purposes of applying R.16 to VASPs, all virtual asset transfers should be treated as cross-border transfers.

52 As defined in INR.16, paragraph 6, or the equivalent information in a virtual asset context.

53 The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to virtual asset transfers.

54 *Appropriate authorities* means *appropriate competent authorities*, as referred to in paragraph 10 of INR.16.

55 Countries that have prohibited VASPs should fulfil this requirement by having in place a legal basis for permitting their relevant competent authorities (e.g. law enforcement agencies) to exchange information on issues related to VAs and VASPs with non-counterparts, as set out in paragraph 17 of INR.40.

RECOMMENDATION 16 WIRE TRANSFERS

Ordering financial institutions

16.1 Financial institutions should be required to ensure that all cross-border wire transfers of USD/EUR 1 000 or more are always accompanied by the following:

(a) Required and accurate[56] originator information:

(i) the name of the originator;

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

(iii) the originator's address, or national identity number, or customer identification number, or date and place of birth.

(b) Required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

16.2 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the financial institution should be required to include the originator's account number or unique transaction reference number.

16.3 If countries apply a *de minimis* threshold for the requirements of criterion 16.1, financial institutions should be required to ensure that all cross-border wire transfers below any applicable *de minimis* threshold (no higher than USD/EUR 1 000) are always accompanied by the following:

(a) Required originator information:

(i) the name of the originator; and

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

56 "Accurate" is used to describe information that has been verified for accuracy; *i.e.* financial institutions should be required to verify the accuracy of the required originator information.

(b) Required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction

16.4 The information mentioned in criterion 16.3 need not be verified for accuracy. However, the financial institution should be required to verify the information pertaining to its customer where there is a suspicion of ML/TF.

16.5 For domestic wire transfers[57], the ordering financial institution should be required to ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means.

16.6 Where the information accompanying the domestic wire transfer can be made available to the beneficiary financial institution and appropriate authorities by other means, the ordering financial institution need only be required to include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering financial institution should be required to make the information available within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

16.7 The ordering financial institution should be required to maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

16.8 The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above at criteria 16.1-16.7.

Intermediary financial institutions

16.9 For cross-border wire transfers, an intermediary financial institution should be required to ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

16.10 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution should be required to keep a record, for at

57 This term also refers to any chain of wire transfers that takes place entirely within the borders of the European Union. It is further noted that the European internal market and corresponding legal framework is extended to the members of the European Economic Area.

least five years, of all the information received from the ordering financial institution or another intermediary financial institution.

16.11 Intermediary financial institutions should be required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

16.12 Intermediary financial institutions should be required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

Beneficiary financial institutions

16.13 Beneficiary financial institutions should be required to take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

16.14 For cross-border wire transfers of USD/EUR 1 000 or more[58], a beneficiary financial institution should be required to verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

16.15 Beneficiary financial institutions should be required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

Money or value transfer service operators

16.16 MVTS providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents.

16.17 In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider should be required to:

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

---

58 Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1 000). Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

Implementation of Targeted Financial Sanctions

16.18 Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions.

RECOMMENDATION 17 RELIANCE ON THIRD PARTIES

17.1 If financial institutions are permitted to rely on third-party financial institutions and DNFBPs to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 (identification of the customer; identification of the beneficial owner; and understanding the nature of the business) or to introduce business, the ultimate responsibility for CDD measures should remain with the financial institution relying on the third party, which should be required to:

(a) obtain immediately the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10;

(b) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

(c) satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

17.2 When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

17.3 For financial institutions that rely on a third party that is part of the same financial group, relevant competent authorities[59] may also consider that the requirements of the criteria above are met in the following circumstances:

(a) the group applies CDD and record-keeping requirements, in line with Recommendations 10 to 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18;

(b) the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and

(c) any higher country risk is adequately mitigated by the group's AML/CFT policies.

[59] The term *relevant competent authorities* in Recommendation 17 means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.

RECOMMENDATION 18 INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES

18.1 Financial institutions should be required to implement programmes against ML/TF, which have regard to the ML/TF risks and the size of the business, and which include the following internal policies, procedures and controls:

(a) compliance management arrangements (including the appointment of a compliance officer at the management level);

(b) screening procedures to ensure high standards when hiring employees;

(c) an ongoing employee training programme; and

(d) an independent audit function to test the system.

18.2 Financial groups should be required to implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in criterion 18.1 and also:

(a) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(b) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done)[60]. Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management[61]; and

(c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

18.3 Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit.

If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups should be required to

60 This could include an STR, its underlying information, or the fact than an STR has been submitted.

61 The scope and extent of the information to be shared in accordance with this criterion may be determined by countries, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors.

RECOMMENDATION 19 HIGHER RISK COUNTRIES

19.1 Financial institutions should be required to apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

19.2 Countries should be able to apply countermeasures proportionate to the risks: (a) when called upon to do so by the FATF; and (b) independently of any call by the FATF to do so.

19.3 Countries should have measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

RECOMMENDATION 20 REPORTING OF SUSPICIOUS TRANSACTIONS[62]

20.1 If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity[63], or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit.

20.2 Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

62 The requirement that financial institutions should report suspicious transactions should be set out in law.

63 "Criminal activity" refers to: (a) all criminal acts that would constitute a predicate offence for ML in the country; or (b) at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3.

RECOMMENDATION 21 TIPPING-OFF AND CONFIDENTIALITY

21.1 Financial institutions and their directors, officers and employees should be protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. This protection should be available even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

21.2 Financial institutions and their directors, officers and employees should be prohibited by law from disclosing the fact that an STR or related information is being filed with the Financial Intelligence Unit. These provisions are not intended to inhibit information sharing under Recommendation 18.

RECOMMENDATION 22 DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPS): CUSTOMER DUE DILIGENCE

22.1 DNFBPs should be required to comply with the CDD requirements set out in Recommendation 10 in the following situations:

(a) Casinos – when customers engage in financial transactions[64] equal to or above USD/EUR 3 000.

(b) Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate[65].

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above USD/EUR 15,000.

(d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for, or carry out, transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creating, operating or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

64 Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link CDD information for a particular customer to the transactions that the customer conducts in the casino. "Financial transactions" does not refer to gambling transactions that involve only casino chips or tokens.

65 This means that real estate agents should comply with the requirements set out in Recommendation 10 with respect to both the purchasers and the vendors of the property.

- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

22.2 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the record-keeping requirements set out in Recommendation 11.

22.3 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the PEPs requirements set out in Recommendation 12.

22.4 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the new technologies requirements set out in Recommendation 15.

22.5 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the reliance on third-parties requirements set out in Recommendation 17.

RECOMMENDATION 23 DNFBPS: OTHER MEASURES

23.1 The requirements to report suspicious transactions set out in Recommendation 20 should apply to all DNFBPs subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants [66] – when, on behalf of, or for, a client, they engage in a financial transaction in relation to the activities described in criterion 22.1(d)[67].

(b) Dealers in precious metals or stones – when they engage in a cash transaction with a customer equal to or above USD/EUR 15,000.

(c) Trust and company service providers – when, on behalf or for a client, they engage in a transaction in relation to the activities described in criterion 22.1(e).

23.2 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the internal controls requirements set out in Recommendation 18.

23.3 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the higher-risk countries requirements set out in Recommendation 19.

23.4 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the tipping-off and confidentiality requirements set out in Recommendation 21[68].

---

66 Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.

67 Where countries allow lawyers, notaries, other independent legal professionals and accountants to send their STRs to their appropriate self-regulatory bodies (SRBs), there should be forms of co-operation between these bodies and the FIU.

68 Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

RECOMMENDATION 24 — TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS[69]

24.1 Countries should have mechanisms that identify and describe: (a) the different types, forms and basic features of legal persons in the country; and (b) the processes for the creation of those legal persons, and for obtaining and recording of basic and beneficial ownership information. This information should be publicly available.

24.2 Countries should assess the ML/TF risks associated with all types of legal person created in the country.

Basic Information

24.3 Countries should require that all companies created in a country are registered in a company registry, which should record the company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, and a list of directors. This information should be publicly available.

24.4 Companies should be required to maintain the information set out in criterion 24.3, and also to maintain a register of their shareholders or members[70], containing the number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights). This information should be maintained within the country at a location notified to the company registry[71].

24.5 Countries should have mechanisms that ensure that the information referred to in criteria 24.3 and 24.4 is accurate and updated on a timely basis.

---

69 Assessors should consider the application of all the criteria to all relevant types of legal persons. The manner in which these requirements are addressed may vary according to the type of legal person involved:

1. *Companies* - The measures required by Recommendation 24 are set out with specific reference to companies.
2. *Foundations, Anstalt, and limited liability partnerships* - countries should take similar measures and impose similar requirements as those required for companies, taking into account their different forms and structures.
3. *Other types of legal persons* - countries should take into account the different forms and structures of those other legal persons, and the levels of ML/TF risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, all legal persons should ensure that similar types of basic information are recorded.

70 The register of shareholders and members can be recorded by the company itself or by a third person under the company's responsibility.

71 In cases in which the company or company registry holds beneficial ownership information within the country, the register of shareholders and members need not be in the country, if the company can provide this information promptly on request.

Beneficial Ownership Information

24.6 Countries should use one or more of the following mechanisms to ensure that information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or can be otherwise determined in a timely manner by a competent authority:

(a) requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

(b) requiring companies to take reasonable measures to obtain and hold up-to-date information on the companies' beneficial ownership;

(c) using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22; (ii) information held by other competent authorities on the legal and beneficial ownership of companies; (iii) information held by the company as required in criterion 24.3 above; and (iv) available information on companies listed on a stock exchange, where disclosure requirements ensure adequate transparency of beneficial ownership.

24.7 Countries should require that the beneficial ownership information is accurate and as up-to-date as possible.

24.8 Countries should ensure that companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner, by:

(a) requiring that one or more natural persons resident in the country is authorised by the company[72], and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

(b) requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

(c) taking other comparable measures, specifically identified by the country.

24.9 All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should be required to maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

[72] Members of the company's board or senior management may not require specific authorisation by the company.

Other Requirements

24.10 Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

24.11 Countries that have legal persons able to issue bearer shares or bearer share warrants should apply one or more of the following mechanisms to ensure that they are not misused for money laundering or terrorist financing:

(a) prohibiting bearer shares and share warrants; or

(b) converting bearer shares and share warrants into registered shares or share warrants (for example through dematerialisation); or

(c) immobilising bearer shares and share warrants by requiring them to be held with a regulated financial institution or professional intermediary; or

(d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity; or

(e) using other mechanisms identified by the country.

24.12 Countries that have legal persons able to have nominee shares and nominee directors should apply one or more of the following mechanisms to ensure they are not misused:

(a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register;

(b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request; or

(c) using other mechanisms identified by the country.

24.13 There should be liability and proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to comply with the requirements.

24.14 Countries should rapidly provide international co-operation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include:

(a) facilitating access by foreign competent authorities to basic information held by company registries;

(b) exchanging information on shareholders; and

(c) using their competent authorities' investigative powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts.

24.15 Countries should monitor the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

RECOMMENDATION 25 TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS[73]

25.1 Countries should require:

(a) trustees of any express trust governed under their law[74] to obtain and hold adequate, accurate, and current information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust;

(b) trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; and

(c) professional trustees to maintain this information for at least five years after their involvement with the trust ceases.

25.2 Countries should require that any information held pursuant to this Recommendation is kept accurate and as up to date as possible, and is updated on a timely basis.

25.3 All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold.

25.4 Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust[75]; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

---

73 The measures required by Recommendation 25 are set out with specific reference to trusts. This should be understood as referring to express trusts (as defined in the glossary). In relation to other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities. When considering examples provided in the Glossary definition of legal arrangement, assessors are reminded that the examples provided should not be considered definitive. Assessors should refer to the Glossary definition of trust and trustee which references Article 2 of the Hague Convention on the law applicable to trusts and their recognition when determining whether a legal arrangement has a similar structure or function to an express trust and therefore falls within the scope of R.25, regardless of whether the country denominates the legal arrangement using the same terminology. If a country does not apply the relevant obligations of R.25 on trustees (or those performing a similar function in relation to other legal arrangements), assessors should confirm whether such exemptions are consistent with criterion 1.6.

74 Countries are not required to give legal recognition to trusts. Countries need not include the requirements of Criteria 25.1; 25.2; 25.3; and 25.4 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

75 Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

25.5 Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to information held by trustees, and other parties (in particular information held by financial institutions and DNFBPs), on the beneficial ownership and control of the trust, including: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

25.6 Countries should rapidly provide international co-operation in relation to information, including beneficial ownership information, on trusts and other legal arrangements, on the basis set out in Recommendations 37 and 40. This should include:

(a) facilitating access by foreign competent authorities to basic information held by registries or other domestic authorities;

(b) exchanging domestically available information on the trusts or other legal arrangement; and

(c) using their competent authorities' investigative powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.

25.7 Countries should ensure that trustees are either (a) legally liable for any failure to perform the duties relevant to meeting their obligations; or (b) that there are proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply[76].

25.8 Countries should ensure that there are proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information regarding the trust referred to in criterion 25.1.

[76] This does not affect the requirements for proportionate and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

RECOMMENDATION 26 REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS

26.1 Countries should designate one or more supervisors that have responsibility for regulating and supervising (or monitoring) financial institutions' compliance with the AML/CFT requirements.

Market Entry

26.2 Core Principles financial institutions should be required to be licensed. Other financial institutions, including those providing a money or value transfer service or a money or currency changing service, should be licensed or registered. Countries should not approve the establishment, or continued operation, of shell banks.

26.3 Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, in a financial institution.

Risk-based approach to supervision and monitoring

26.4 Financial institutions should be subject to:

(a) *for core principles institutions* - regulation and supervision in line with the core principles[77], where relevant for AML/CFT, including the application of consolidated group supervision for AML/CFT purposes.

(b) *for all other financial institutions* - regulation and supervision or monitoring, having regard to the ML/TF risks in that sector. At a minimum, for *financial institutions providing a money or value transfer service, or a money or currency changing service* - systems for monitoring and ensuring compliance with national AML/CFT requirements.

26.5 The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions or groups should be determined on the basis of:

(a) the ML/TF risks and the policies, internal controls and procedures associated with the institution or group, as identified by the supervisor's assessment of the institution's or group's risk profile;

(b) the ML/TF risks present in the country; and

77 The Core Principles which are relevant to AML/CFT include: Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29; International Association of Insurance Supervisors (IAIS) Principles 1, 3-11, 18, 21-23, and 25; and International Organization of Securities Commission (IOSCO) Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D. Assessors may refer to existing assessments of the country's compliance with these Core Principles, where available.

(c) the characteristics of the financial institutions or groups, in particular the diversity and number of financial institutions and the degree of discretion allowed to them under the risk-based approach.

26.6 The supervisor should review the assessment of the ML/TF risk profile of a financial institution or group (including the risks of non-compliance) periodically, and when there are major events or developments in the management and operations of the financial institution or group.

RECOMMENDATION 27 POWERS OF SUPERVISORS

27.1 Supervisors should have powers to supervise or monitor and ensure compliance by financial institutions with AML/CFT requirements.

27.2 Supervisors should have the authority to conduct inspections of financial institutions.

27.3 Supervisors should be authorised to compel[78] production of any information relevant to monitoring compliance with the AML/CFT requirements.

27.4 Supervisors should be authorised to impose sanctions in line with Recommendation 35 for failure to comply with the AML/CFT requirements. This should include powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's licence.

78 The supervisor's power to compel production of or to obtain access for supervisory purposes should not be predicated on the need to require a court order.

RECOMMENDATION 28 REGULATION AND SUPERVISION OF DNFBPS

Casinos

28.1 Countries should ensure that casinos are subject to AML/CFT regulation and supervision. At a minimum:

(a) Countries should require casinos to be licensed.

(b) Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, or being an operator of a casino.

(c) Casinos should be supervised for compliance with AML/CFT requirements.

DNFBPs other than casinos

28.2 There should be a designated competent authority or SRB responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements.

28.3 Countries should ensure that the other categories of DNFBPs are subject to systems for monitoring compliance with AML/CFT requirements.

28.4 The designated competent authority or self-regulatory body (SRB) should:

(a) have adequate powers to perform its functions, including powers to monitor compliance;

(b) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function in a DNFBP; and

(c) have sanctions available in line with Recommendation 35 to deal with failure to comply with AML/CFT requirements.

All DNFBPs

28.5 Supervision of DNFBPs should be performed on a risk-sensitive basis, including:

(a) determining the frequency and intensity of AML/CFT supervision of DNFBPs on the basis of their understanding of the ML/TF risks, taking into consideration the characteristics of the DNFBPs, in particular their diversity and number; and

(b) taking into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

RECOMMENDATION 29 FINANCIAL INTELLIGENCE UNITS (FIU)

29.1 Countries should establish an FIU with responsibility for acting as a national centre for receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis.[79]

29.2 The FIU should serve as the central agency for the receipt of disclosures filed by reporting entities, including:

(a) Suspicious transaction reports filed by reporting entities as required by Recommendation 20 and 23; and

(b) any other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

29.3 The FIU should[80]:

(a) in addition to the information that entities report to the FIU, be able to obtain and use additional information from reporting entities, as needed to perform its analysis properly; and

(b) have access to the widest possible range[81] of financial, administrative and law enforcement information that it requires to properly undertake its functions.

29.4 The FIU should conduct:

(a) operational analysis, which uses available and obtainable information to identify specific targets, to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences and terrorist financing; and

(b) strategic analysis, which uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns.

29.5 The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities, and should use dedicated, secure and protected channels for the dissemination.

---

79 Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

80 In the context of its analysis function, an FIU should be able to obtain from any reporting entity additional information relating to a suspicion of ML/TF. This does not include indiscriminate requests for information to reporting entities in the context of the FIU's analysis (e.g., "fishing expeditions").

81 This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate commercially held data.

29.6 The FIU should protect information by:

(a) having rules in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access to, information;

(b) ensuring that FIU staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information; and

(c) ensuring that there is limited access to its facilities and information, including information technology systems.

29.7 The FIU should be operationally independent and autonomous, by:

(a) having the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or forward or disseminate specific information;

(b) being able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information;

(c) when it is located within the existing structure of another authority, having distinct core functions from those of the other authority; and

(d) being able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

29.8 Where a country has created an FIU and is not an Egmont Group member, the FIU should apply for membership in the Egmont Group. The FIU should submit an unconditional application for membership to the Egmont Group and fully engage itself in the application process.

RECOMMENDATION 30 RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

30.1 There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, associated predicate offences and terrorist financing offences are properly investigated, within the framework of national AML/CFT policies.

30.2 Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related ML/TF offences during a parallel financial investigation[82], or be able to refer the case to another agency to follow up with such investigations, regardless of where the predicate offence occurred.

30.3 There should be one or more designated competent authorities to expeditiously identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime.

30.4 Countries should ensure that Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

30.5 If anti-corruption enforcement authorities are designated to investigate ML/TF offences arising from, or related to, corruption offences under Recommendation 30, they should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

---

82 A '*parallel financial investigation*' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s).

A '*financial investigation*' means an enquiry into the financial affairs related to a criminal activity, with a view to: (i) identifying the extent of criminal networks and/or the scale of criminality; (ii) identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and (iii) developing evidence which can be used in criminal proceedings.

RECOMMENDATION 31 POWERS OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

31.1 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for:

(a) the production of records held by financial institutions, DNFBPs and other natural or legal persons;

(b) the search of persons and premises;

(c) taking witness statements; and

(d) seizing and obtaining evidence.

31.2 Competent authorities conducting investigations should be able to use a wide range of investigative techniques for the investigation of money laundering, associated predicate offences and terrorist financing, including:

(a) undercover operations;

(b) intercepting communications;

(c) accessing computer systems; and

(d) controlled delivery.

31.3 Countries should have mechanisms in place:

(a) to identify, in a timely manner, whether natural or legal persons hold or control accounts; and

(b) to ensure that competent authorities have a process to identify assets without prior notification to the owner.

31.4 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to ask for all relevant information held by the FIU.

RECOMMENDATION 32 CASH COURIERS

Note to Assessors:
Recommendation 32 may be implemented on a supra-national basis by a supra-national jurisdiction, such that only movements that cross the external borders of the supra-national jurisdiction are considered to be cross-border for the purposes of Recommendation 32. Such arrangements are assessed on a supra-national basis, on the basis set out in Annex I.

32.1 Countries should implement a declaration system or a disclosure system for incoming and outgoing cross-border transportation of currency and bearer negotiable instruments (BNIs). Countries should ensure that a declaration or disclosure is required for all physical cross-border transportation, whether by travellers or through mail and cargo, but may use different systems for different modes of transportation.

32.2 In a declaration system, all persons making a physical cross-border transportation of currency or BNIs, which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15 000, should be required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system:

(a) A written declaration system for all travellers;

(b) A written declaration system for all travellers carrying amounts above a threshold; and/or

(c) An oral declaration system for all travellers.

32.3 In a disclosure system, travellers should be required to give a truthful answer and provide the authorities with appropriate information upon request, but are not required to make an upfront written or oral declaration.

32.4 Upon discovery of a false declaration or disclosure of currency or BNIs or a failure to declare or disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs, and their intended use.

32.5 Persons who make a false declaration or disclosure should be subject to proportionate and dissuasive sanctions, whether criminal, civil or administrative.

32.6 Information obtained through the declaration/disclosure process should be available to the FIU either through: (a) a system whereby the FIU is notified about suspicious cross-border transportation incidents; or (b) by making the declaration/disclosure information directly available to the FIU in some other way.

32.7 At the domestic level, countries should ensure that there is adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

32.8 Competent authorities should be able to stop or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/TF may be found in cases:

(a) where there is a suspicion of ML/TF or predicate offences; or

(b) where there is a false declaration or false disclosure.

32.9 Countries should ensure that the declaration/disclosure system allows for international co-operation and assistance, in accordance with Recommendations 36 to 40. To facilitate such co-operation, information[83] shall be retained when:

(a) a declaration or disclosure which exceeds the prescribed threshold is made; or

(b) there is a false declaration or false disclosure; or

(c) there is a suspicion of ML/TF.

32.10 Countries should ensure that strict safeguards exist to ensure proper use of information collected through the declaration/disclosure systems, without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

32.11 Persons who are carrying out a physical cross-border transportation of currency or BNIs that are related to ML/TF or predicate offences should be subject to: (a) proportionate and dissuasive sanctions, whether criminal, civil or administrative; and (b) measures consistent with Recommendation 4 which would enable the confiscation of such currency or BNIs.

83 At a minimum, the information should set out (i) the amount of currency or BNIs declared, disclosed or otherwise detected, and (ii) the identification data of the bearer(s).

RECOMMENDATION 33 STATISTICS

33.1 Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems.[84] This should include keeping statistics on:

(a) STRs, received and disseminated;

(b) ML/TF investigations, prosecutions and convictions;

(c) Property frozen; seized and confiscated; and

(d) Mutual legal assistance or other international requests for co-operation made and received.

[84] For purposes of technical compliance, the assessment should be limited to the four areas listed below.

RECOMMENDATION 34 GUIDANCE AND FEEDBACK

34.1 Competent authorities, supervisors, and SRBs should establish guidelines and provide feedback, which will assist financial institutions and DNFBPs in applying national AML/CFT measures, and in particular, in detecting and reporting suspicious transactions.

RECOMMENDATION 35 SANCTIONS

35.1 Countries should ensure that there is a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT requirements of Recommendations 6, and 8 to 23.[85]

35.2 Sanctions should be applicable not only to financial institutions and DNFBPs but also to their directors and senior management.

[85] The sanctions should be directly or indirectly applicable for a failure to comply. They need not be in the same document that imposes or underpins the requirement, and can be in another document, provided there are clear links between the requirement and the available sanctions.

RECOMMENDATION 36 INTERNATIONAL INSTRUMENTS

36.1 Countries should become a party to the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption (the Merida Convention) and the Terrorist Financing Convention.

36.2 Countries should fully implement[86] the Vienna Convention, the Palermo Convention, the Merida Convention and the Terrorist Financing Convention.

86 The relevant articles are: the Vienna Convention (Articles 3-11, 15, 17 and 19), the Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31, & 34), the Merida Convention (Articles 14-17, 23-24, 26-31, 38, 40, 43-44, 46, 48, 50-55, 57-58), and the Terrorist Financing Convention (Articles 2-18).

RECOMMENDATION 37 MUTUAL LEGAL ASSISTANCE

37.1 Countries should have a legal basis that allows them to rapidly provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions and related proceedings.

37.2 Countries should use a central authority, or another established official mechanism, for the transmission and execution of requests. There should be clear processes for the timely prioritisation and execution of mutual legal assistance requests. To monitor progress on requests, a case management system should be maintained.

37.3 Mutual legal assistance should not be prohibited or made subject to unreasonable or unduly restrictive conditions.

37.4 Countries should not refuse a request for mutual legal assistance:

(a) on the sole ground that the offence is also considered to involve fiscal matters; or

(b) on the grounds of secrecy or confidentiality requirements on financial institutions or DNFBPs, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.

37.5 Countries should maintain the confidentiality of mutual legal assistance requests that they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry.

37.6 Where mutual legal assistance requests do not involve coercive actions, countries should not make dual criminality a condition for rendering assistance.

37.7 Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

37.8 Powers and investigative techniques that are required under Recommendation 31 or otherwise available to domestic competent authorities should also be available for use in response to requests for mutual legal assistance, and, if consistent with the domestic framework, in response to a direct request from foreign judicial or law enforcement authorities to domestic counterparts. These should include:

(a) all of the specific powers required under Recommendation31 relating to the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques.

RECOMMENDATION 38 MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION

38.1 Countries should have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize, or confiscate:

(a) laundered property from,

(b) proceeds from,

(c) instrumentalities used in, or

(d) instrumentalities intended for use in,

money laundering, predicate offences, or terrorist financing; or

(e) property of corresponding value.

38.2 Countries should have the authority to provide assistance to requests for co-operation made on the basis of non-conviction based confiscation proceedings and related provisional measures, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown, unless this is inconsistent with fundamental principles of domestic law.

38.3 Countries should have: (a) arrangements for co-ordinating seizure and confiscation actions with other countries; and (b) mechanisms for managing, and when necessary disposing of, property frozen, seized or confiscated.

38.4 Countries should be able to share confiscated property with other countries, in particular when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

RECOMMENDATION 39 EXTRADITION

39.1 Countries should be able to execute extradition requests in relation to ML/TF without undue delay. In particular, countries should:

(a) ensure ML and TF are extraditable offences;

(b) ensure that they have a case management system, and clear processes for the timely execution of extradition requests including prioritisation where appropriate; and

(c) not place unreasonable or unduly restrictive conditions on the execution of requests.

39.2 Countries should either:

(a) extradite their own nationals; or

(b) where they do not do so solely on the grounds of nationality, should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request.

39.3 Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

39.4 Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms[87] in place.

[87] Such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

RECOMMENDATION 40 OTHER FORMS OF INTERNATIONAL CO-OPERATION

General Principles

40.1 Countries should ensure that their competent authorities can rapidly provide the widest range of international co-operation in relation to money laundering, associated predicate offences and terrorist financing. Such exchanges of information should be possible both spontaneously and upon request.

40.2 Competent authorities should:

(a) have a lawful basis for providing co-operation;

(b) be authorised to use the most efficient means to co-operate;

(c) have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests;

(d) have clear processes for the prioritisation and timely execution of requests; and

(e) have clear processes for safeguarding the information received.

40.3 Where competent authorities need bilateral or multilateral agreements or arrangements to co-operate, these should be negotiated and signed in a timely way, and with the widest range of foreign counterparts.

40.4 Upon request, requesting competent authorities should provide feedback in a timely manner to competent authorities from which they have received assistance, on the use and usefulness of the information obtained.

40.5 Countries should not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of exchange of information or assistance. In particular, competent authorities should not refuse a request for assistance on the grounds that:

(a) the request is also considered to involve fiscal matters; and/or

(b) laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies); and/or

(c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

(d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

40.6 Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorisation has been given by the requested competent authority.

40.7 Competent authorities should maintain appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Competent authorities should be able to refuse to provide information if the requesting competent authority cannot protect the information effectively.

40.8 Competent authorities should be able to conduct inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

Exchange of Information between FIUs

40.9 FIUs should have an adequate legal basis for providing co-operation on money laundering, associated predicate offences and terrorist financing[88].

40.10 FIUs should provide feedback to their foreign counterparts, upon request and whenever possible, on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

40.11 FIUs should have the power to exchange:

(a) all information required to be accessible or obtainable directly or indirectly by the FIU, in particular under Recommendation 29; and

(b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

Exchange of information between financial supervisors[89]

40.12 Financial supervisors should have a legal basis for providing co-operation with their foreign counterparts (regardless of their respective nature or status), consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

40.13 Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, in a manner proportionate to their respective needs.

40.14 Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other supervisors that have a shared responsibility for financial institutions operating in the same group:

---

88 FIUs should be able to provide cooperation regardless of whether their counterpart FIU is administrative, law enforcement, judicial or other in nature.

89 This refers to financial supervisors which are competent authorities and does not include financial supervisors which are SRBs.

(a) regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors;

(b) prudential information, in particular for Core Principles supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness; and

(c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

40.15 Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

40.16 Financial supervisors should ensure that they have the prior authorisation of the requested financial supervisor for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation.

Exchange of information between law enforcement authorities

40.17 Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

40.18 Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement co-operation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

40.19 Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations.

Exchange of information between non-counterparts

40.20 Countries should permit their competent authorities to exchange information indirectly[90] with non-counterparts, applying the relevant principles above. Countries should ensure

[90] Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting

that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made.

authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country.

EFFECTIVENESS ASSESSMENT

Immediate Outcome 1	Money laundering and terrorist financing risks are understood and, where appropriate, actions co-ordinated domestically to combat money laundering and the financing of terrorism and proliferation.

Characteristics of an effective system

A country properly identifies, assesses and understands its money laundering and terrorist financing risks, and co-ordinates domestically to put in place actions to mitigate these risks. This includes the involvement of competent authorities and other relevant authorities; using a wide range of reliable information sources; using the assessment(s) of risks as a basis for developing and prioritising AML/CFT policies and activities; and communicating and implementing those policies and activities in a co-ordinated way across appropriate channels. The relevant competent authorities also co-operate, and co-ordinate policies and activities to combat the financing of proliferation. Over time, this results in substantial mitigation of money laundering and terrorist financing risks.

This outcome relates primarily to Recommendations 1, 2, 33 and 34, and also elements of R.15.

Note to Assessors:

1) Assessors are not expected to conduct an in-depth review of, or assess the country's assessment(s) of risks. Assessors, based on their views of the reasonableness of the assessment(s) of risks, should focus on how well the competent authorities use their understanding of the risks in practice to inform policy development and actions to mitigate the risks.

2) Assessors should take into consideration their findings for this Immediate Outcome (IO) in their assessment of the other IOs. However, assessors should only let their findings relating to the co-operation and co-ordination of measures to combat the financing of proliferation affect the assessments of IO.11 and not of the other IOs. (*i.e.* IO.2 to IO.10) that deal with combating money laundering and terrorist financing.

Core Issues to be considered in determining if the Outcome is being achieved

1.1. How well does the country understand its ML/TF risks?

1.2. How well are the identified ML/TF risks addressed by national AML/CFT policies and activities?

1.3. To what extent are the results of the assessment(s) of risks properly used to justify exemptions and support the application of enhanced measures for higher risk scenarios, or simplified measures for lower risk scenarios?

1.4. To what extent are the objectives and activities of the competent authorities and SRBs consistent with the evolving national AML/CFT policies and with the ML/TF risks identified?

1.5. To what extent do the competent authorities and SRBs co-operate and co-ordinate the development and implementation of policies[91] and activities to combat ML/TF and, where appropriate, the financing of proliferation of weapons of mass destruction?[92]

1.6. To what extent does the country ensure that respective financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the relevant results of the national ML/TF risk assessment(s)?

a) Examples of Information that could support the conclusions on Core Issues

1. The country's assessment(s) of its ML/TF risks (e.g., *types of assessment(s) produced; types of assessment(s) published / communicated*).

2. AML/CFT policies and strategies (e.g., *AML/CFT policies, strategies and statements communicated/published; engagement and commitment at the senior officials and political level*).

3. Outreach activities to private sector and relevant authorities (e.g., *briefings and guidance on relevant conclusions from risk assessment(s); frequency and relevancy of consultation on policies and legislation, input to develop risk assessment(s) and other policy products*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

4. What are the methods, tools, and information used to develop, review and evaluate the conclusions of the assessment(s) of risks? How comprehensive are the information and data used?

5. How useful are strategic financial intelligence, analysis, typologies, and guidance?

6. Which competent authorities and relevant stakeholders (including financial institutions and DNFBPs) are involved in the assessment(s) of risks? How do they provide inputs to the national level ML/TF assessment(s) of risks, and at what stage?

7. Is the assessment(s) of risks kept up-to-date, reviewed regularly and responsive to significant events or developments (including new threats and trends)?

---

91 Having regard to AML/CFT requirements and Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation) as needed.

92 Considering that there are different forms of co-operation and co-ordination between relevant authorities, Core Issue 1.5 does not prejudge a country's choice for a particular form and applies equally to all of them.

8. To what extent is the assessment(s) of risks reasonable and consistent with the ML/TF threats, vulnerabilities and specificities faced by the country? Where appropriate, does it take into account risks identified by other credible sources?

9. Do the policies of competent authorities respond to changing ML/TF risks?

10. What mechanism(s) or body do the authorities use to ensure proper and regular co-operation and co-ordination of the national framework and development and implementation of policies to combat ML/TF, at both policymaking and operational levels (and where relevant, the financing of proliferation of weapons of mass destruction)? Does the mechanism or body include all relevant authorities?

11. Is interagency information sharing undertaken in a timely manner on a bilateral or multiagency basis as appropriate?

12. Are there adequate resources and expertise involved in conducting the assessment(s) of risks, and for domestic co-operation and co-ordination?

Immediate Outcome 2	International co-operation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.

Characteristics of an effective system

The country provides constructive and timely information or assistance when requested by other countries. Competent authorities assist with requests to:

- locate and extradite criminals; and
- identify, freeze, seize, confiscate and share assets and provide information (including evidence, financial intelligence, supervisory and beneficial ownership information) related to money laundering, terrorist financing or associated predicate offences.

Competent authorities also seek international co-operation to pursue criminals and their assets. Over time, this makes the country an unattractive location for criminals (including terrorists) to operate in, maintain their illegal proceeds in, or use as a safe haven.

This outcome relates primarily to Recommendations 36 - 40 and also elements of Recommendations 9, 15, 24, 25 and 32.

Note to Assessors:

Assessors should take into consideration how their findings on the specific role of relevant competent authorities in seeking and delivering international co-operation under this IO would impact other IOs (particularly IO.3, IO.5, IOs. 6 to 10) including how the country seeks international co-operation with respect to domestic cases when appropriate.

Core Issues to be considered in determining if the Outcome is being achieved

2.1. To what extent has the country provided constructive and timely mutual legal assistance and extradition across the range of international co-operation requests? What is the quality of such assistance provided?

2.2. To what extent has the country sought legal assistance for international co-operation in an appropriate and timely manner to pursue domestic ML, associated predicate offences and TF cases which have transnational elements?

2.3. To what extent do the different competent authorities seek other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes?

2.4. To what extent do the different competent authorities provide (including spontaneously) other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in a constructive and timely manner with their foreign counterparts for AML/CFT purposes?

2.5. How well are the competent authorities providing and responding to foreign requests for co-operation in identifying and exchanging basic and beneficial ownership information of legal persons and arrangements?

a) Examples of Information that could support the conclusions on Core Issues

1. Evidence of handling and making requests for international co-operation with respect to extradition, mutual legal assistance and other forms of international co-operation (*e.g., number of requests made, received, processed, granted, or refused relating to different competent authorities (e.g., central authority, FIU, supervisors, and law enforcement agencies) and types of request; timeliness of response, including prioritisation of requests; cases of spontaneous dissemination / exchange*).
2. Types and number of co-operation arrangements with other countries (including bilateral and multilateral MOUs, treaties, co-operation based on reciprocity, or other co-operation mechanisms).
3. Examples of: (a) making requests for, and (b) providing successful international co-operation (e.g.*, making use of financial intelligence / evidence provided to or by the country (as the case may be); investigations conducted on behalf or jointly with foreign counterparts; extradition of suspects/criminals for ML/TF*).
4. Information on investigations, prosecutions, confiscation and repatriation/sharing of assets (e.g., *number of ML/TF investigations/ prosecutions, number and value of assets frozen and confiscated (including non-conviction-based confiscation) arising from international co-operation; value of assets repatriated or shared*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What operational measures are in place to ensure that appropriate safeguards are applied, requests are handled in a confidential manner to protect the integrity of the process (*e.g.,* investigations and inquiry), and information exchanged is used for authorised purposes?
6. What mechanisms (including case management systems) are used among the different competent authorities to receive, assess, prioritise and respond to requests for assistance?
7. What are the reasons for refusal in cases where assistance is not or cannot be provided?
8. What mechanisms (including case management systems) are used among the different competent authorities to select, prioritise and make requests for assistance?
9. How do different competent authorities ensure that relevant and accurate information is provided to the requested country to allow it to understand and assess the requests?

10. How well has the country worked with the requesting or requested country to avoid or resolve conflicts of jurisdiction or problems caused by poor quality information in requests?

11. How do competent authorities ensure that details of the contact persons and requirements for international co-operation requests are clear and easily available to requesting countries?

12. To what extent does the country prosecute its own nationals without undue delay in situations when it is unable by law to extradite them?

13. What measures and arrangements are in place to manage and repatriate assets confiscated at the request of other countries?

14. Are there aspects of the legal, operational or judicial process (*e.g.,* excessively strict application of dual criminality requirements etc.) that impede or hinder international co-operation?

15. To what extent are competent authorities exchanging information, indirectly, with non-counterparts?

16. Are adequate resources available for: (a) receiving, managing, coordinating and responding to incoming requests for co-operation; and (b) making and coordinating requests for assistance in a timely manner?

Immediate Outcome 3	Supervisors appropriately supervise, monitor and regulate financial institutions, DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks.

Characteristics of an effective system

Supervision and monitoring address and mitigate the money laundering and terrorist financing risks in the financial and other relevant sectors by:

- preventing criminals and their associates from holding, or being the beneficial owner of, a significant or controlling interest or a management function in financial institutions, DNFBPs or VASPs; and
- promptly identifying, remedying, and sanctioning, where appropriate, violations of AML/CFT requirements or failings in money laundering and terrorist financing risk management.

Supervisors[93] provide financial institutions, DNFBPs and VASPs with adequate feedback and guidance on compliance with AML/CFT requirements. Over time, supervision and monitoring improve the level of AML/CFT compliance, and discourage attempts by criminals to abuse the financial, DNFBP and VASP sectors, particularly in the sectors most exposed to money laundering and terrorist financing risks.

This outcome relates primarily to Recommendations 14, 15, 26 to 28, 34 and 35, and also elements of Recommendations 1 and 40.

Note to Assessors:

1) Assessors should determine which financial, DNFBP and VASP sectors to weight as being most important, moderately important or less important, and should reflect their judgment in Chapters 1, 5 and 6 of the report. While judging on the overall effectiveness of this IO, assessors should explain how they have weighted the identified deficiencies and also explain how these have been taken into account in relation to how the assessors have weighted the different sectors.

2) When determining how to weight the various financial, DNFBP and VASP sectors, assessors should consider their relative importance, taking into account the following factors:

a) the ML/TF risks facing each sector, taking into account the materiality relevant to each sector (e.g. the relative importance of different parts of the financial sector and different

[93] In relation to financial institutions and DNFBPs (but not to VASPs), references to "Supervisors" include SRBs for the purpose of the effectiveness assessment.

DNFBPs and VASPs; the size, integration and make-up of the financial sector[94]; the relative importance of different types of financial products or institutions; the amount of business which is domestic or cross-border; the extent to which the economy is cash-based; and estimates of the size of the informal sector and/or shadow economy), and

b) structural elements and other contextual factors (e.g. whether established supervisors with accountability, integrity and transparency are in place for each sector; and the maturity and sophistication of the regulatory and supervisory regime for each sector)[95].

For more information on how assessors should take risk, materiality, structural elements and other contextual factors into account, see paragraphs 5 to 12 of the Methodology. For more guidance on how to reflect in the report their judgment on the relative importance of the financial, DNFBP and VASP sectors, see the Mutual Evaluation Report Template in Annex II of the Methodology.

3) Assessors should also consider the relevant findings (including at the financial group level) on the level of international co-operation which supervisors are participating in when assessing this IO.

Core Issues to be considered in determining if the Outcome is being achieved

3.1. How well does licensing, registration or other controls implemented by supervisors or other authorities prevent criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions, DNFBPs or VASPs? How well are breaches of such licensing or registration requirements detected?

3.2. How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions?

3.3. With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions, DNFBPs and VASPs are complying with their AML/CFT requirements?

3.4. To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?

3.5. To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions, DNFBPs and VASPs?

3.6. How well do the supervisors promote a clear understanding by financial institutions, DNFBPs and VASPs of their AML/CFT obligations and ML/TF risks?

94 E.g. including, but not limited to, the business concentration in the different sectors.

95 E.g. special supervisory activities, such as thematic reviews and targeted outreach to specific sectors or institutions.

a) Examples of Information that could support the conclusions on Core Issues

1. Contextual factors regarding the size, composition, and structure of the financial, DNFBP and VASP sectors and informal or unregulated sector (e.g., *number and types of financial institutions (including MVTS), DNFBPs and VASPs licensed or registered in each category; types of financial (including cross-border) activities; relative size, importance and materiality of sectors*).
2. Supervisors' risk models, manuals and guidance on AML/CFT (e.g., *operations manuals for supervisory staff; publications outlining AML/CFT supervisory / monitoring approach; supervisory circulars, good and poor practises, thematic studies; annual reports*).
3. Information on supervisory engagement with the industry, the FIU and other competent authorities on AML/CFT issues (e.g., *providing guidance and training, organising meetings or promoting interactions with financial institutions, DNFBPs and VASPs*).
4. Information on supervision (e.g., *frequency, scope and nature of monitoring and inspections (on-site and off-site); nature of breaches identified; sanctions and other remedial actions* (e.g., *corrective actions, reprimands, fines) applied, examples of cases where sanctions and other remedial actions have improved AML/CFT compliance*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What are the measures implemented to prevent the establishment or continued operation of shell banks in the country?
6. To what extent are "fit and proper" tests or other similar measures used with regard to persons holding senior management functions, holding a significant or controlling interest, or professionally accredited in financial institutions, DNFBPs and VASPs?
7. What measures do supervisors employ in order to assess the ML/TF risks of the sectors and entities they supervise/monitor? How often are the risk profiles reviewed, and what are the trigger events (e.g., changes in management or business activities)?
8. What measures and supervisory tools are employed to ensure that financial institutions (including financial groups), DNFBPs and VASPs are regulated and comply with their AML/CFT obligations (including those which relate to targeted financial sanctions on terrorism, and to countermeasures called for by the FATF)? To what extent has this promoted the use of the formal financial system?
9. To what extent do the frequency, intensity and scope of on-site and off-site inspections relate to the risk profile of the financial institutions (including financial group), DNFBPs and VASPs?
10. What is the level of co-operation between supervisors and other competent authorities in relation to AML/CFT (including financial group ML/TF risk management) issues? What are the circumstances where supervisors share or seek information from other competent authorities with regard to AML/CFT issues (including market entry)?

11. What measures are taken to identify, license or register, monitor and sanction as appropriate, persons who carry out MVTs and virtual asset services or activities?

12. Do supervisors have adequate resources to conduct supervision or monitoring for AML/CFT purposes, taking into account the size, complexity and risk profiles of the sector supervised or monitored?

13. What are the measures implemented to ensure that financial supervisors have operational independence so that they are not subject to undue influence on AML/CFT matters?

Immediate Outcome 4	Financial institutions, DNFBPs and VASPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.

Characteristics of an effective system

Financial institutions, DNFBPs and VASPs understand the nature and level of their money laundering and terrorist financing risks; develop and apply AML/CFT policies (including group-wide policies), internal controls, and programmes to adequately mitigate those risks; apply appropriate CDD measures to identify and verify the identity of their customers (including the beneficial owners) and conduct ongoing monitoring; adequately detect and report suspicious transactions; and comply with other AML/CFT requirements. This ultimately leads to a reduction in money laundering and terrorist financing activity within these entities.

This outcome relates primarily to Recommendations 9 to 23, and also elements of Recommendations 1, 6 and 29.

Note to Assessors:

1) Assessors should determine which financial, DNFBP and VASP sectors to weight as being most important, moderately important or less important, and should reflect their judgment in Chapters 1, 5 and 6 of the report. While judging on the overall effectiveness of this IO, assessors should explain how they have weighted the identified deficiencies and also explain how these have been taken into account in relation to how the assessors have weighted the different sectors.

2) When determining how to weight the various financial, DNFBP and VASP sectors, assessors should consider their relative importance, taking into account the following factors:

a) the ML/TF risks facing each sector, taking into account the materiality relevant to each sector (e.g. the relative importance of different parts of the financial sector and different DNFBPs and VASPs; the size, integration and make-up of the financial sector[96]; the relative importance of different types of financial products or institutions; the amount of business which is domestic or cross-border; the extent to which the economy is cash-based; and estimates of the size of the informal sector and/or shadow economy), and

96 E.g. including, but not limited to, the business concentration in the different sectors.

b) structural elements and other contextual factors (e.g. whether established supervisors with accountability, integrity and transparency are in place for each sector; and the maturity and sophistication of the regulatory and supervisory regime for each sector)[97].

For more information on how assessors should take risk, materiality, structural elements and other contextual factors into account, see paragraphs 5 to 12 of the Methodology. For more guidance on how to reflect in the report their judgment on the relative importance of the financial, DNFBP and VASP sectors, see the Mutual Evaluation Report Template in Annex II of the Methodology.

3) Assessors are not expected to conduct an in-depth review of the operations of financial institutions, DNFBPs or VASPS, but should consider, on the basis of evidence and interviews with supervisors, FIUs, financial institutions, DNFBPs and VASPs, whether financial institutions, DNFBPs and VASPs have adequately assessed and understood their exposure to money laundering and terrorist financing risks; whether their policies, procedures and internal controls adequately address these risks; and whether regulatory requirements (including STR reporting) are being properly implemented.

Core Issues to be considered in determining if the Outcome is being achieved

4.1. How well do financial institutions, DNFBPs and VASPs understand their ML/TF risks and AML/CFT obligations?

4.2. How well do financial institutions, DNFBPs and VASPs apply mitigating measures commensurate with their risks?

4.3. How well do financial institutions, DNFBPs and VASPs apply the CDD and record-keeping measures (including beneficial ownership information and ongoing monitoring)? To what extent is business refused when CDD is incomplete?

4.4. How well do financial institutions, DNFBPs and VASPs apply the enhanced or specific measures for: (a) PEPs, (b) correspondent banking, (c) new technologies, (d) wire transfer rules[98], (e) targeted financial sanctions relating to TF, and (f) higher-risk countries identified by the FATF?

4.5. To what extent do financial institutions, DNFBPs and VASPs meet their reporting obligations on the suspected proceeds of crime and funds in support of terrorism? What are the practical measures to prevent tipping-off?

4.6. How well do financial institutions, DNFBPs and VASPs apply internal controls and procedures (including at financial group level) to ensure compliance with AML/CFT requirements? To what extent are there legal or regulatory requirements (*e.g.,* financial secrecy) impeding its implementation?

---

97 E.g. special supervisory activities, such as thematic reviews and targeted outreach to specific sectors or institutions.

98 In the context of VASPs, this refers to virtual asset transfer rules.

a) Examples of Information that could support the conclusions on Core Issues

1. Contextual factors regarding the size, composition, and structure of the financial, DNFBP and VASP sectors and informal or unregulated sector (e.g., *number and types of financial institutions (including MVTS), DNFBPs and VASPs licensed or registered in each category; types of financial (including cross-border) activities; relative size, importance and materiality of sectors*).
2. Information (including trends) relating to risks and general levels of compliance (e.g., *internal AML/CFT policies, procedures and programmes, trends and typologies reports*).
3. Examples of compliance failures (e.g., *sanitised cases; typologies on the misuse of financial institutions, DNFBPs and VASPs*).
4. Information on compliance by financial institutions, DNFBPs and VASPs (e.g., *frequency of internal AML/CFT compliance review; nature of breaches identified and remedial actions taken or sanctions applied; frequency and quality of AML/CFT training; time taken to provide competent authorities with accurate and complete CDD information for AML/CFT purposes; accounts/relationships rejected due to incomplete CDD information; wire transfers rejected due to insufficient requisite information*).
5. Information on STR reporting and other information as required by national legislation (e.g., *number of STRs submitted, and the value of associated transactions; number and proportion of STRs from different sectors; the types, nature and trends in STR filings corresponding to ML/TF risks; average time taken to analyse the suspicious transaction before filing an STR*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

6. What are the measures in place to identify and deal with higher (and where relevant, lower) risk customers, business relationships, transactions, products and countries?
7. Does the manner in which AML/CFT measures are applied prevent the legitimate use of the formal financial system, and what measures are taken to promote financial inclusion?
8. To what extent do the CDD and enhanced or specific measures vary according to ML/TF risks across different sectors / types of institution, and individual institutions? What is the relative level of compliance between international financial groups and domestic institutions?
9. To what extent is there reliance on third parties for the CDD process and how well are the controls applied?
10. How well do financial institutions and groups, DNFBPs and VASPs ensure adequate access to information by the AML/CFT compliance function?
11. Do internal policies and controls of the financial institutions and groups, DNFBPs and VASPs enable timely review of: (i) complex or unusual transactions, (ii) potential STRs for reporting to the FIU, and (iii) potential false-positives? To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?

12. What are the measures and tools employed to assess risk, formulate and review policy responses, and institute appropriate risk mitigation and systems and controls for ML/TF risks?

13. How are AML/CFT policies and controls communicated to senior management and staff? What remedial actions and sanctions are taken by financial institutions, DNFBPs and VASPs when AML/CFT obligations are breached?

14. How well are financial institutions, DNFBPs and VASPs documenting their ML/TF risk assessments, and keeping them up to date?

15. Do financial institutions, DNFBPs and VASPs have adequate resources to implement AML/CFT policies and controls relative to their size, complexity, business activities and risk profile?

16. How well is feedback provided to assist financial institutions, DNFBPs and VASPs in detecting and reporting suspicious transactions?

Immediate Outcome 5	Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.

Characteristics of an effective system:

Measures are in place to:

- prevent legal persons and arrangements from being used for criminal purposes;
- make legal persons and arrangements sufficiently transparent; and
- ensure that accurate and up-to-date basic and beneficial ownership information is available on a timely basis.

Basic information is available publicly, and beneficial ownership information is available to competent authorities. Persons who breach these measures are subject to effective, proportionate and dissuasive sanctions. This results in legal persons and arrangements being unattractive for criminals to misuse for money laundering and terrorist financing.

This outcome relates primarily to Recommendations 24 and 25, and also elements of Recommendations 1, 10, 37 and 40.

Note to Assessors:

Assessors should also consider the relevant findings in relation to the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent to which competent authorities seek and are able to provide the appropriate assistance in relation to identifying and exchanging information (including beneficial ownership information) for legal persons and arrangements.

Core Issues to be considered in determining if the Outcome is being achieved

5.1. To what extent is the information on the creation and types of legal persons and arrangements in the country available publicly?

5.2. How well do the relevant competent authorities identify, assess and understand the vulnerabilities, and the extent to which legal persons created in the country can be, or are being misused for ML/TF?

5.3. How well has the country implemented measures to prevent the misuse of legal persons and arrangements for ML/TF purposes?

5.4. To what extent can relevant competent authorities obtain adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner?

5.5. To what extent can relevant competent authorities obtain adequate, accurate and current beneficial ownership information on legal arrangements, in a timely manner?

5.6. To what extent are effective, proportionate and dissuasive sanctions applied against persons who do not comply with the information requirements?

a) Examples of Information that could support conclusion on Core Issues

1. Contextual information on the types, forms and basic features of legal persons and arrangements in the jurisdiction.

2. Experiences of law enforcement and other relevant competent authorities (e.g., *level of sanctions imposed for breach of the information requirements; where and how basic and beneficial ownership information (including information on the settlor, trustee(s), protector and beneficiaries) is obtained; information used in supporting investigation*).

3. Typologies and examples of the misuse of legal persons and arrangements (e.g., *frequency with which criminal investigations find evidence of the country's legal persons and arrangements being used for ML/TF; legal persons misused for illegal activities dismantled or struck-off).*

4. Sources of basic and beneficial ownership information (e.g., *types of public information available to financial institutions and DNFBPs; types of information held in the company registry or by the company*).

5. Information on the role played by "gatekeepers" (e.g., *company service providers, accountants, legal professionals*) in the formation and administration of legal persons and arrangements.

6. Other information (e.g., *information on existence of legal arrangements; responses (positive and negative) to requests for basic or beneficial ownership information received from other countries; information on the monitoring of quality of assistance*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

7. What are the measures taken to enhance the transparency of legal persons (including dealing with bearer shares and share warrants, and nominee shareholders and directors) and arrangements?

8. How do relevant authorities ensure that accurate and up-to-date basic and beneficial ownership information on legal persons is maintained? Is the presence and accuracy of information monitored, tested/certified or verified?

9. To what extent is the time taken for legal persons to register changes to the required basic and beneficial ownership information adequate to ensure that the information is accurate and

up to date? Where applicable, to what extent are similar changes in legal arrangements registered in a timely manner?

10. To what extent can financial institutions and DNFBPs obtain accurate and up-to-date basic and beneficial ownership information on legal persons and arrangements? What is the extent of information that trustees disclose to financial institutions and DNFBPs?

11. Do the relevant authorities have adequate resources to implement the measures adequately?

Immediate Outcome 6	Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.

Characteristics of an effective system

A wide variety of financial intelligence and other relevant information is collected and used by competent authorities to investigate money laundering, associated predicate offences and terrorist financing. This delivers reliable, accurate, and up-to-date information; and the competent authorities have the resources and skills to use the information to conduct their analysis and financial investigations, to identify and trace the assets, and to develop operational analysis.

This outcome relates primarily to Recommendations 29 to 32 and also elements of Recommendations 1, 2, 4, 8, 9, 15, 34 and 40.

Note to Assessors:

1) This outcome includes the work that the FIU does to analyse STRs and other data; and the use by competent authorities of FIU products, other types of financial intelligence and other relevant information[99].

2) Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which FIUs and law enforcement agencies are able to, and do seek appropriate financial and law enforcement intelligence and other information from their foreign counterparts.

Core Issues to be considered in determining if the Outcome is being achieved

6.1. To what extent are financial intelligence and other relevant information accessed and used in investigations to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF?

[99] The sources include information derived from STRs, cross-border reports on currency and bearer negotiable movements, law enforcement intelligence; criminal records; supervisory and regulatory information; and information with company registries etc. Where applicable, it would also include reports on cash transactions, foreign currency transactions, wire transfers records, information from other government agencies including security agencies; tax authorities, asset registries, benefits agencies, NPOs authorities; and information which can be obtained through compulsory measures from financial institutions and DNFBPs including CDD information and transaction records, as well as information from open sources.

6.2. To what extent are the competent authorities receiving or requesting reports (e.g., STRs, reports on currency and bearer negotiable instruments) that contain relevant and accurate information that assists them to perform their duties?

6.3. To what extent is FIU analysis and dissemination supporting the operational needs of competent authorities?

6.4. To what extent do the FIU and other competent authorities co-operate and exchange information and financial intelligence? How securely do the FIU and competent authorities protect the confidentiality of the information they exchange or use?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences of law enforcement and other competent authorities (e.g., *types of financial intelligence and other information available; frequency with which they are used as investigative tools).*

2. Examples of the co-operation between FIUs and other competent authorities and use of financial intelligence (e.g., *statistics of financial intelligence disseminated/exchanged; cases where financial intelligence was used in investigation and prosecution of ML/TF and associated predicate offences, or in identifying and tracing assets*).

3. Information on STRs (e.g., *number of STRs/cases analysed; perception of quality of information disclosed in STRs; frequency with which competent authorities come across examples of unreported suspicious transactions; cases of tipping-off; see also Immediate Outcome 4 for information on STR reporting).*

4. Information on other financial intelligence and information *(*e.g., *number of currency and bearer negotiable instruments reports received, and analysed; types of information that law enforcement and other competent authorities receive or obtain/access from other authorities, financial institutions and DNFBPs).*

5. Other documents (e.g., *guidance on the use and reporting of STRs and other financial intelligence; typologies produced using financial intelligence*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

6. How well does the FIU access and use additional information to analyse and add value to STRs? How does the FIU ensure the rigour of its analytical assessments?

7. How well do competent authorities make use of the information contained in STRs and other financial intelligence to develop operational analysis?

8. To what extent does the FIU incorporate feedback from competent authorities, typologies and operational experience into its functions?

9. What are the mechanisms implemented to ensure full and timely co-operation between competent authorities, and from financial institutions, DNFBPs and other reporting entities to provide the relevant information? Are there any impediments to the access of information?

10. To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?

11. To what extent do the relevant competent authorities review and engage (including outreach by the FIU) reporting entities to enhance financial intelligence reporting?

12. Do the relevant authorities have adequate resources (including IT tools for data mining and analysis of financial intelligence and to protect its confidentiality) to perform its functions?

13. What are the measures implemented to ensure that the FIU has operational independence so that it is not subject to undue influence on AML/CFT matters?

Immediate Outcome 7	Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.

Characteristics of an effective system

Money laundering activities, and in particular major proceeds-generating offences, are investigated; offenders are successfully prosecuted; and the courts apply effective, proportionate and dissuasive sanctions to those convicted. This includes pursuing parallel financial investigations and cases where the associated predicate offences occur outside the country, and investigating and prosecuting stand-alone money laundering offences. The component parts of the systems (investigation, prosecution, conviction, and sanctions) are functioning coherently to mitigate the money laundering risks. Ultimately, the prospect of detection, conviction, and punishment dissuades potential criminals from carrying out proceeds generating crimes and money laundering.

This outcome relates primarily to Recommendations 3, 30 and 31, and also elements of Recommendations 1, 2, 15, 32, 37, 39 and 40.

Note to Assessors:

Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent to which law enforcement agencies are seeking appropriate assistance from their foreign counterparts in cross-border money laundering cases.

Core Issues to be considered in determining if the Outcome is being achieved

7.1. How well, and in what circumstances are potential cases of ML identified and investigated (including through parallel financial investigations)?

7.2. To what extent are the types of ML activity being investigated and prosecuted consistent with the country's threats and risk profile and national AML/CFT policies?

7.3. To what extent are different types of ML cases prosecuted (*e.g.,* foreign predicate offence, third-party laundering, stand-alone offence[100] etc.) and offenders convicted?

[100] **Third party money laundering** is the laundering of proceeds by a person who was not involved in the commission of the predicate offence. **Self-laundering** is the laundering of proceeds by a person who was involved in the commission of the predicate offence. **Stand-alone (or autonomous) money laundering** refers to the prosecution of ML offences independently, without also necessarily prosecuting the predicate offence. This could be particularly relevant inter alia i) when there is insufficient evidence of the particular predicate offence that gives rise to the criminal proceeds; or ii) in situations where there is a lack of territorial jurisdiction over the predicate offence. The proceeds may have been laundered by the defendant (self-laundering) or by a third party (third party ML).

7.4. To what extent are the sanctions applied against natural or legal persons convicted of ML offences effective, proportionate and dissuasive?

7.5. To what extent do countries apply other criminal justice measures in cases where a ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure a ML conviction? Such alternative measures should not diminish the importance of, or be a substitute for, prosecutions and convictions for ML offences.

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of investigations, prosecutions and convictions*(* e.g., *examples of cases rejected due to insufficient investigative evidence; what are the significant or complex ML cases that the country has investigated and prosecuted; examples of successful cases against domestic and transnational organised crime; cases where other criminal sanctions or measures are pursued instead of ML convictions).*

2. Information on ML investigations, prosecutions and convictions (e.g., *number of investigations and prosecutions for ML activity; proportion of cases leading to prosecution or brought to court; number or proportion of ML convictions relating to third party laundering, stand-alone offence, self-laundering, and foreign predicate offences; types of predicate crimes involved; level of sanctions imposed for ML offences; sanctions imposed for ML compared with those for other predicate offences).*

b) Examples of Specific Factors that could support the conclusions on Core Issues

3. What are the measures taken to identify, initiate and prioritise ML cases (at least in relation to all major proceeds-generating offences) for investigation (*e.g.,* focus between small and larger or complex cases, between domestic and foreign predicates etc.)?

4. To what extent, and how quickly, can competent authorities obtain or access relevant financial intelligence and other information required for ML investigations?

5. To what extent are joint or cooperative investigations (including the use of multi-disciplinary investigative units) and other investigative techniques (*e.g.,* postponing or waiving the arrest or seizure of money for the purpose of identifying persons involved) used in major proceeds generating offences?

6. How are ML cases prepared for timely prosecution and trial?

7. In what circumstances are decisions made not to proceed with prosecutions where there is indicative evidence of a ML offence?

8. To what extent are ML prosecutions: (i) linked to the prosecution of the predicate offence (including foreign predicate offences), or (ii) prosecuted as an autonomous offence?

9. How do the relevant authorities, taking into account the legal systems, interact with each other throughout the life-cycle of a ML case, from the initiation of an investigation, through gathering of evidence, referral to prosecutors and the decision to go to trial?

10. Are there other aspects of the investigative, prosecutorial or judicial process that impede or hinder ML prosecutions and sanctions?

11. Do the competent authorities have adequate resources (including financial investigation tools) to manage their work or address the ML risks adequately?

12. Are dedicated staff/units in place to investigate ML? Where resources are shared, how are ML investigations prioritised?

Immediate Outcome 8	Proceeds and instrumentalities of crime are confiscated.

Characteristics of an effective system

Criminals are deprived (through timely use of provisional and confiscation measures) of the proceeds and instrumentalities of their crimes (both domestic and foreign) or of property of an equivalent value. Confiscation includes proceeds recovered through criminal, civil or administrative processes; confiscation arising from false cross-border disclosures or declarations; and restitution to victims (through court proceedings). The country manages seized or confiscated assets, and repatriates or shares confiscated assets with other countries. Ultimately, this makes crime unprofitable and reduces both predicate crimes and money laundering.

This outcome relates primarily to Recommendations 1, 4, 32 and also elements of Recommendations 15, 30, 31, 37, 38, and 40.

Note to Assessors:

Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which law enforcement and prosecutorial agencies are seeking appropriate assistance from their foreign counterparts in relation to cross-border proceeds and instrumentalities of crime.

Core Issues to be considered in determining if the Outcome is being achieved

8.1. To what extent is confiscation of criminal proceeds, instrumentalities and property of equivalent value pursued as a policy objective?

8.2. How well are the competent authorities confiscating[101] (including repatriation, sharing and restitution) the proceeds and instrumentalities of crime, and property of an equivalent value, involving domestic and foreign predicate offences and proceeds which have been moved to other countries?

8.3. To what extent is confiscation regarding falsely / not declared or disclosed cross-border movements of currency and bearer negotiable instruments being addressed and applied as

[101] For the purposes of assessing the effectiveness of IO.8, full credit should be given for relevant use of the tax system, namely amounts recovered using tax assessment procedures that relate to the proceeds and instrumentalities of crime. The assessed country should ensure that any data provided is limited to tax recoveries that are linked to criminal proceeds/instrumentalities, or the figures should be appropriately caveated.

an effective, proportionate and dissuasive sanction by border/custom or other relevant authorities?

8.4. How well do the confiscation results reflect the assessments(s) of ML/TF risks and national AML/CFT policies and priorities?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of confiscation proceedings (e.g., *the most significant cases in the past; types of confiscation orders obtained by the country; trends indicating changes in methods by which proceeds of crime is being laundered).*

2. Information on confiscation (e.g., *number of criminal cases where confiscation is pursued; type of cases which involve confiscation; value of proceeds of crimes, instrumentalities or property of equivalent value confiscated, broken down by foreign or domestic offences, whether through criminal or civil procedures (including non-conviction-based confiscation); value of falsely / not declared or disclosed cross-border currency and bearer negotiable instruments confiscated; value or proportion of seized or frozen proceeds that is subject to confiscation; value or proportion of confiscation orders realised*).

3. Other relevant information (*e.g. value of criminal assets seized / frozen*; *amount of proceeds of crime restituted to victims, shared or repatriated).*

b) Examples of Specific Factors that could support the conclusions on Core Issues

4. What are the measures and approach adopted by competent authorities to target proceeds and instrumentalities of crime (including major proceeds-generating crimes and those that do not originate domestically or have flowed overseas)?

5. How do authorities decide, at the outset of a criminal investigation, to commence a financial investigation, with a view to confiscation?

6. How well are competent authorities identifying and tracing proceeds and instrumentalities of crimes or assets of equivalent value? How well are provisional measures (*e.g.,* freeze or seizures) used to prevent the flight or dissipation of assets?

7. What is the approach adopted by the country to detect and confiscate cross-border currency and bearer negotiable instruments that are suspected to relate to ML/TF and associated predicate offences or that are falsely / not declared or disclosed?

8. What are the measures adopted to preserve and manage the value of seized/confiscated assets?

9. Are there other aspects of the investigative, prosecutorial or judicial process that promote or hinder the identification, tracing and confiscation of proceeds and instrumentalities of crime or assets of equivalent value?

10. Do the relevant competent authorities have adequate resources to perform their functions adequately?

Immediate Outcome 9	Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.

Characteristics of an effective system

Terrorist financing activities are investigated; offenders are successfully prosecuted; and courts apply effective, proportionate and dissuasive sanctions to those convicted. When appropriate, terrorist financing is pursued as a distinct criminal activity and financial investigations are conducted to support counter terrorism investigations, with good co-ordination between relevant authorities. The components of the system (investigation, prosecution, conviction and sanctions) are functioning coherently to mitigate the terrorist financing risks. Ultimately, the prospect of detection, conviction and punishment deters terrorist financing activities.

This outcome relates primarily to Recommendations 5, 30, 31 and 39, and also elements of Recommendations 1, 2, 15, 32, 37 and 40.

Note to Assessors:

1) Assessors should be aware that some elements of this outcome may involve material of a sensitive nature (*e.g.,* information that is gathered for national security purposes) which countries may be reluctant or not able to make available to assessors.

2) Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which law enforcement and prosecutorial agencies are seeking appropriate assistance from their foreign counterparts in cross-border terrorist financing cases.

Core Issues to be considered in determining if the Outcome is being achieved

9.1. To what extent are the different types of TF activity (*e.g.,* collection, movement and use of funds or other assets) prosecuted and offenders convicted? Is this consistent with the country's TF risk profile?

9.2. How well are cases of TF identified, and investigated? To what extent do the investigations identify the specific role played by the terrorist financier?

9.3. To what extent is the investigation of TF integrated with, and used to support, national counter-terrorism strategies and investigations (*e.g.,* identification and designation of terrorists, terrorist organisations and terrorist support networks)?

9.4. To what extent are the sanctions or measures applied against natural and legal persons convicted of TF offences effective, proportionate and dissuasive?

9.5. To what extent is the objective of the outcome achieved by employing other criminal justice, regulatory or other measures to disrupt TF activities where it is not practicable to secure a TF conviction?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of TF investigations and prosecutions (e.g., *cases where TF investigations are used to support counter-terrorism investigations and prosecutions; significant cases where (foreign or domestic) terrorists and terrorist groups are targeted, prosecuted or disrupted; observed trends in TF levels and techniques; cases where other criminal sanctions or measures are pursued instead of TF convictions).*

2. Information on TF investigations, prosecutions and convictions (e.g., *number of TF investigations and prosecutions; proportion of cases leading to TF prosecution, type of TF prosecutions and convictions (*e.g., *distinct offences, foreign or domestic terrorists, financing of the travel of foreign terrorist fighters); level of sanctions imposed for TF offences; sanctions imposed for TF compared with those for other criminal activity; types and level of disruptive measures applied*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

3. What are the measures taken to identify, initiate and prioritise TF cases to ensure prompt investigation and action against major threats and to maximise disruption?

4. To what extent and how quickly can competent authorities obtain and access relevant financial intelligence and other information required for TF investigations and prosecutions?

5. What are the underlying considerations for decisions made not to proceed with prosecutions for a TF offence?

6. To what extent do the authorities apply specific action plans or strategies to deal with particular TF threats and trends? Is this consistent with the national AML/CFT policies, strategies and risks?

7. How well do law enforcement authorities, the FIU, counter-terrorism units and other security and intelligence agencies co-operate and co-ordinate their respective tasks associated with this outcome?

8. Are there other aspects of the investigative, prosecutorial or judicial process that impede or hinder TF prosecutions, sanctions or disruption?

9. Do the competent authorities have adequate resources (including financial investigation tools) to manage their work or address the TF risks adequately?

10. Are dedicated staff/units in place to investigate TF? Where resources are shared, how are TF investigations prioritised?

Immediate Outcome 10	Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.

Characteristics of an effective system

Terrorists, terrorist organisations and terrorist support networks are identified and deprived of the resources and means to finance or support terrorist activities and organisations. This includes proper implementation of targeted financial sanctions against persons and entities designated by the United Nations Security Council and under applicable national or regional sanctions regimes. The country also has a good understanding of the terrorist financing risks and takes appropriate and proportionate actions to mitigate those risks, including measures that prevent the raising and moving of funds through entities or methods which are at greatest risk of being misused by terrorists. Ultimately, this reduces terrorist financing flows, which would prevent terrorist acts.

This outcome relates primarily to Recommendations 1, 4, 6 and 8, and also elements of Recommendations 14, 15, 16, 30 to 32, 37, 38 and 40.

Note to Assessors:

Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome.

Core Issues to be considered in determining if the Outcome is being achieved

10.1. How well is the country implementing targeted financial sanctions pursuant to (i) UNSCR1267 and its successor resolutions, and (ii) UNSCR1373 (at the supra-national or national level, whether on the country's own motion or after examination, to give effect to the request of another country)?

10.2. To what extent, without disrupting or discouraging legitimate NPO activities, has the country applied focused and proportionate measures to such NPOs which the country has identified as being vulnerable to terrorist financing abuse, in line with the risk-based approach?

10.3. To what extent are terrorists, terrorist organisations and terrorist financiers deprived (whether through criminal, civil or administrative processes) of assets and instrumentalities related to TF activities?

10.4. To what extent are the above measures consistent with the overall TF risk profile?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences of law enforcement, FIU and counter terrorism authorities (e.g., *trends indicating that terrorist financiers are researching alternative methods for raising / transmitting funds;*

intelligence/source reporting indicating that terrorist organisations are having difficulty raising funds in the country).

2. Examples of interventions and confiscation (e.g., *significant cases where terrorists, terrorist organisations or terrorist financiers are prevented from raising, moving and using funds or their assets seized / confiscated; investigations and interventions in NPOs misused by terrorists).*

3. Information on targeted financial sanctions (e.g., *persons and accounts subject to targeted financial sanctions under UNSC or other designations; designations made (relating to UNSCR1373); assets frozen; transactions rejected; time taken to designate individuals; time taken to implement asset freeze following designation*).

4. Information on sustained outreach and targeted risk-based supervision and monitoring of NPOs that the country has identified as being at risk of terrorist financing abuse (*e.g. frequency of review and monitoring of such NPOs (including risk assessments); frequency of engagement and outreach (including guidance) to NPOs regarding CFT measures and trends; remedial measures and sanctions taken against NPOs*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What measures has the country adopted to ensure the proper implementation of targeted financial sanctions without delay? How are those designations and obligations communicated to financial institutions, DNFBPs, VASPs and the general public in a timely manner?

6. How well are the procedures and mechanisms implemented for (i) identifying targets for designation / listing, (ii) freezing / unfreezing, (iii) de-listing, and (iv) granting exemption? How well is the relevant information collected?

7. To what extent is the country utilising the tools provided by UNSCRs 1267 and 1373 to freeze and prevent the financial flows of terrorists?

8. How well do the systems for approving or licensing the use of assets by designated entities for authorised purposes comply with the requirements set out in the relevant UNSCRs (*e.g.,* UNSCR 1452 and any successor resolutions)?

9. What is the approach adopted by competent authorities to target terrorist assets? To what extent are assets tracing, financial investigations and provisional measures (*e.g.,* freezing and seizing) used to complement the approach?

10. To what extent are all four of the following elements being used to identify, prevent and combat terrorist financing abuse of NPOs: (a) sustained outreach, (b) targeted risk-based supervision or monitoring, (c) effective investigation and information gathering, and (d) effective mechanisms for international cooperation. To what extent are the measures being applied focused and proportionate and in line with the risk-based approach such that NPOs are protected from terrorist financing abuse and legitimate charitable activities are not disrupted or discouraged?

11. To what extent are appropriate investigative, criminal, civil or administrative actions, co-operation and coordination mechanisms applied to NPOs suspected of being exploited by, or

actively supporting terrorist activity or terrorist organisations? Do the appropriate authorities have adequate resources to perform their outreach / supervision / monitoring / investigation duties effectively?

12. How well do NPOs understand their vulnerabilities and comply with the measures to protect themselves from the threat of terrorist abuse?

13. Are there other aspects of the investigative, prosecutorial or judicial process that promote or hinder the identification, tracing and deprivation of assets and instrumentalities related to terrorists, terrorist organisations or terrorist financiers?

14. Do the relevant competent authorities have adequate resources to manage their work or address the terrorist financing risks adequately

15. Where resources are shared, how are terrorist financing related activities prioritised?

Immediate Outcome 11	Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

Characteristics of an effective system

Persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD.

This outcome relates to Recommendation 7 and elements of Recommendations 2 and 15.

Core Issues to be considered in determining if the Outcome is being achieved

11.1. How well is the country implementing, without delay, targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation?

11.2. To what extent are the funds or other assets of designated persons and entities (and those acting on their behalf or at their direction) identified and such persons and entities prevented from operating or from executing financial transactions related to proliferation?

11.3. To what extent do financial institutions, DNFBPs and VASPs comply with, and understand their obligations regarding targeted financial sanctions relating to financing of proliferation?

11.4. How well are relevant competent authorities monitoring and ensuring compliance by financial institutions, DNFBPs and VASPs with their obligations regarding targeted financial sanctions relating to financing of proliferation?

a) Examples of Information that could support the conclusions on Core Issues

1. Examples of investigations and intervention relating to financing of proliferation (e.g., *investigations into breaches of sanctions; significant cases in which country has taken enforcement actions (*e.g., *freezing or seizures) or provided assistance).*

2. Information on targeted financial sanctions relating to financing of proliferation (e.g., *accounts of individuals and entities subject to targeted financial sanctions; value of frozen assets and property; time taken to designate persons and entities; time taken to freeze assets and property of individuals and entities following their designation by the UNSC*).

3. Monitoring and other relevant information relating to financing of proliferation (*e.g., frequency of review and monitoring of financial institutions, DNFBPs and VASPs for compliance with targeted financial sanctions; frequency of engagement and outreach; guidance documents; level of sanctions applied on financial institutions, DNFBPs* and VASPs *for breaches*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

4. What measures has the country adopted to ensure the proper implementation of targeted financial sanctions relating to financing of proliferation without delay? How are these designations and obligations communicated to relevant sectors in a timely manner?

5. Where relevant, how well are the procedures implemented for (i) designation / listing, (ii) freezing / unfreezing, (iii) de-listing, and (iv) granting exemption? To what extent do they comply with the UNSCR requirements?

6. How well do the systems and mechanisms for managing frozen assets and licensing the use of assets by designated individuals and entities for authorised purposes, safeguard human rights and prevent the misuse of funds?

7. What mechanisms are used to prevent the evasion of sanctions? Do relevant competent authorities provide financial institutions, DNFBPs and VASPs with other guidance or specific feedback?

8. To what extent would the relevant competent authorities be able to obtain accurate basic and beneficial ownership information on legal persons (*e.g.,* front companies), when investigating offences or breaches concerning the UNSCRs relating financing of proliferation?

9. To what extent are the relevant competent authorities exchanging intelligence and other information for investigations of violations and breaches of targeted financial sanctions in relation to financing of proliferation, as per the relevant UNSCRs?

10. Do the relevant competent authorities have adequate resources to manage their work or address the financing of proliferation risks adequately?

ANNEX I

SUPRA-NATIONAL ASSESSMENT

[Annex to be finalised]

ANNEX II

MUTUAL EVALUATION REPORT TEMPLATE

Notes for Assessors:

This template should be used as the basis for preparing Mutual Evaluation Reports (MERs) for evaluations conducted using the FATF's 2013 Methodology. It sets out the structure of the MER, and the information and conclusions which should be included in each section.

The template incorporates guidance to assessors on how the MER should be written, including what information should be included, and the way analysis and conclusions should be presented. This guidance is clearly indicated in grey shaded text (like this section). It should not appear in the final MER. Text which appears in unshaded script (including chapter and section headings and pro-forma paragraphs) should be included in the final report (with any square brackets completed as necessary).

Assessors should note that a completed MER is expected to be 100 pages or less (together with a technical annex of 60 pages or less). There is no predetermined limit to the length of each chapter, and assessors may decide to devote more, or less, attention to any specific issue, as the country's situation requires. Nevertheless, assessors should ensure the MER does not become excessively long, and should be prepared to edit their analysis as necessary. In order to ensure the right balance in the final report, assessors should aim to summarise technical compliance with each Recommendation in one or two paragraphs, totalling a maximum of half a page. Assessors may be very brief on issues where there is little or no substance to report (e.g. a single sentence description of technical compliance would be sufficient for Recommendations rated "compliant").

The Executive Summary is intended to serve as the basis for Plenary discussion of each Mutual Evaluation, and to provide clear conclusions and recommendations for ministers, legislators, and other policymakers in the assessed country. It is therefore important that it does not exceed five pages, and that assessors follow the guidance in that section on the selection and presentation of issues.

Assessors are urged to include statistics and case studies where relevant. These should be provided in the format shown at the end of the template.

EXECUTIVE SUMMARY

1. This report summarises the AML/CFT measures in place in [name of assessed country] as at the date of the on-site visit [date]. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of [country]'s AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

a)

b) Assessors should provide a short summary of the key findings, both positive and negative, taking into account the country's risk profile and AML/CFT regime. The focus should be on 5-7 points raised in the report rather than a summary of each and every single IO or chapter.

Risks and General Situation

2.

3. This section should give a brief summary (1-2 paragraphs) of the country's ML/TF risk situation and context – focusing in particular on the country's exposure to domestic and international ML/TF risks, and identifying the issues and sectors that present the greatest risks. Assessors should note any areas where they have identified material risks which were not considered in the country's own risk assessment, or where they consider the level of risk to be significantly different.

Overall Level of Compliance and Effectiveness

4.

5. Assessors should give a very brief overview of the AML/CFT situation in the country, based on the level of both compliance and effectiveness.

6. In the sections below, assessors should briefly summarise, the overall level of effectiveness of the country's AML/CFT system in each thematic area as well as the overall level of technical compliance with the FATF Recommendations, noting any areas of particular strength or weakness. Assessors should also note the progress since the last MER, highlighting any significant changes and flagging any key issues that remain outstanding from the previous assessment.

Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

7.

8. Assessors should set out their main findings in more details and for each chapter of the main report as structured in sub-sections below. Any relevant factors of importance would need to be highlighted such as high-risk or significant contextual or other issues for the country; areas where the country performs particularly well both on effectiveness and technical compliance, highlighting unusual or innovative mechanisms; significant failures of effectiveness; and important areas of technical

non-compliance. Each section should contain a brief summary of the assessor's conclusions on the overall level of compliance and effectiveness – including highlighting key findings for each relevant IOs- and any actions required. The description should include sufficient detail for readers to understand assessors' conclusions and the main issues/positive features. However, it should not include a full analysis, and should not defend assessors' conclusions or anticipate and rebut objections. Any additional information should be set out in the main body of the report, rather than in the executive summary.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

9.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

10.

Preventive measures (Chapter 5; IO.4; R.9–23)

11.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

12.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

13.

International cooperation (Chapter 8; IO.2; R.36–40)

14.

Priority Actions

a)

b)

The report should set out a series of priority actions that the country should take:

Assessors should set out the priority actions which the country should take to improve its AML/CFT system. This can include measures to improve effectiveness; to address technical compliance problems; or to tackle structural or cross-cutting issues.

Assessors should indicate briefly what action is required and the reason why it should be prioritised (e.g. that it is a fundamental building block of the AML/CFT system).

The actions identified will normally correspond to the issues set out in the key findings section above – but need not always do so, e.g. if assessors identify scope for a single action to address a number of deficiencies which are not included in the key findings.

The priority actions should normally take up one page or less.

If assessors identify actions which offer the opportunity to make a significant improvement quickly or at a relatively low cost, these should also be highlighted in this section

Effectiveness & Technical Compliance Ratings

Table 1. Effectiveness Ratings

IO.1	IO.2	IO.3	IO.4	IO.5	IO.6	IO.7	IO.8	IO.9	IO.10	IO.11

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

Table 2. Technical Compliance Ratings

R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10
R.11	**R.12**	**R.13**	**R.14**	**R.15**	**R.16**	**R.17**	**R.18**	**R.19**	**R.20**
R.21	**R.22**	**R.23**	**R.24**	**R.25**	**R.26**	**R.27**	**R.28**	**R.29**	**R.30**
R.31	**R.32**	**R.33**	**R.34**	**R.35**	**R.36**	**R.37**	**R.38**	**R.39**	**R.40**

Note: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of theAML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from [dates].

The evaluation was conducted by an assessment team consisting of: [list names and agencies of examiners and their role *e.g.* legal expert] with the support from the FATF Secretariat of [list names from the FATF Secretariat]. The report was reviewed by [list names of reviewers].

[Country] previously underwent a FATF Mutual Evaluation in [year], conducted according to the 2004 FATF Methodology. The [date] evaluation [*and [date] follow-up report*] has been published and is available at [web address].

That Mutual Evaluation concluded that the country was compliant with [...] Recommendations; largely compliant with [...]; partially compliant with [...]; and non-compliant with [...]. [Country] was rated compliant or largely compliant with ... of the 16 Core and Key Recommendations.

[Note the country's status in the follow-up process – including whether and when the country entered and exited follow-up, and the basis on which this was done (*i.e.* LC with all Core and Key Recommendations, or with outstanding issues). Assessors should note any core or key Recommendations which are not yet considered equivalent to an LC.]

CHAPTER 1. ML/TF RISKS AND CONTEXT

15.

16. This section should begin with a very brief description of the country's general situation: its size, territorial makeup, population, GDP, and constitutional structure.

17. This section should note any territorial or jurisdictional issues affecting the evaluation, (*e.g.* if the MER includes assessment of territories or regions with different AML/CFT regimes, or if the country is part of a supranational jurisdiction).

18. For any of the information contained in sub-sections 1.1-1.4, assessors should provide a balanced picture where possible thus covering, for example, higher risk or lower risk areas, strengths and weaknesses.

1.1 ML/TF Risks and Scoping of Higher-Risk Issues

1.1.1 Overview of ML/TF Risks

19.

20. This section should set out the ML and TF threats and risks faced by the country. It should include the main underlying threats, drawing on the country's risk assessment and on other relevant information, as set out in the introduction to the methodology. Particular points to cover include:

- the underlying levels of proceeds generating crime in the country, and its nature;
- the country's exposure to cross-border illicit flows (related to crimes in other countries) – including any significant potential role as a transit route for illicit goods or funds;
- any available information on the country's exposure to terrorist financing threats (including the existence of terrorist groups active in the country; or the use of the country as a source of funds or recruits for terrorist groups active in other countries) and financing of proliferation; and
- the ML/TF risks, taking into account vulnerabilities (including vulnerabilities posed by virtual asset activity) and consequences.

1.1.2 Country's risk assessment & Scoping of Higher Risk Issues

21.

22. The above should be framed in the context of the country's understanding and assessment of its own risks. Assessors should set out the arrangements for the preparation of the National Risk Assessment(s), including how the risk assessment(s) was commissioned, how it is structured (e.g. as a single assessment or on the basis of regional/sectoral assessments), how it was prepared and the type of information used in conducting the risk assessment(s), as well as assessors' conclusions on the adequacy of the process. Assessors should set out their views regarding the reasonableness of the conclusions of the assessment(s), as well as any points on which they consider the conclusions were not reasonable, and any additional risks or risk factors which they consider significant, but which were not adequately taken into account in the assessment. If assessors identify such additional risks, they should note

the basis for their judgement, and the credible or reliable sources of information supporting this. In addition assessors should summarise the scoping exercise conducted prior to the onsite in order to identify higher and lower risk issues to be considered in more detail in the course of the assessment. This should include setting out the reasons why they consider each issue to be higher or lower risk, and noting how additional attention was given to these issues in the course of the evaluation.

1.2 Materiality

23.

24. This section should set out the size and general makeup of the economy, and of the financial sector, DNFBP and VASP sectors. It should note the relative importance of different types of financial institution, DNFBP and VASP and their activity, the international role of the country's financial, DNFBP and VASP sectors (*e.g.* if the country is a regional financial centre, an international financial centre, a centre for company formation and registration), and highlight particularly significant features of the country's financial, DNFBP and VASP sectors. This section should also note any other significant factors affecting materiality, as set out in paragraph 8 of the introduction to the Methodology. It should be a brief summary.

1.3 Structural Elements

25.

26. Assessors should note whether the main structural elements required for an effective AML/CFT system are present in the country (as set out in paragraph 9 of the introduction to the Methodology).

27. If there are serious concerns that any of the structural elements which underpin an effective AML/CFT system is weak or absent, assessors should highlight those concerns in this section. Note that assessors are not expected to reach a general conclusion about the extent to which such factors are present.

1.4 Background and other Contextual Factors

28.

29. Assessors should note domestic and international contextual factors that might significantly influence the effectiveness of the country's AML/CFT measures. This could include such factors as the maturity and sophistication of the AML/CFT regime and the institutions which implement it, or issues of corruption or financial exclusion. All other background information necessary for the understanding of the effectiveness analysis in the main chapters of the report should be incorporated here as well including the following:

1.4.1 AML/CFT strategy

30.

31. This section should set out the main policies and objectives of the Government for combating money laundering and terrorist financing. It should describe the government's priorities and objectives in these areas, noting where there are also

wider policy objectives (such as financial inclusion) which affect the AML/CFT strategy. Any relevant policies and objectives for combating the financing of proliferation should also be set out in this section.

1.4.2. Legal & institutional framework

32.

33. Assessors should give a brief overview of which ministries, agencies, and authorities are responsible for formulating and implementing the government's AML/CFT and proliferation financing policies. Assessors should briefly describe the principal role and responsibilities of each body involved in the AML/CFT strategy, as well as noting the bodies responsible for combating the financing of proliferation. Assessors should indicate any significant changes since the last MER to the institutional framework, including the rationale for those changes. This section should also set out the country's legal framework for AML/CFT and proliferation financing in a brief summary form. Detailed description and analysis of each element is not necessary – this should be included in the technical annex. Assessors should describe the co-operation and coordination mechanisms used by the country to assist the development of AML/CFT policies, and policies for combating the financing of proliferation.

1.4.3 Financial sector, DNFBPs and VASPs

34.

35. In this section, assessors should describe the size and makeup of the financial sector, DNFBP and VASP sectors. The section should note the relative importance of different types of financial institutions and activity, DNFBPs and generic types of virtual asset activities and providers primarily being used in the country. It is important that assessors explain their weighting of the relative importance of the different types of financial institutions, DNFBPs and VASPs to ensure consistent weighting throughout the MER, particularly when assessing IO.3 and IO.4. This is important because the risks, materiality and context varies widely from country to country (e.g. in some countries, a particular type of DNFBP such as TCSPs or casinos may be as (or almost as) important as the banking sector which means that weak supervision or weak preventive measures in that sector would be weighted much more heavily in IO.3 and IO.4 than in countries where such sectors are of lesser importance).

36. Assessors may explain how they have weighted the different sectors, in general terms (e.g. by explaining which sectors were weighted most important, highly important, moderately important or less important) rather than trying to rank each sector's prevalence individually (e.g. 1, 2, 3, 4, 5, 6, 7, 8…) which would be overly granular and a rather artificial distinction given the many different types of financial institutions, DNFBPs and VASPs that are subject to the FATF Recommendations.

37. In this section, the assessors should also describe the international role of the country's financial sector – *e.g.* if the country is a regional financial centre, an international financial centre, or a centre for company formation and registration, and should highlight particularly significant or important features of the country's financial, DNFBP and VASP sectors.

38. They should also summarise the types and key features of financial institutions, DNFBPs and VASPs which exist in the country, and the numbers of each type of

institution, as well as some information relating to the materiality of the sector and the institutions within it. Tables may be used in order to summarise the information.

1.4.4 Preventive measures

39.

40. This section should set out the legal (or other enforceable) instruments through which they are applied, and the scope of such obligations. If assessors identify any problems regarding the scope of AML/CFT obligations, they should briefly identify such issues in this section. If countries have exempted specific sectors or activities from the requirements, these exemptions should be noted in this section. Assessors should indicate whether such exemptions meet the criteria set out in R.1, and whether they consider the exemptions justified on the basis of the country's ML/TF risk assessment(s). This section should also note cases where countries have decided, on the basis of risk, to require AML/CFT preventive measures to be applied by additional sectors which are normally outside the scope of the FATF Recommendations.

1.4.5 Legal persons and arrangements

41.

42. Assessors should briefly describe the types of legal persons and legal arrangements that can be established or created in the country and relevant from an AML/CFT perspective. Basic characteristics of these should be provided as well as their numbers and their significance within the country and in financial and DNFBP sectors. Tables may be used in order to summarise the information. As per sub-section (c), the international elements should be covered in particular the extent to which the country acts as an international centre for the creation or administration of legal persons or arrangements (even if only as a source-of-law jurisdiction); and the extent to which legal persons and arrangements created in another jurisdiction (or under the law of another jurisdiction) hold assets or used in the country.

1.4.6 Supervisory arrangements[102]

43.

44. Assessors should set out the institutional arrangements for supervision and oversight of financial institutions, DNFBPs and VASPs, including the roles and responsibilities of regulators, supervisors and SRBs; their general powers and resources. Similarly, this section should also note the institutional framework for legal persons and arrangements, including the authorities (if any) with responsibility for the creation, registration, and supervision of legal persons and arrangements.

1.4.7 International Cooperation

45.

102 Assessors should describe the supervisory arrangements in place for financial institutions, DNFBPs and VASPs.

46. Assessors should briefly summarise the international ML/TF risks and threats faced by the country, including the potential use of the country to launder proceeds of crime in other countries and vice-versa. To the extent possible, assessors should identify the country's most significant international partners with respect to ML/TF issues. This section should also note any institutional framework for international cooperation e.g. a Central Authority for MLA.

Table 1.1. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 1.1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Recommended Actions

a) This section should set out a targeted and prioritised set of recommendations on how the country should improve its level of effectiveness and its level of compliance with the FATF Recommendations. The section should include assessors' recommendations regarding the Immediate Outcomes and Recommendations covered in this chapter of the MER. Assessors will therefore need to consider a range of Outcomes and Recommendations, and actions aimed at addressing both technical deficiencies and practical issues of implementation or effectiveness, and decide which actions should be prioritised.

b) Assessors should clearly indicate which Recommendation(s) or Outcome(s) each recommended action is intended to address. Assessors should follow the same general approach when making recommendations in other chapters of the MER.

47. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.

2.2 Immediate Outcome 1 (Risk, Policy and Coordination)

48. This section should set out assessors' analysis of Immediate Outcome 1. The first paragraph(s) should note any general considerations regarding the country's risks and context which affect the assessment.

49. This section should also summarise assessors' general impression of whether the country appears to exhibit the characteristics of an effective system.

50. Assessors should cover each of the Core Issues in their analysis. Assessors have some flexibility about how they organise the analysis in this section. For some immediate

outcomes, it may be appropriate to consider each of the core issues in turn. For others (e.g. I.O.4) it may be better to set out the analysis sector-by-sector; or (e.g. for I.O.7) to proceed step-by-step with the analysis of each element of the process covered by the Outcome. Whichever approach assessors take to organising their analysis, they should ensure that they consider each of the core issues, ***and should highlight any general conclusions they reach on them***. Assessors are required to resort to sub-headings to structure their analysis and clearly sign-post how core issues have been addressed. This does not preclude the use of additional sub-headings where necessary or to indicate that a particular Core Issue is not applicable in a particular country (and why). In the case of IO1, this includes the suggested sub-headings below.

51. Examples of sub-headings for other IOs are provided in this template. Assessors still retain full flexibility to amend and order these as most benefit their analysis and the overall report. Similarly, assessors may add or delete sub-headings as they see fit and in line with the specific circumstances of the assessed country. In all cases sub-headings should be neutral and not provide any qualitative comment as to how the country is performing on a given IO. Assessors should note the main sources of information and evidence used (e.g. the sources noted in sections (a) and (b) of the Immediate Outcome). Assessors are not required to use all the information noted in the methodology – but should set out here the information and evidence which has a material influence on their conclusion. Assessors should also note in their analysis any technical compliance issues which influence the level of effectiveness.

2.2.1 Country's understanding of its ML/TF risks

52.

2.2.2 National policies to address identified ML/TF risks

53.

2.2.3 Exemptions, enhanced and simplified measures

54.

2.2.4 Objectives and activities of competent authorities

55.

2.2.5 National coordination and cooperation

56.

2.2.6 Private sector's awareness of risks

57.

Overall Conclusion on IO.1

58. [Weighting and conclusion]

59. [Evaluated country] is rated as having a [rating] level of effectiveness for IO.1.

60. At the end of this section, assessor***s should indicate the effectiveness rating for the Immediate Outcome***. When deciding on the overall level of effectiveness, assessors should take into account: (a) the core issues, (b) any relevant technical compliance issues/deficiencies; (c) risks and contextual factors; and (d) the level of effectiveness in other Immediate Outcomes that are relevant. Assessors should briefly explain their conclusion on the appropriate effectiveness rating. They should be explicit about the weight and importance they attach to the elements taken into account. The conclusion should not duplicate the Key Findings section at the beginning of each chapter and should be, ideally, not more than one or two paragraphs long.

61. Assessors should follow the same general approach when setting out their analysis of effectiveness for all other outcomes.

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Table 2.1. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 2.1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1 Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Recommended Actions

a)

b) Assessors should list all the main corrective actions required for the country to improve its level of effectiveness and technical compliance in a targeted and prioritised way. Assessors should clearly indicate which IO/REC the recommended actions relate to.

62. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

3.2 Immediate Outcome 6 (Financial Intelligence ML/TF)

63. This Immediate Outcome relates to both money laundering and the financing of terrorism. Assessors should note any issues which relate specifically to either ML or TF. Sub-headings related to core issues could include:

3.2.1. Use of financial intelligence and other information

64.

3.2.2. STRs received and requested by competent authorities

65.

3.2.3. Operational needs supported by FIU analysis and dissemination

66.

3.2.4. Cooperation and exchange of information/financial intelligence

67.

Overall conclusion on IO.6

68. [Weighting and conclusion: See IO.1 for instructions]

69. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.6.**

3.3 Immediate Outcome 7 (ML investigation and prosecution)

3.3.1. ML identification and investigation

70.

3.3.2. Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

71.

3.3.3. Types of ML cases pursued

72.

3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions

73.

3.3.5. Use of alternative measures

74.

Overall conclusion on IO.7

75. [Weighting and conclusion: See IO.1 for instructions]

76. [Evaluated country] is rated as having a [rating] level of effectiveness for IO.7.

3.4 Immediate Outcome 8 (Confiscation)

3.4.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

77.

3.4.2. Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

78.

3.4.3. Confiscation of falsely or undeclared cross-border transaction of currency/BNI

79.

3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

80.

Overall conclusion on IO.8

81. [Weighting and conclusion: See IO.1 for instructions]
82. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.8.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Table 3.1. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 3.1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Recommended Actions

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

83. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

4.2. Immediate Outcome 9 (TF investigation and prosecution)

4.2.1. Prosecution/conviction of types of TF activity consistent with the country's risk-profile

84.

4.2.2. TF identification and investigation

85.

4.2.3. TF investigation integrated with –and supportive of- national strategies

86.

4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions

87.

4.2.5. Alternative measures used where TF conviction is not possible (e.g. disruption)

88.

Overall conclusions on IO.9

89. [Weighting and conclusion: See IO.1 for instructions]
90. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.9.**

4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

4.3.1. Implementation of targeted financial sanctions for TF without delay

91.

4.3.2. Targeted approach, outreach and oversight of at-risk non-profit organisations

92.

4.3.3. Deprivation of TF assets and instrumentalities

93.

4.3.4. Consistency of measures with overall TF risk profile

94.

Overall conclusions on IO.10

95. [Weighting and conclusion: See IO.1 for instructions]
96. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.10**.

4.4. Immediate Outcome 11 (PF financial sanctions)

4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay

97.

4.4.2. Identification of assets and funds held by designated persons/entities and prohibitions

98.

4.4.3. FIs and DNFBPs' understanding of and compliance with obligations

99.

4.4.4. Competent authorities ensuring and monitoring compliance

100.

Overall conclusion on IO.11

101. [Weighting and conclusion: See IO.1 for instructions]

102. [Evaluated country] is rated as having a [rating] level of effectiveness for IO.11.

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Table 4.1. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 4.1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!!. Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

CHAPTER 5. PREVENTIVE MEASURES

5.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Recommended Actions

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

103. The relevant Immediate Outcome considered and assessed in this chapter is IO.4[103]. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

5.2. Immediate Outcome 4 (Preventive Measures) [104]

5.2.1. Understanding of ML/TF risks and AML/CFT obligations

104.

[103] When assessing effectiveness under Immediate Outcome 4, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of Financial Institutions, DNFBPs and VASPs, as required in the instructions under that heading in the Methodology.

[104] The first paragraph should give a short summary of what relative importance assessors have given to the different types of financial institutions, designated non-financial businesses and professions and VASPs, taking into account the risk, context and materiality of the country being assessed. This should be supplemented by a cross-reference to the more detailed information in Chapter One on how each sector has been weighted (based on risk, context and materiality) (as required in the instructions under that heading in the Methodology).

5.2.2. Application of risk mitigating measures

105.

5.2.3. Application of CDD and record-keeping requirements

106.

5.2.4. Application of EDD measures

107.

5.2.5. Reporting obligations and tipping off

108.

5.2.6. Internal controls and legal/regulatory requirements impending implementation

109.

Overall conclusions on IO.4

110. [Weighting and conclusion]

111. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.4.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Table 5.1. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 5.1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

CHAPTER 6. SUPERVISION

6.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Recommended Actions

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

112. The relevant Immediate Outcome considered and assessed in this chapter is IO.3[105]. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

6.2. Immediate Outcome 3 (Supervision) [106]

6.2.1. Licensing, registration and controls preventing criminals and associates from entering the market

113.

[105] When assessing effectiveness under Immediate Outcome 3, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of Financial Institutions, DNFBPs and VASPs, as required in the instructions under that heading in the Methodology.

[106] The first paragraph should give a short summary of what relative importance assessors have given to the different types of financial institutions, designated non-financial businesses and professions and VASPs, taking into account the risk, context and materiality of the country being assessed. This should be supplemented by a cross-reference to the more detailed information in Chapter One on how each sector has been weighted (based on risk, context and materiality) (as required in the instructions under that heading in the Methodology).

6.2.2. Supervisors' understanding and identification of ML/TF risks

114.

6.2.3. Risk-based supervision of compliance with AML/CFT requirements

115.

6.2.4. Remedial actions and effective, proportionate, and dissuasive sanctions

116.

6.2.5. Impact of supervisory actions on compliance

117.

6.2.6. Promoting a clear understanding of AML/CFT obligations and ML/TF risks

118.

Overall conclusion on IO.3

119. [Weighting and conclusion]

120. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.3.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Table 6.1. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 6.1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

7.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Recommended Actions

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

121. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40.[107]

7.2. Immediate Outcome 5 (Legal Persons and Arrangements)

7.2.1. Public availability of information on the creation and types of legal persons and arrangements

122.

7.2.2. Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

123.

[107] The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

7.2.3. Mitigating measures to prevent the misuse of legal persons and arrangements

124.

7.2.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

125.

7.2.5. Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

126.

7.2.6. Effectiveness, proportionality and dissuasiveness of sanctions

127.

Overall conclusion on IO.5

128. [Weighting and conclusion: See IO.1 for instructions]

129. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.5.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Table 7.1. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 7.1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

CHAPTER 8. INTERNATIONAL COOPERATION

8.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Recommended Actions

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

130. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40 and elements of R.9, 15, 24, 25 and 32.

8.2. Immediate Outcome 2 (International Cooperation)

8.2.1. Providing constructive and timely MLA and extradition

131.

8.2.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

132.

8.2.3. Seeking other forms of international cooperation for AML/CFT purposes

133.

8.2.4. Providing other forms international cooperation for AML/CFT purposes

134.

8.2.5. International exchange of basic and beneficial ownership information of legal persons and arrangements

135.

Overall conclusions on IO.2

136. [Weighting and conclusion: See IO.1 for instructions]

137. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.2.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Table 8.2. <Sample table>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Box 8.2. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

ANNEX A. TECHNICAL COMPLIANCE ANNEX

1. This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.
2. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in [date]. This report is available from [link].

Recommendation 1 – Assessing risks and applying a risk-based approach

For each Recommendation, an opening paragraph should set out the issues on which new analysis is needed, and the issues where earlier analysis will be referred-to. This should include:

- the rating given in the previous MER, where applicable, and the main deficiencies identified;
- any conclusions reached in the follow-up process about whether the country has addressed its deficiencies;
- new FATF requirements, relative to the 2004 methodology; and
- the main changes to the relevant laws, regulations, and other elements in the country.

Criterion 1.1 – (Met / Mostly met / Partly met / Not met)

Each of the criteria should be reviewed, normally in a single paragraph.

If one or more criteria have been considered previously and the relevant laws, enforceable means, or other elements are unchanged, assessors should not repeat the previous analysis. Instead, they should summarise the conclusions, and include a reference to the report where the detailed analysis is set out (including paragraph numbers). Such references should only be made to MERs, FSAPs, or exit-from-follow-up reports which are publicly available; were analysed, considered, and adopted by an assessment body; and if assessors consider the analysis and conclusion were correct.

For each criterion, and prior to the narrative, the assessment team should set out in parenthesis whether the country is meeting FATF requirements. These sub-ratings will ultimately be removed before publication but will guide discussions ahead of and during the Plenary.

Criterion 1.2 – (Met / Mostly met / Partly met / Not met)

Assessors should include only their analysis of whether the criterion is met. General descriptions of the country's situation, context, or of the legal and institutional framework should be included in the main report, and not in this annex (though assessors may cross-reference any relevant points in the main report).

Assessors have flexibility to devote more space to their analysis where necessary, particularly to complex criteria or criteria which apply to a number of different sectors. In such cases, it may be helpful to set out their analysis in the form of a table. However, assessors should remember that the overall length of this technical annex should normally be limited to a maximum of 60 pages.

Weighting and Conclusion

Assessors should set out their conclusion on the appropriate technical compliance rating, and the reasoning for this. They should be explicit about the importance they attach to each of the criteria (including with reference to the country's risk and context, as set out in the main MER). **The rating should be stated in bold at the end of the paragraph.**

Recommendation 2 - National Cooperation and Coordination

Criterion 2.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 3 - Money laundering offence

Criterion 3.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 4 - Confiscation and provisional measures

Criterion 4.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 5 - Terrorist financing offence

Criterion 5.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

Criterion 6.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 7 – Targeted financial sanctions related to proliferation

Criterion 7.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 8 – Non-profit organisations

Criterion 8.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 9 – Financial institution secrecy laws

Criterion 9.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 10 – Customer due diligence

Criterion 10.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 11 – Record-keeping

Criterion 11.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 12 – Politically exposed persons

Criterion 12.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 13 – Correspondent banking

Criterion 13.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 14 – Money or value transfer services

Criterion 14.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 15 – New technologies

Criterion 15.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 16 – Wire transfers

Criterion 16.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 17 – Reliance on third parties

Criterion 17.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 18 – Internal controls and foreign branches and subsidiaries

Criterion 18.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 19 – Higher-risk countries

Criterion 19.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 20 – Reporting of suspicious transaction

Criterion 20.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 21 – Tipping-off and confidentiality

Criterion 21.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 22 – DNFBPs: Customer due diligence

Criterion 22.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 23 – DNFBPs: Other measures

Criterion 23.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 24 – Transparency and beneficial ownership of legal persons

Criterion 24.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Criterion 25.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 26 – Regulation and supervision of financial institutions

Criterion 26.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 27 – Powers of supervisors

Criterion 27.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 28 – Regulation and supervision of DNFBPs

Criterion 28.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 29 - Financial intelligence units

Criterion 29.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Criterion 30.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 31 - Powers of law enforcement and investigative authorities

Criterion 31.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 32 – Cash Couriers

Criterion 32.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 33 – Statistics

Criterion 33.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 34 – Guidance and feedback

Criterion 34.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 35 – Sanctions

Criterion 35.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 36 – International instruments

Criterion 36.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 37 - Mutual legal assistance

Criterion 37.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 38 – Mutual legal assistance: freezing and confiscation

Criterion 38.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 39 – Extradition

Criterion 39.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

Recommendation 40 – Other forms of international cooperation

Criterion 40.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

Annex Table 1. <!!Type the title here!!>

<!!Type the subtitle here. If you do not need a subtitle, please delete this line.!!>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			
<!!Table Row Heading (Alt+W)!!>	<!!Table Cell (Alt+E)!!>			

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

Annex Box 1. <Sample Case Study box (enter title here)>

<!!Box heading - If you do not need a box heading, please delete this line.!!>

<!! Do not forget to delete or replace this text.!!>

<!!Box heading 2!!>

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

SUMMARY OF TECHNICAL COMPLIANCE – KEY DEFICIENCIES

Annex Table 2. Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	[C]	This table should set out the rating, and a summary of all the factors contributing to each rating.
2. National cooperation and coordination	[LC]	•
3. Money laundering offences	[PC]	•
4. Confiscation and provisional measures	[NC]	•
5. Terrorist financing offence		•
6. Targeted financial sanctions related to terrorism & TF		•
7. Targeted financial sanctions related to proliferation		•
8. Non-profit organisations		•
9. Financial institution secrecy laws		•
10. Customer due diligence		•
11. Record keeping		•
12. Politically exposed persons		•
13. Correspondent banking		•
14. Money or value transfer services		•
15. New technologies		•
16. Wire transfers		•
17. Reliance on third parties		•
18. Internal controls and foreign branches and subsidiaries		•
19. Higher-risk countries		•
20. Reporting of suspicious transaction		•
21. Tipping-off and confidentiality		•
22. DNFBPs: Customer due diligence		•
23. DNFBPs: Other measures		•
24. Transparency and beneficial ownership of legal persons		•
25. Transparency and beneficial ownership of legal arrangements		•
26. Regulation and supervision of financial institutions		•
27. Powers of supervisors		•
28. Regulation and supervision of DNFBPs		•
29. Financial intelligence units		•
30. Responsibilities of law enforcement and investigative authorities		•

Recommendations	Rating	Factor(s) underlying the rating
31. Powers of law enforcement and investigative authorities		•
32. Cash couriers		•
33. Statistics		•
34. Guidance and feedback		•
35. Sanctions		•
36. International instruments		•
37. Mutual legal assistance		•
38. Mutual legal assistance: freezing and confiscation		•
39. Extradition		•
40. Other forms of international cooperation		•

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>

GLOSSARY OF ACRONYMS[108]

	DEFINITION
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism

Note: <!!Add the note here. If you do not need a note, please delete this line.!!>
Source: <!!Add the source here. If you do not need a source, please delete this line.!!>

[108] Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

ANNEX III

FATF GUIDANCE DOCUMENTS

Assessors may consider FATF Guidance as background information on the practicalities of how countries can implement specific requirements. However, assessors should remember that FATF guidance is ***non-binding***. The application of any guidance should not form part of the assessment. See Methodology para. 29.

Guidance	Relevant FATF Standards/Methodology
National money laundering and terrorist financing risk assessment (05 Mar 2013) Terrorist Financing Risk Assessment Guidance (05 Jul 2019)	**R.1** (Assessing Risks and Applying a Risk Based Approach)
Best Practices Paper on Recommendation 2: Sharing among domestic competent authorities information related to the financing of proliferation (07 Mar 2012)	**R.2** (National Co-operation and Co-ordination) **R.7** (TFS Related to Proliferation)
Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery (19 Oct 2012)	**R.4** (Confiscation and Provisional Measures) **R.38** (Freezing and Confiscation)
Guidance on Criminalising Terrorist Financing (21 Oct 2016)	**R.5** (Terrorist Financing Offence)
International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6) (28 June 2013)	**R.6** (Targeted Financial Sanctions related to Terrorism and Terrorist Financing)
FATF Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (28 Feb 2018)	**R.7** (Targeted Financial Sanctions related to Proliferation)
Best Practices on Combating the Abuse of Non-Profit Organisations (26 Jun 2015)	**R.8** (Non-Profit Organisations (NPOs))
Guidance on Digital ID (6 March 2020)	**R.10** (Customer due diligence (CDD)=
FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) (27 Jun 2013)	**R.12** (Politically Exposed Persons (PEPs)) **R.22** (Designated Non-Financial Businesses and Professions (DNFBPs): Customer Due Diligence)

Guidance	Relevant FATF Standards/Methodology
Guidance on Correspondent Banking Services (21 Oct 2016)	**R.13** (Correspondent Banking)
Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (21 Jun 2019)	**R.15** (New technologies)
FATF Guidance - Private Sector Information Sharing (04 Nov 2017)	**R.18** (Internal Controls and Foreign Branches and Subsidiaries) **R.21** (Tipping-Off and Confidentiality)
Best Practices on Beneficial Ownership for Legal Persons (16 October 2019) Guidance on Transparency and Beneficial Ownership (27 Oct 2014)	**R.24** (Transparency and Beneficial Ownership of Legal Persons) **R.25** (Transparency and Beneficial Ownership of Legal Arrangements) **Methodology IO.5** (Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments)
Operational Issues - Financial Investigations Guidance (11 Jul 2012)	**R.30** (Responsibilities of Law Enforcement and Investigative Authorities) **R.31** (Powers of Law Enforcement and Investigative Authorities) **Methodology IO.7** (Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions)
Guidance on AML/CFT-related data and statistics (27 Nov 2015)	**R.33** (Statistics) **Methodology** *Effectiveness Assessment*
Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement (23 Oct 2015)	**Methodology IO.3** (Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks)
FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence (04 Nov 2017)	**Methodology IO.4** (Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions)
Best Practices Paper: The Use of the FATF Recommendations to Combat Corruption (18 Oct 2013)	**Methodology** *Introduction* (Corruption)

Guidance	Relevant FATF Standards/Methodology
• Guidance for a Risk Based Approach for Legal Professionals (26 Jun 2019) • Guidance for a Risk-Based Approach for the Accounting Profession (26 Jun 2019) • Guidance for a Risk-Based Approach for Trust and Company Service Providers (26 Jun 2019) • Guidance for a Risk-Based Approach: Life Insurance Sector (29 Oct 2018) • Guidance for a Risk-Based Approach: Securities Sector (29 Oct 2018) • Guidance for a Risk-Based Approach: Money or Value Transfer Services (23 Feb 2016) • Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement (23 Oct 2015) • Guidance for a Risk-Based Approach: Virtual Currencies (26 June 2015) • Guidance for a Risk-Based Approach: The Banking Sector (27 Oct 2014) • Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services (26 June 2013)	**Methodology** *Introduction* (RBA)

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS AND VASPS

1. All requirements for financial institutions, DNFBPs or VASPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).

2. In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.

3. The term "*Enforceable means*" refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).

4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:

   (a) There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:

      (i) if particular measures use the word *shall* or *must*, this should be considered mandatory;

      (ii) if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).

   (b) The document/mechanism must be issued or approved by a competent authority.

   (c) There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:

(i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

(ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and

(iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.

5. In all cases it should be apparent that financial institutions, DNFBPs and VASPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

GENERAL GLOSSARY

Terms	Definitions
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Please refer to the IN to Recommendation 16.
Agent	For the purposes of Recommendations 14 and 16, *agent* means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.
Appropriate authorities	Please refer to the IN to Recommendation 8.
Associate NPOs	Please refer to the IN to Recommendation 8.
Batch transfer	Please refer to the IN to Recommendation 16.
Bearer negotiable instruments	*Bearer negotiable instruments (BNIs)* includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
Beneficial owner	*Beneficial owner* refers to the natural person(s) who ultimately[109] owns or controls a customer[110] and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiaries	Please refer to the IN to Recommendation 8.
Beneficiary	The meaning of the term *beneficiary* in the FATF Recommendations depends on the context: ■ In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or

109 Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

110 This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Terms	Definitions
	legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. Please also refer to the Interpretive Notes to Recommendation 16.
Beneficiary Financial Institution	Please refer to the IN to Recommendation 16.
Competent authorities	*Competent authorities* refers to all public authorities[111] with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as competent authorities.
Confiscation	The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked

111 This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
	to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to *country* or *countries* apply equally to territories or jurisdictions.
Cover Payment	Please refer to the IN. to Recommendation 16.
Criminal activity	*Criminal activity* refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Cross-border Wire Transfer	Please refer to the IN to Recommendation 16.
Currency	*Currency* refers to banknotes and coins that are in circulation as a medium of exchange.
Designated categories of offences	*Designated categories of offences* means: ■ participation in an organised criminal group and racketeering; ■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking;

Terms	Definitions
	■ illicit trafficking in stolen and other goods; ■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime; ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos[112] b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.

[112] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

Terms	Definitions
	f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; ■ acting as (or arranging for another person to act as) a nominee shareholder for another person.
Designated person or entity	The term designated person or entity refers to: (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any individual, natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1718 (2006) and any future successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to resolution 1718 (2006) (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and

Terms	Definitions
	(v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 2231 (2015) and any future successor resolutions by the Security Council.
Designation	The term *designation* refers to the identification of a person[113], individual or entity that is subject to targeted financial sanctions pursuant to: ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution 1718 (2006) and any future successor resolutions; ■ Security Council resolution 2231 (2015) and any future successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. As far as Security Council resolution 2231 (2015) and any future successor resolutions are concerned, references to "designations" apply equally to "listing".
Domestic Wire Transfer	Please refer to the IN to Recommendation 16.
Enforceable means	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Ex Parte	The term *ex parte* means proceeding without prior notification and participation of the affected party.
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).

[113] Natural or legal.

Terms	Definitions
False declaration	Please refer to the IN to Recommendation 32.
False disclosure	Please refer to the IN to Recommendation 32.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[114] 2. Lending.[115] 3. Financial leasing.[116] 4. Money or value transfer services.[117] 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading. 8. Participation in securities issues and the provision of financial services related to such issues.

114 This also captures private banking.

115 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

116 This does not extend to financial leasing arrangements in relation to consumer products.

117 It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

Terms	Definitions
	9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[118]. 13. Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).
Freeze	In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court. In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.

[118] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Terms	Definitions
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	The term *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.
Funds or other assets	The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.
Identification data	The term *identification data* refers to reliable, independent source documents, data or information.
Intermediary financial institution	Please refer to the IN to Recommendation 16.
International organisations	International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

Terms	Definitions
Law	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Legal arrangements	*Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
Legal persons	*Legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a *money laundering offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.
Non-conviction based confiscation	*Non-conviction based confiscation* means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.
Non-profit organisations	Please refer to the IN to Recommendation 8.
Originator	Please refer to the IN to Recommendation 16.
Ordering financial institution	Please refer to the IN to Recommendation 16.
Payable-through accounts	Please refer to the IN to Recommendation 13.
Physical cross-border transportation	Please refer to the IN. to Recommendation 32.

Terms	Definitions
Politically Exposed Persons (PEPs)	*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Persons who are or have been entrusted with a prominent function by an international organisation* refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Qualifying wire transfers	Please refer to the IN to Recommendation 16.
Reasonable measures	The term *Reasonable Measures* means: appropriate measures which are commensurate with the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	Please refer to the IN. to Recommendation 32.
Required	Please refer to the IN to Recommendation 16.
Risk	All references to *risk* refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.

Terms	Definitions
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
Serial Payment	Please refer to the IN. to Recommendation 16.
Settlor	*Settlors* are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
Straight-through processing	Please refer to the IN. to Recommendation 16.
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*" [119]) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they

[119] Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

Terms	Definitions
	perform, and be supervised by a competent authority in relation to such functions.
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
Terrorist	The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A *terrorist act* includes: (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	*Terrorist financing* is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist financing abuse	Please refer to the IN to Recommendation 8.

Terms	Definitions
Terrorist financing offence	References (except in Recommendation 4) to a *terrorist financing offence* refer not only to the primary offence or offences, but also to ancillary offences.
Terrorist organisation	The term *terrorist organisation* refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term *third parties* includes, but is not limited to, financial institutions and DNFBPs. Please also refer to the IN to Recommendation 17.
Trustee	The terms *trust* and *trustee* should be understood as described in and consistent with Article 2 of the *Hague Convention on the law applicable to trusts and their recognition*[120]. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family).
Unique transaction reference number	Please refer to the IN. to Recommendation 16.

120 Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

a) the assets constitute a separate fund and are not a part of the trustee's own estate;

b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;

c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

Terms	Definitions
Virtual Asset	A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations
Virtual Asset Service Providers	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer[121] of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Without delay	The phrase without delay means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

121 In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

INFORMATION ON UPDATES MADE TO THE FATF METHODOLOGY

The following amendments have been made to the FATF Methodology since the text was adopted in February 2013.

Date	Type of amendments	Sections subject to amandments
Oct 2015	Addition of footnote to clarify the interpretation of criterion 29.3.	• R.29 – page 81 To add a footnote to guide the application of the methodology for criterion 29.3 on the FIU's power to obtain additional information.
Feb 2016	Revision of R.5 and IO.9.	• R.5 and IO.9 – pages 32-33 and 124-125 To align the methodology for R.5 and IO.9 with the revised Interpretive Note to Recommendation 5 relating to UNSCR 2178.
Feb 2016	Addition of footnote to clarify the requirements of criterion 33.1.	• R.33 – page 87 To add a footnote to clarify the application of the methodology for criterion 33.1.
Feb 2016	Addition of footnote on the terminology of different types of ML activity to IO.7.	• IO.7 – pages 119-121 To add a footnote clarifying the terminology of different types of ML activity as referred to in the Methodology for IO.7 (core issue 7.3).
Oct 2016	Revision of R.8 and IO.10.	• R.8 and IO.10, and Glossary – pages 41-43 and 126-128 To align the methodology for R.8 and IO.10 with the revised Recommendation 8 and Interpretive Note to Recommendation 8.
Oct 2016	Addition of footnote on tax and confiscation to IO.8.	• IO.8 – pages 122-123 To add a footnote about how tax confiscation figures should be taken into account for the assessment of effectiveness under IO.8 (core issue 8.2).
Feb 2017	Revision of R.5 and IO.9.	• R.5 and IO.9 – pages 32-33 and 124-125 To align the methodology for R.5 and IO.9 with the revised Interpretive Note to Recommendation 5 and the Glossary term "funds or other assets".
Nov 2017	Revision to Recommendation 7.	• R.7 – page 38-40 To amend R.7 to mirror amendments to the FATF Standards (INR.7 and the Glossary) made in June 2017 which reflected changes to the UN Security Council Resolutions on proliferation financing since the FATF standards were issued in February 2012.

Date	Type of amendments	Sections subject to amandments
Nov 2017	Revision of footnote to Recommendation 25.	• R.25 – page 75-76 To amend footnote 73 to the methodology for R.25 to provide guidance on how to identify other legal arrangements that fall within the scope of R.25 and IO.5 because of characteristics and features which are similar to express trusts and could be particularly vulnerable from a ML/TF perspective, and to ensure a consistent approach across mutual evaluations.
Feb 2018	Revision of Recommendations 18 and 21	• R.18 – pages 63-64 and R.21 - page 67 To amend R.18 and R.21 to reflect the November 2017 amendments to the FATF Standards (INR.18 and R.21) which clarified the requirements on sharing of information related to unusual or suspicious transactions within financial groups, and the interaction of these requirements with tipping-off provisions.
Oct 2018	Revision of Recommendation 2 and Immediate Outcome 1	• R.2 – page 28 and IO.1 – page 99 To reflect the February 2018 amendments to the FATF Standards (R.2) which clarify the need for compatability of AML/CFT requirements and data protection and privacy rules and build on the conclusions of RTMG's report on inter-agency CT/CFT information sharing.
Oct 2018	Revisions to Chapter 1 and addition of footnotes in Chapters 5 and 6 related to Immediate Outcomes 3 and 4	• Chapter 1 – page 138 • Chapter 5 – page 146, and Chapter 6 – page 147 Addition of footnotes to clarify the expectations when assessing effectiveness under IO.3 and IO.4, taking into consideration the risk, context and materiality of the country being assessed.
Feb 2019	Revisions to Immediate Outcomes 3 and 4 Addition of notes to assessors and footnotes	• Outcome 3 - pages 105-106 • Outcome 4 - pages 109-110 Addition of notes to assessors and footnotes to provide further guidance on how to assess the relative importance of the different sectors of financial institutions and DNFBPs.

Date	Type of amendments	Sections subject to amandments
Oct 2019	Revisions to Recommendation 15 and Immediate Outcomes 1 - 4, and 6 – 11 to reflect amendments to the FATF Standards (R.15, INR.15 and Glossary terms) incorporating virtual assets and virtual asset service providers	• Introduction paragraph 15 – page 8 New paragraph and footnote to provide guidance on how to assess requirements relating to virtual assets and virtual asset service providers. • Introduction paragraphs 21, 22, 24 and diagram at paragraph 44 – pages 9, 10 and 18 Addition of references to virtual assets and virtual asset service providers. • Recommendation 15, Note to assessors and criteria 15.3 – 15.11 – pages 54-57 • Immediate Outcomes 3 and 4 – pages 105 - 112 Addition of further guidance on how to assess requirements relating to virtual assets and virtual asset service providers and new criteria to reflect the amendments to the FATF Standards (R.15, INR.15 and Glossary terms “virtual assets” and “virtual asset service provider”). • Immediate Outcomes 1, 2, 3, 4, 6, 7, 8, 9, 10 and 11 – pages 97, 102, 105-108, 109-112, 116, 119, 122, 124, 126-127, and 129-130. Addition of reference to R.15, or elements of R.15, as being related to the outcome and reference to VASPs as needed.

www.fatf-gafi.org

Appendix G:

FATF, *Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations* (Paris: FATF, 2019).

PROCEDURES FOR THE FATF FOURTH ROUND OF AML/CFT MUTUAL EVALUATIONS

Updated October 2019

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2019), *Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations,* updated October 2019, FATF, Paris, France, www.fatf-gafi.org/publications/mutualevaluations/documents/4th-round-procedures.html

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
ECG	Evaluations and Compliance Group
ES	Executive Summary
FIU	Financial Intelligence Unit
FSAP	Financial Sector Assessment Programme
FSRB	FATF-Style Regional Body
FT	Financing of Terrorism
IO	Immediate Outcome
IFI	International Financial Institution (IMF and World Bank)
MER	Mutual Evaluation Report
ML	Money Laundering
NC	Non-compliant
PC	Partially Compliant
STR	Suspicious transaction report
SRB	Self-Regulatory Body
TC	Technical Compliance

PROCEDURES FOR THE FATF FOURTH ROUND OF AML/CFT MUTUAL EVALUATIONS

INTRODUCTION

1. The FATF is conducting a fourth round of mutual evaluations for its members based on the FATF Recommendations (2012), and the Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (2013), as amended from time to time. This document sets out the procedures that are the basis for that fourth round of mutual evaluations.

I. SCOPE, PRINCIPLES AND OBJECTIVES FOR THE FOURTH ROUND

2. As set out in the Methodology, the scope of the evaluations will involve two inter-related components for technical compliance and effectiveness. The technical compliance component will assess whether the necessary laws, regulations or other required measures are in force and effect, and whether the supporting anti-money laundering (AML) / countering the financing of terrorism (CFT) institutional framework is in place. The effectiveness component will assess whether the AML/CFT systems are working, and the extent to which the country is achieving the defined set of outcomes.

3. There are a number of general principles and objectives that govern FATF mutual evaluations, as well as AML/CFT assessments conducted by the FATF-Style Regional Bodies (FSRBs), IMF or World Bank. The procedures should:

a) Produce objective and accurate reports of a high standard in a timely way.

b) Ensure that there is a level playing field, whereby mutual evaluation reports (MERs), including the executive summaries, are consistent, especially with respect to the findings, the recommendations and ratings.

c) Ensure that there is transparency and equality of treatment, in terms of the assessment process, for all countries assessed.

d) Seek to ensure that the evaluation and assessment exercises conducted by all relevant organisations and bodies (FATF, IMF, World Bank, FSRBs) are equivalent, and of a high standard.

e) (i) be clear and transparent; (ii) encourage the implementation of higher standards, (iii) identify and promote good and effective practices, and (iv) alert governments and the private sector to areas that need strengthening.

f) Be sufficiently streamlined and efficient to ensure that there are no unnecessary delays or duplication in the process and that resources are used effectively.

II. CHANGES IN THE FATF STANDARDS

4. As a dynamic process, on-going work within the FATF could lead to further changes to the Recommendations, the Interpretive Notes or the Methodology. All countries should be evaluated on the basis of the FATF Recommendations and Interpretative Notes, and the Methodology as they exist at the date of the country's on-site visit. The report should state clearly if an assessment has been made against recently amended Standards. To ensure equality of treatment, and to protect the international financial systems, compliance with the relevant elements of the changes could be assessed as part of the follow-up process (see section X below), if they have not been assessed or as part of the mutual evaluation.

III. SCHEDULE FOR THE FOURTH ROUND

5. The schedule of mutual evaluations for the fourth round, and the number of evaluations to be prepared each year is primarily governed by the number of MERs that can be discussed at each Plenary meeting, and by the need to complete the entire round in a reasonable timeframe.

6. A schedule of mutual evaluations showing the fixed or proposed date of the on-site visit, of relevant Financial Sector Assessment Programme (FSAP) missions and the date for the Plenary discussion of the MER will be maintained. Any proposed changes to the evaluation dates will require Plenary approval. Normally two MERs will be discussed per Plenary, but this could, on an exceptional basis, extend to three MERs. Other relevant information that will be provided includes information on the countries which have volunteered to provide assessors for forthcoming mutual evaluations. The considerations underlying the sequence of evaluations were:

- Members' views on their preferred date - members are consulted on the possible dates for on-site visits and Plenary discussion of their MER, and this is taken into account in the schedule.
- The scheduled date of any possible FSAP mission – see section IX below regarding the timing of the FSAP and of a mutual evaluation.
- The date of the last mutual evaluation or International Financial Institution (IFI) assessment.

IV. PROCEDURES AND STEPS IN THE EVALUATION PROCESS

7. A summary of the key steps and timelines for the assessment team and the country in the FATF mutual evaluation process is set out at Appendix 1. Those steps are described more fully below. The assessed countries and assessment teams have the flexibility to extend the overall timeline by up to one or two months in order to plan around FATF Plenary meetings, events or holidays, or to adjust the date of the on-site visit to the most appropriate time. In practice, this may require an earlier start to the evaluation process as there is no scope for reducing the time allocated to the post-onsite stages of the process, and the assessed country and assessment team should therefore agree on the broad timeline of the evaluation at least 14 months before the FATF Plenary discussion.

PREPARATION FOR THE ON-SITE VISIT

8. At least six months before the on-site visit or as early as possible, the Secretariat will fix the precise dates for the evaluation on-site visit as well as the timelines for the whole process in consultation with the country, and based on the timelines in Appendix 1 (some flexibility is permissible). The country will advise whether they wish to conduct the evaluation in English or French. The onus is on the country to demonstrate that it has complied with the Standards and that its AML/CFT regime is effective, hence, the country should provide all relevant information to the assessment team during the course of the assessment. As appropriate, assessors should be able to request or access documents (redacted if necessary), data, or other relevant information.

9. All updates and information should be provided in an electronic format and countries should ensure that laws, regulations, guidelines and other relevant documents are made available in the language of the evaluation and the original language.

(a) Information Updates on Technical Compliance

10. The updates and information provided by the assessed country are intended to provide key information for the preparatory work before the on-site visit, including understanding the country's ML/TF risks, identifying potential areas of increased focus for the on-site, and preparing the draft MER. Countries should provide the necessary updates and information to the Secretariat no less than six months before the on-site. Prior to that, it would be desirable to have informal engagement between the country and the Secretariat.

11. In some countries AML/CFT issues are matters that are addressed not just at the level of the national government, but also at state/province or local levels. Countries are requested to note the AML/CFT measures that are the responsibility of state/provincial/local level authorities, and to provide an appropriate description of these measures. Assessors should also be aware that AML/CFT measures may be taken at one or more levels of government, and should examine and take into account all the relevant measures, including those taken at a state/provincial/local level. Equally, assessors should take into account and refer to supra-national laws or regulations that apply to a country.

12. Countries should rely on the questionnaire for the technical compliance update (see Appendix 3) to provide relevant information to the assessment team. Along with previous reports, this will be used as a starting basis for the assessment team to conduct the desk-based review on technical compliance. The questionnaire is a guide to assist countries to provide relevant information in relation to: (i) background information on the institutional framework; (ii) information on risks and context; (iii) information on the measures that the country has taken to meet the criteria for each Recommendation. Countries should complete the questionnaire and may choose to present other information in whatever manner they deem to be most expedient or effective.

(b) Information on Effectiveness

13. Countries should provide information on effectiveness based on the 11 Immediate Outcomes identified in the effectiveness assessment no less than four months before the on-site. They should set out fully how each of the core issues is being addressed as set out in each Immediate Outcome. It

is important for countries to provide a full and accurate description (including examples of information, data and other factors) that would help to demonstrate the effectiveness of the AML/CFT regime.

(c) Composition and Formation of Assessment Team

14. The assessors are confirmed by the President through the Secretariat. This will normally take place at least four months before the on-site, and will be coordinated with member countries that had earlier volunteered assessors for the proposed assessment. The President or the Executive Secretary will formally advise the country of the composition of the assessment team at the time the team is confirmed.

15. An assessment team will usually consist of five to six expert assessors (comprising at least one legal, financial[1] and law enforcement expert), principally drawn from FATF members, and will be supported by members of the FATF Secretariat. Depending on the country and the ML/TF risks, additional assessors or assessors with specific expertise may also be required. In selecting the assessors, a number of factors will be considered: (i) their relevant operational and assessment experience; (ii) language of the evaluation; (iii) nature of the legal system (civil law or common law) and institutional framework; and (iv) specific characteristics of the jurisdiction (e.g. size and composition of the economy and financial sector, geographical factors, and trading or cultural links), to ensure that the assessment team has the correct balance of knowledge and skills. Assessors should be very knowledgeable about the FATF Standards, and are required to attend a fourth round assessor training seminar before they conduct a mutual evaluation. Usually, at least one of the assessors should have had previous experience conducting an assessment.

16. In joint evaluations, the assessment team will be made up of assessors from both the FATF and the relevant FSRB(s) (see section VII) and will also be supported by members of the FATF Secretariat. For some other FATF evaluations, the Secretariat could, with the consent of the assessed country, invite an expert from an FSRB (member or Secretariat) or the IMF/World Bank[2] to participate as an expert on the assessment team, on the basis of reciprocity. Normally there should be no more than one, or in exceptional cases two, such experts per evaluation.

17. Due to the nature of the peer review process, the Secretariat will work to ensure that the mutuality of the process is maintained, and all members should provide qualified experts to be assessors at least five times[3] over the course of the fourth round as a minimum, on a graduated basis, with the largest countries being expected to provide assessors at least nine times during the round. Taking into account that this minimum contribution of five assessors is a huge effort for smaller countries, flexibility will be introduced on the basis that the Secretariat will work with those countries, give them priority when forming assessment teams, and take into account their preferences for what assessor expertise they wish to provide and which countries they wish to assess, as agreed by the

1 The assessment team should have assessors with expertise relating to the preventive measures necessary for the financial sector and designated non-financial businesses and professions.

2 Participation (on a reciprocal basis) of experts from other observers that are conducting assessments, such as UNCTED, could be considered on a case by case basis.

3 The commitment of providing a minimum of five assessors could be met by the same person(s) participating as an assessor in multiple evaluations.

Plenary. Up to 2 assessors provided by FATF members to FSRB-only assessments should be recognised as contributions to FATF assessments. Countries that do not provide their minimum expected contribution of assessors should make a financial contribution to the FATF in an amount equivalent to the cost of providing such assessors, as determined by the Plenary. A list of countries' contribution of assessors for assessments will be maintained and monitored by the FATF's Evaluations and Compliance Group (ECG).

(d) Responsibilities of the Secretariat

18. The Secretariat

- Supports the assessment team and the assessed country;
- Focuses on quality and consistency;
- Ensures compliance with process and procedures;
- Assists assessors and assessed country in the interpretation of the standards, methodology and process in line with past Plenary decisions;
- Ensures that assessors and assessed countries have access to relevant documentation;
- Project-leads the process and other tasks as indicated in these procedures.

(e) Responsibilities of the Assessment Team (Assessors)

19. The core function of the assessment team is, collectively, to produce an independent report (containing analysis, findings and recommendations) concerning the country's compliance with the FATF Standards, in terms of both technical compliance and effectiveness. A successful assessment of an AML/CFT regime requires, at a minimum, a combination of financial, legal and law enforcement expertise, particularly in relation to the assessment of effectiveness. Experts therefore have to conduct an evaluation in a fully collaborative process, whereby all aspects of the review are conducted holistically. Each expert is expected to contribute to all parts of the review, but should take the lead on, or take primary responsibility for topics related to his or her own area of expertise. An overview of assessors' respective primary responsibilities should be shared with the assessed country, even if the assessment remains an all-team responsibility. As a result, assessors will be actively involved in all areas of the report and beyond their primary assigned areas of responsibilities.) It is also important that assessors are able to devote their time and resources to reviewing all the documents (including the information updates on technical compliance, and information on effectiveness), raising queries prior to the on-site, preparing and conducting the assessment, drafting the MER, attending the meetings (e.g. on-site, face-to-face meeting, and Plenary discussion), and adhere to the deadlines indicated.

20. The mutual evaluation is a dynamic and continuous process. The assessment team/Secretariat should engage and consult the assessed country on an on-going basis, commencing at least six months before the on-site. The country should indicate an identified contact person(s) or point(s) for the assessment. Throughout the process the Secretariat will ensure that the assessors can access all relevant material and that regular conference calls take place between assessors and the assessed country so as to ensure a smooth exchange of information and open lines of communication.

(f) Desk Based Review for Technical Compliance

21. Prior to the on-site visit, the assessment team will conduct a desk-based review of the country's level of technical compliance, and the contextual factors and ML/TF risks. The review will be based on information provided by the country in the information updates on technical compliance, pre-existing information drawn from the country's third round MER, follow-up reports and other credible or reliable sources of information. This information will be carefully taken into account, though the assessment team can review the findings from the previous MER and follow-up reports, and may highlight relevant strengths or weaknesses not previously noted. If the assessors reach a different conclusion to previous MERs and follow-up reports (in cases where the Standards and the legislation have not changed) then they should explain the reasons for their conclusion.

22. The technical compliance annex is drafted by the Secretariat on the basis of a comprehensive prior analysis by the assessors. This requires assessors to indicate if each sub-criterion is met, mostly met, partly met or not met and why. When drafting the TC Annex for assessors, the Secretariat takes into account the quality and consistency of mutual evaluation reports. Subsequent to the review, the assessment team will provide the country with a first draft of the technical compliance annex (which needs not contain ratings or recommendations) about three months before the on-site. This will include a description, analysis, and list of potential technical deficiencies noted. The country will have one month to clarify and comment on this first draft on technical compliance.

23. In conducting the assessment, assessors should only take into account relevant laws, regulations or other AML/CFT measures that are in force and effect at that time, or will be in force and effect by the end of the on-site visit. Where relevant bills or other specific proposals to amend the system are made available, these will be referred to in the MER (including for the purpose of the recommendations to be made to the country) but should not be taken into account in the conclusions of the assessment or for ratings purposes.

(g) Ensuring Adequate Basis to Assess International Cooperation

24. Six months before the on-site visit, FATF members and FSRBs[4] will be invited to provide information on their experience of international co-operation with the country being evaluated.

25. In addition, the assessment team and the country may also identify key countries which the assessed country has provided international cooperation to or requested it from, and seek specific feedback. The feedback could relate to: (i) general experience, (ii) positive examples, and (iii) negative examples, on the assessed country's level of international cooperation. The responses received will be made available to the assessment team and the assessed country.

(h) Identifying Potential Areas of Increased Focus for On-Site Visit

26. The assessment team will have to examine the country's level of effectiveness in relation to all the 11 Immediate Outcomes during the on-site. The assessment team may also, based on its preliminary analysis (of both technical compliance and effectiveness issues) prior to the on-site,

[4] FSRBs and their members will only be invited to provide this information where they are willing to reciprocally invite FATF members to provide the same type of information in relation to their mutual evaluations.

identify specific areas which it would pay more attention to during the on-site visit and in the MER, as well as the areas of reduced focus. This will usually relate to effectiveness issues but could also include technical compliance issues. In doing so, the team will consult the country. In addition, delegations will be invited to provide any comments that they may have that would assist the team to focus on areas of higher or lower risks that need increased or reduced focus.

27. Where there are potential areas of increased focus for the on-site, the assessment team should obtain and consider all relevant information and commence discussion of these areas approximately four months before the on-site, and consult the country at least two months before the on-site. The country should normally provide additional information regarding the areas which the assessment team would like to pay more attention to. While the prerogative lies with the assessment team, the areas for increased focus should, to the extent possible, be mutually agreed with the country, and should be set out in a draft scoping note. The scoping note should set out briefly (in no more than two pages) the areas for increased focus, as well as areas of reduced focus, and why these areas have been selected. The draft scoping note, along with relevant background information (e.g. the country's risk assessment(s)), should be sent to the reviewers (described in the section on quality and consistency, below) and to the country. Reviewers should, within one week of receiving the scoping note, provide their feedback to the assessment team regarding whether the scoping note reflects a reasonable view on the focus of the assessment, having regard to the material made available to them as well as their general knowledge of the jurisdiction. The assessment team should consider the merit of the reviewers' comments, and amend the scoping note as needed, in consultation with the country. The final version should be sent to the country, at least four weeks prior to the on-site, along with any requests for additional information on the areas of increased focus. The country should seek to accommodate any requests arising from the additional focus. The country should also consider holding a presentation on its risk and context at the start of the on-site visit for assessors to better evaluate the country's understanding of risks.

28. To expedite the mutual evaluation process, and to facilitate the on-site visit, the assessment team will, one week before the on-site visit, prepare a revised draft TC annex and an outline of initial findings/key issues to discuss on effectiveness. In order to facilitate the discussions on-site, the revised TC annex will be sent to the country at that time.

(i) Programme for On-Site Visit (Pre-Plenary)

29. The country (designated contact) should work with the Secretariat, and prepare a draft programme and coordinate the logistics for the on-site. The draft programme, together with any specific logistical arrangements, should be sent to the assessment team no later than eight weeks before the visit. Please see Appendix 2 for the list of authorities and businesses that would usually be involved in the on-site. To assist in their preparation, the assessment team should prepare a preliminary analysis identifying key issues on effectiveness, eight weeks before the on-site.

30. The draft programme should take into account the areas where the assessment team may want to apply increased focus. Where practical, meetings could be held in the premises of the agency/organisation being met, since this allows the assessors to meet the widest possible range of staff and to obtain information more easily. However, for some evaluations travelling between venues can be time consuming and wasteful, and generally, unless venues are in close proximity, there should

be no more than two to three venues per day. The programme should be finalised at least three weeks prior to the on-site visit. The assessment team may also request additional meetings during the on-site.

31. Both in terms of the programme and more generally, the time required for interpretation, and for translation of documents, must be taken into account. During the on-site visit there also needs to be professional and well-prepared interpreters if interpretation from the country language to English/French is required. However, for the efficient use of time, meetings should generally be conducted in the language of the assessment.

(j) Confidentiality

32. All documents and information produced: (i) by an assessed country during a mutual evaluation exercise (e.g. updates and responses, documents describing a country's AML/CFT regime, measures taken or risks faced (including those for which there will be increased focus), or responses to assessors' queries); (ii) by the FATF Secretariat or assessors (e.g. reports from assessors, draft MER); and (iii) comments received through the consultation or review mechanisms, should be treated as confidential. They should only be used for the specific purposes provided and not be made publicly available, unless the assessed country and the FATF (and where applicable, the originator of the document) consents to their release. These confidentiality requirements apply to the assessment team, the Secretariat, reviewers, officials in the assessed country and any other person with access to the documents or information. In addition, at least four months before the on-site visit, the members of the assessment team and reviewers should sign a confidentiality agreement, which will include text regarding the need to declare a conflict of interest.

ON-SITE VISIT

33. The on-site visit provides the best opportunity to clarify issues relating to the country's AML/CFT system, and assessors need to be fully prepared to review the 11 Immediate Outcomes relating to the effectiveness of the system, and clarify any outstanding technical compliance issues. Assessors should also pay more attention to areas where higher money laundering and terrorist financing risks are identified. Assessors must be cognisant of the different country circumstances and risks, and that countries may adopt different approaches to meet the FATF Standards and to create an effective system. Assessors thus need to be open and flexible, and seek to avoid narrow comparisons with their own national requirements.

34. Experience has shown that at least seven to eight days of meetings are required for countries with developed AML/CFT systems. A typical on-site visit could thus allow for the following.

- An initial half day preparatory meeting between the Secretariat and assessors.
- Seven to eight days of meetings[5] with representatives of the country, including an opening and closing meeting. Time may have to be set aside for additional or follow-up

[5] The assessment team should also set aside time midway through the on-site to review the progress of the mutual evaluation and where relevant, the identified areas of increased focus for the on-site initially.

meetings, if, in the course of the set schedule, the assessors identify new issues that need to be explored, or if they need further information on an issue already discussed.

- One to two days where assessors work on the draft MER (supported by the Secretariat), ensure that all the major issues that arose during the evaluation are noted in the report, and discuss and agree ratings, and key recommendations. The assessment team should provide a written summary of its key findings to the assessed country officials at the closing meeting.

35. The total length of the mission for a normal evaluation is therefore likely to be in the order of ten working days, but this could be extended for large or complex jurisdictions.

36. It is important that the assessment team be able to request and meet with all relevant agencies during the on-site. The country being evaluated, and the specific agencies met should ensure that appropriate staff are available for each meeting. The assessment team should be provided with a specific office for the duration of the on-site mission, and the room should have photocopying, printing and other basic facilities, as well as internet access.

37. Meetings with the private sector or other non-government representatives[6] are an important part of the visit, and generally, the assessors should be given the opportunity to meet with such bodies or persons in private, and without a government official present, if there is concern that the presence of the officials may inhibit the openness of the discussion. The team may also request that meetings with certain government agencies are restricted to those agencies only.

POST ON-SITE - PREPARATION OF DRAFT EXECUTIVE SUMMARY AND MER

38. There should be a minimum of twenty seven (27) weeks between the end of the on-site visit and the discussion of the MER in Plenary. The timely preparation of the MER and Executive Summary[7] will require the assessors to work closely with the Secretariat and the country. Depending on when the Plenary discussion is scheduled, the time period may also be extended or adjusted. In exceptional cases, and based on justified circumstances (and with the consent of the assessed country), a shorter period of time may be allowed for.

39. The steps in finalising a draft report for discussion at Plenary, and the approximate time that is required for each part, are set out in greater detail below (see also Appendix 1). With the aim to facilitate communication between the assessment team and the assessed country, the Secretariat should facilitate regular conference calls between all parties, in particular after the circulation of an updated draft MER. In their drafting of the first and second draft MER, assessors should aim to clarify as much as possible how information submitted by the assessed country was taken into account, if/where additional information is still needed, and state clearly if they are not willing to change their views on a particular topic.

6 E.g. those listed in Appendix 2.

7 The format for the Executive Summary and MER is contained in Annex II of the Methodology. Assessors should also pay attention to the guidance on how to complete the Executive Summary and MER, including with respect to the expected length of the MER (100 pages or less, together with a technical annex of up to 60 pages).

(k) 1st Draft MER

40. The assessment team will have six weeks to coordinate and refine the first draft MER (including the key findings, potential issues of note and recommended actions for the country). The first draft MER will include the preliminary recommended actions and ratings. This is then sent to the country for comments. The country will have four weeks to review and provide its comments on the first draft MER to the assessment team. During this time, the assessment team would have to be prepared to respond to queries and clarifications that may be raised by the country.

(l) 2nd Draft MER and Executive Summary

41. On receipt of the country's comments on the first draft MER, the assessment team will have four weeks to review the various comments and make further amendments, as well as prepare the Executive Summary. The second draft MER and Executive Summary will then be sent to the country and to the reviewers (approximately 14 weeks after the on-site). As in the case of the first draft, assessors should aim to clarify as much as possible, in writing, how specific information was taken into account in their analysis.

(m) Initial Quality & Consistency Review

42. As part of the FATF mutual evaluation process, there will be a quality and consistency review. The main functions of the initial reviewers are to ensure MERs are of an acceptable level of quality and consistency, and to assist both the assessment team and the assessed country by reviewing and providing timely input on the scoping note and the draft MER and Executive Summary (including any annexes) with a view to:

- Commenting on assessors' proposals for the scope of the on-site.
- Reflecting a correct interpretation of the FATF Standards and application of the Methodology (including the assessment of risks, integration of the findings on technical compliance and effectiveness, and areas where the analysis and conclusions are identified as being clearly deficient).
- Checking whether the description and analysis supports the conclusions (including ratings), and whether, based on these findings, sensible recommended actions and priority actions for improvement are made.
- Where applicable, highlighting potential inconsistencies with earlier decisions adopted by the FATF on technical compliance and effectiveness issues.
- Checking that the substance of the report is generally coherent and comprehensible.

43. The review will involve drawing on expertise from a pool of qualified volunteer experts. This pool would contain experts from FATF and FSRB delegations, FSRB Secretariat members, and the IFIs. To avoid potential conflicts, the reviewers selected for any given quality and consistency review will be from countries other than those of the assessors, and will be made known to the country and assessors in advance. Generally, three reviewers would be allocated to each assessment; comprising two reviewers from the FATF, and one reviewer from another assessment body, each of whom could in principle focus on part of the report.

44. The reviewers will need to be able to commit time and resources to review the scoping note and the quality, coherence and internal consistency of the second draft MER, as well as consistency with the FATF Standards and FATF precedent. In doing so, the reviewers should have a copy of the comments provided by the country on the first draft MER. Reviewers need to be able to access all key supporting documents – from the assessed country's technical compliance submission to its risk assessment. To ensure transparency, all comments from the reviewers will be disclosed to the assessors and country. The reviewers will have three weeks to examine the second draft MER and provide their comments to the assessment team. These comments will be forwarded to the assessed country. The reviewers for the quality and consistency review do not have any decision making powers or powers to change a report. It is the responsibility of the assessment team to consider the reviewers' comments and then decide whether any changes should be made to the report. The assessment team will provide a short response to the Plenary regarding the changes it has made to the report based on the reviewers' comments and on the decisions that it has made.

45. The assessed country will have the opportunity to submit further comments on the second draft MER, in parallel with the review process. After three weeks, the comments from the country and reviewers on the second draft MER will be used as input for the face-to-face meeting.

46. Due to the nature of the peer review process, the Secretariat will work to ensure that the mutuality of the process is maintained, and members should provide qualified experts as reviewers. A list of past and forthcoming reviewers will be maintained and monitored by ECG.

(n) Face-to-Face Meeting

47. As is indicated in paragraph 44, following the conclusion of the initial review, the assessment team and the country will have three weeks to consider country and reviewers' comments received on the second draft MER and Executive Summary, discuss likely changes and unresolved issues, and identify issues for discussion at the face-to-face meeting.

48. A face-to-face meeting is an important way to assist the country and assessment team to resolve outstanding issues. The assessment team (including Secretariat) and the country should have a face-to-face meeting to further discuss the second draft MER and Executive Summary. During this session, the assessment team and country should work to resolve any disagreements over technical compliance or effectiveness issues and identify potential key issues for Plenary discussion. The face-to-face meeting should occur at least eight weeks before the Plenary (i.e. approximately 19 weeks after the on-site). As a rule, and whenever possible, the face-to-face meeting is also attended by the ECG co-chairs as this will assist the identification of key issues for Plenary discussions.

49. Subsequent to the face-to-face meeting, the assessment team will consider whether any further changes should be made to the draft MER and Executive Summary.

(o) Identifying Issues for Plenary Discussion

50. The revised Executive Summary and MER (third draft going to the Plenary), will then be sent to all members, associate members and observers at least five weeks (ideally six weeks) prior to Plenary. The assessed country's comments on this draft will be circulated then as well. Where the original draft is in French, the English translation will also be distributed at this time. Delegations will

have two weeks to provide any written comments on the MER and Executive Summary, and in particular, to identify any key issues that they wish to discuss in ECG/Plenary. The comments should focus on the substantive key issues, or on other high-level or horizontal aspects of the assessment, though other observations may also be made. The comments received will be made available to all delegations.

51. Based on the MER and Executive Summary, and comments received, the ECG co-chairs will engage the country, the assessment team and prepare a list of (usually five to seven) priority and substantive key issues that will be discussed in ECG. This should take into account the issues that the assessed country and delegations are most keen to discuss. After consultation with the President, the list of substantive key issues for Plenary discussion will be distributed. The list of key issues for discussion in ECG would include key issues arising from the report (whether referenced by the country, the assessment team or delegations), as well as any areas of interpretation or inconsistency with other MERs adopted by the FATF.

52. The finalised list of key issues will be circulated to delegations two weeks before the Plenary discussion. Drafting amendments received on the Executive Summary or MER can be made after the Plenary, and will also take into account the decisions made. After discussions in ECG, a revised key issue document is submitted to the Plenary for discussions.

(p) Respecting Timelines

53. The timelines are intended to provide guidance on what is required if the reports are to be prepared within a reasonable timeframe, and in sufficient time for discussion in Plenary. It is therefore important that all parties respect the timelines.

54. Delays may significantly impact the ability of the Plenary to discuss the report in a meaningful way. The draft schedule of evaluations has been prepared so as to allow enough time between the on-site visit and the Plenary discussion. A failure to respect the timetables may mean that this would not be the case. By agreeing to participate in the mutual evaluation process, the country and the assessors undertake to meet the necessary deadlines and to provide full, accurate and timely responses, reports or other material as required under the agreed procedure. Where there is a failure to comply with the agreed timelines, then the following actions could be taken (depending on the nature of the default):

a) Failure by the country - the FATF President may write to the head of delegation or the relevant Minister in the country. The Plenary will be advised as to reasons for deferral, and publicity could be given to the deferment (as appropriate) or other additional action considered. In addition the assessment team may have to finalise and conclude the report based on the information available to them at that time.

b) Failure by the assessors, the reviewers or the Secretariat - the President may write a letter to or liaise with the head of delegation of the assessor or reviewer, or the FATF Executive Secretary (for the Secretariat).

55. The Secretariat will keep the Presidency advised of any failures so that the President can respond in an effective and timely way. The Plenary is also to be advised if the failures result in a request to delay the discussion of the MER.

THE PLENARY DISCUSSION

56. The discussion of each MER and Executive Summary in Plenary (particularly the list of key issues)[8] will focus on high-level and substantive key issues, primarily concerning effectiveness. Where appropriate, important technical issues would also be discussed. Adequate time should always be set aside to discuss the country's response to the mutual evaluation and other issues. The discussion is likely, on average, to take three to four hours of Plenary time. The procedure for the discussion will be as follows:

- Assessment team briefly presents in high-level terms the key issues and findings from the report. The team will have the opportunity to intervene/comment on any issue concerning the Executive Summary or MER.
- Assessed country makes a short opening statement.
- The Plenary discusses the list of key issues identified by the ECG. This would usually be introduced briefly by ECG co-chairs.
- Adequate time (approximately half the Plenary's time) will be set aside to discuss the overall situation of the assessed country's AML/CFT regime and ML/TF risks, the priority actions set out in the Executive Summary, the country's response to the mutual evaluation including any actions already taken, and the key findings.
- Time permitting, other issues could be raised from the floor, and discussed by the Plenary.

ADOPTION OF THE MER AND EXECUTIVE SUMMARY

57. At the end of the Plenary discussion, the MER and the Executive Summary will be submitted to Plenary for adoption. The adopted report will be subject to further checks for typographical or similar errors.

58. If the MER and the Executive Summary are not agreed, then the assessors, the country and the Secretariat should prepare amendments to meet the issues raised by the Plenary. Where substantive changes are required, either because additional information is required to be added, or the report has to be substantially amended, then the Plenary could decide to: (a) defer adoption of the report, and agree to have a further discussion of an amended report at the following Plenary, or (b) where the required changes are less significant, adopt the report subject to it being amended, and the amended report being approved through a written process. The assessment team would be responsible for ensuring that all the changes agreed by the Plenary have been made. Following the discussion of the report, and prior to its formal adoption, the Plenary should discuss the nature of the follow-up measures that would be required (see section X below).

59. The final report is a report of the FATF, and not simply a report by the assessors. As such, the Plenary will retain the final decision on the wording of any report, consistent with the requirements of the FATF Standards and Methodology. The Plenary will give careful consideration to the views of

[8] The Executive Summary will describe the key risks, the strengths and weaknesses of the system, and the priority actions for the country to improve its AML/CFT regime.

the assessors and the country when deciding on the wording, as well as take into account the need to ensure consistency between reports.

V. POST-PLENARY QUALITY AND CONSISTENCY (Q&C) REVIEW AND PUBLICATION

60. Where an FATF or FSRB member, the FATF Secretariat, FSRB Secretariat or an IFI considers that a FATF or FSRB report has significant problems of quality and consistency (Q&C), it should wherever possible raise such concerns with the body conducting the assessment (the assessment body) prior to adoption. The assessment body, assessment team and assessed country should consider and work to appropriately address the concerns.

61. Nevertheless, highly exceptional situations may arise where significant concerns about the Q&C of a report remain after its adoption. To address such issues, the post-Plenary Q&C process applies to all assessment bodies with a view to preventing the publication of reports with significant Q&C problems and ensuring that poor quality assessments do not damage the FATF brand.

62. The post-Plenary quality and consistency (Q&C) review process applies to all mutual evaluation reports (MERs) (including their executive summaries), detailed assessment reports (DARs)[9] (including their executive summaries), mutual evaluation follow-up reports with technical compliance re-ratings (FURs) and follow-up assessment reports (FUARs).[10] The exception is FURs with technical compliance (TC) re-ratings where no Q&C issues are raised through the pre-plenary review process or during the relevant working group/plenary discussion. Such FURs are not subject to the post-Plenary review process and ordinarily should be published within six weeks after their adoption by Plenary.

STEPS IN THE POST-PLENARY Q&C PROCESS

63. After adoption of the report, the FATF Secretariat will amend all documents as necessary and will circulate a revised version of the report to the country within one week of the Plenary. Within two weeks of receiving it from the Secretariat, the country must confirm that the report is accurate and/or advise of any typographical or similar errors. Care will be taken to ensure that no confidential information is included in any published report.

64. The FATF Secretariat will then circulate the report to all FATF members, FSRBs and the IFIs, along with a template for referring Q&C issues for consideration. Parties who identify any serious or major Q&C issues have two weeks to advise the FATF Secretariat (for FATF reports) or both the FATF

[9] Where the evaluation is conducted by one of the International Financial Institutions (IFI) (IMF or World Bank).

[10] In this section, MERs, DARs, FURs and FUARs are collectively referred to as *reports.*

Secretariat and assessment body (for non-FATF reports)[11] in writing, using the template provided to indicate their specific concerns and how these concerns meet the substantive threshold.[12]

65. To be considered further in this process, a specific concern should be raised by at least two of the following parties: FATF or FSRB members[13] or Secretariats or IFIs, at least one of which should have taken part in the adoption of the report. Otherwise, the post-Plenary Q&C review process is complete, the FATF Secretariat will advise the assessment body and delegations accordingly and the report will be published.[14]

66. If two or more parties identify a specific concern, the Co-Chairs of the FATF Evaluations and Compliance Group (ECG) will review the concern to determine whether *prima facie* it meets the substantive threshold and procedural requirements. To aid in this decision, the FATF Secretariat will liaise with the relevant FATF or FSRB Secretariat team to provide the ECG Co-Chairs with any necessary background information on the issue, including (where relevant and appropriate):

a) information submitted by parties raising the Q&C issue

b) background information on any related comments raised at the pre-Plenary stage

c) the rationale for the relevant rating/issue under discussion based on the facts in the report and/or any relevant co-chairs' report or summary record from the working group/Plenary meeting where the report was discussed (including whether the issue was discussed in detail, what the outcome of the those discussions was and any reasons cited for maintaining or changing the rating or report)

d) objective cross-comparisons with previous FATF reports that have similar issues

e) the report's consistency with the corresponding parts of the Methodology

f) any connection or implications for the ICRG process, and

g) what next steps might be appropriate.

67. If the ECG Co-Chairs conclude that *prima facie* the substantive threshold and procedural requirements are met, the Secretariat will circulate the report to all FATF delegations for

11 Where FATF or FSRB members or secretariats consider that an MER which has been adopted by an IFI has or continues to have significant problems of quality or consistency, they should promptly inform the IFI of those concerns (and the FATF Secretariat when the concerns are raised by others).

12 The substantive threshold is *when serious or major issues of quality and consistency are identified, with the potential to affect the credibility of the FATF brand as a whole*.

13 Not including the assessed country.

14 Ordinarily publication would happen within six weeks of the report being adopted if no further steps in the post-Plenary Q&C process are needed.

consideration by the ECG along with a decision paper prepared by the FATF Secretariat in consultation with the relevant assessment body (FSRB/Secretariat/IFI). On the other hand, if the ECG Co-Chairs conclude that *prima facie* the substantive threshold and procedural requirements are not met, the issue would not be taken forward for discussion, but a short note explaining the Co-Chair's position would be presented to ECG for information.

68. Issues identified less than four to six weeks before the FATF Plenary will be discussed at the next FATF Plenary to ensure sufficient time for consultation among Secretariats and preparation of the decision paper. The decision paper prepared by the FATF Secretariat in consultation with the relevant assessment body will include the background information listed above in paragraph 66 to the extent that it is relevant and appropriate.

69. The ECG will decide whether the report meets the substantive threshold (serious or major issues of Q&C with the potential to affect the credibility of the FATF brand as a whole). Examples of situations meeting this substantive threshold include:

a) the ratings are clearly inappropriate and not consistent with the analysis

b) there has been a serious misinterpretation of the Standards, Methodology and/or Procedures

c) an important part of the Methodology has been systematically misapplied, or

d) laws that are not in force and effect have been taken into account in the analysis and ratings of a report.

70. If ECG decides that the report meets the substantive threshold, it will refer the matter to the FATF Plenary along with clear recommendations on what action would be appropriate (e.g. requesting that the relevant assessment body reconsiders the report and/or makes appropriate changes before any publication). On the other hand, if ECG decides that the report does not meet the substantive threshold, the FATF Secretariat will advise the assessment body and delegations that the post-Plenary Q&C review is complete, and the report will be published.

71. Where ECG has referred a post-Plenary Q&C issue, the FATF Plenary will discuss the matter and decide on the appropriate action. The Secretariat will advise the assessment body of the FATF Plenary's decision. If the assessment body declines to respond to the action requested by the FATF, the FATF Plenary will consider what further action may be necessary. The assessment body will not publish the report until the issue is resolved within FATF and the assessment body, and the FATF Secretariat advises that the post-Plenary Q&C review process is complete.

72. Following completion of the post-Plenary Q&C review process, the assessment body will publish the report on its website. Additionally, the FATF publishes all reports on its website to give timely publicity to an important part of the work of FATF and the global network.

VI. EVALUATIONS OF NEW MEMBERS

73. Where a potential new member undergoes a mutual evaluation by the FATF in order to assess whether it meets the criteria for FATF membership, the procedures laid out in sections I to V of these procedures will apply. If the criteria for membership are met, and the country is admitted as an FATF member, but if deficiencies are identified in the country's AML/CFT system, the Plenary shall apply the FATF's follow-up policy (section X). However, if the membership criteria are not met and a country agrees to an action plan, and is admitted as a new member before the completion of the action plan, the new member will then be required to provide more detailed information as part of its enhanced follow-up reports focusing on progress towards achieving the IOs identified in the action plan. Plenary retains the discretion to vary the specific frequency of reporting by new members in enhanced follow-up.

VII. JOINT MUTUAL EVALUATIONS WITH FSRBS

74. The FATF's policy is that FATF members that are also members of FSRB(s) will undergo a joint evaluation by these bodies. Generally, the FATF will be the principal organiser, and will provide three assessors, while one to two assessors could be provided by the participating FSRBs. The FATF and the FSRB(s) Secretariats will participate. Reviewers should be provided by FATF, the FSRB(s), and another assessment body. To ensure adequate attention is given to consistency, a joint evaluation may use additional reviewers beyond the three set out in section IV(m). The first discussion of the MER should take place in the FATF, and given the additional measures adopted for joint evaluations, the presumption is that the FATF's view would be conclusive.

75. The process (including the FATF procedures for preparing the draft MER and Executive Summary) for joint evaluations would be the same as for other FATF evaluations, with the FSRB(s) and its/their members having opportunities to participate directly through being part of the assessment team, and also being able to provide comments and input like other delegations. FSRBs should allow reciprocal participation in mutual evaluation discussions for FATF members, and on this basis, the following measures should also apply for joint evaluations.

- A representative from the FSRB(s) will be given a specific opportunity to intervene during the Plenary discussion of the MER.
- All the FATF assessors on the assessment team are encouraged to attend the FSRB Plenary(ies) at which the joint evaluation report is considered, and at least one FATF assessor should attend the FSRB Plenary(ies). The same approach should be applied to IFI-led assessments of FATF members that are also members of FSRBs.
- In an exceptional case where a report was agreed within FATF but subsequently the FSRB identified major difficulties with the text of the report, then the FSRB Secretariat would advise the FATF Secretariat of the issues, and the issues should be discussed at the following FATF Plenary.
- Consideration will also be given to the timing of publication, if the MER has not been discussed in the FSRB(s), with a view to finding a mutually agreed publication date.

- If scheduling permits, the Plenary discussion of a joint MER may take place at a joint Plenary meeting of the FATF and the FSRB, with the full participation of all FATF and FSRB members.

76. For the evaluation of a member country of the Gulf Cooperation Council, the assessment team may adopt Arabic as the working language, provided that bilingual assessors, reviewers, and FATF and MENAFATF secretariat staff are available. In this case, laws and other documents would be provided in Arabic and meetings conducted in Arabic. The third draft report (post face-to-face meeting) would be translated into English, in time for circulation, which would be the primary language for Plenary discussion.

VIII. IMF OR WORLD BANK LED ASSESSMENTS OF FATF MEMBERS

77. The FATF is responsible for the mutual evaluation process for all of its members, and there is a presumption that the FATF will conduct the mutual evaluations[15] of all FATF members as part of this process. The presumption can be overridden at the discretion of the FATF Plenary on a case by case basis, with the country's agreement. For the purposes of the FATF fourth round of mutual evaluations, the FATF Plenary has discretion as to the number of FATF assessments that could be conducted by the IMF or World Bank (IFI), but the expectation is that there would be five to six IFI-led assessments during the fourth round of mutual evaluations (one a year), and such IFI-led assessments should be agreed and fixed on the same basis as other evaluations in the schedule (see section III).

78. For the FATF assessment schedule to be fixed with appropriate certainty and in a coordinated manner, the process leading to the Plenary decision as to which FATF countries will have an assessment led by an IFI team should be clear and transparent. In order for the evaluation schedule to be appropriately planned and assessment teams to be formed in sufficient time, it will be necessary for the FATF to be involved at an early stage in the process of determining which countries will be assessed by an IFI. The ECG will be informed at every Plenary as to the current status of the assessment schedule, including proposals as to whether assessments will be IFI-led, and the Plenary will decide on any such requests. Where the IMF or World Bank conduct an AML/CFT assessment as part of the FATF fourth round they should use procedures and a timetable similar to those of the FATF.

79. The FATF Plenary will in all cases have to approve an IFI assessment that is conducted under the FATF fourth round for it to be accepted as a mutual evaluation.

IX. CO-ORDINATION WITH THE FSAP PROCESS

80. The FATF Standards are recognised by the IFIs as one of 12 key standards and codes, for which Reports on the Observance of Standards and Codes (ROSCs) are prepared, often in the context of a Financial Sector Assessment Programme (FSAP). Under current FSAP policy, every FSAP and FSAP update should incorporate timely and accurate input on AML/CFT. Where possible, this input should be based on a comprehensive quality AML/CFT assessment, and in due course, on a follow-up assessment conducted against the prevailing standard. The FATF and the IFIs should therefore co-

15 Including any follow up that may be required.

ordinate with a view to ensuring a reasonable proximity between the date of the FSAP mission and that of a mutual evaluation or follow-up assessment conducted under the prevailing methodology, to allow for the key findings of that evaluation or follow-up assessment to be reflected in the FSAP; and members are encouraged to co-ordinate the timing for both processes internally, and with the FATF Secretariat and IFI staff.[16]

81. The basic products of the evaluation process are the MER and the Executive Summary (for the FATF) and the DAR and ROSC (for the IFIs)[17]. The Executive Summary, whether derived from a MER or follow-up assessment report, will form the basis of the ROSC. Following the Plenary, and after the finalisation of the Executive Summary, the summary is provided by the Secretariat to the IMF or World Bank so that a ROSC can be prepared, following a pro forma review.

82. The substantive text of the draft ROSC will be the same as that of the Executive Summary, though a formal paragraph will be added at the beginning:

> "This Report on the Observance of Standards and Codes for the *FATF Recommendations and Effectiveness of AML/CFT Systems* was prepared by the Financial Action Task Force (FATF). The report provides a summary of [the/certain][18] AML/CFT measures in place in [*Jurisdiction*] as at [*date*], the level of compliance with the FATF Recommendations, the level of effectiveness of the AML/CFT system, and contains recommendations on how the latter could be strengthened. The views expressed in this document have been agreed by the FATF and [*Jurisdiction*], but do not necessarily reflect the views of the Boards or staff of the IMF or World Bank."

X. FOLLOW-UP PROCESS

83. The follow-up process is intended to: (i) encourage members' implementation of the FATF Standards; (ii) provide regular monitoring and up-to-date information on countries' compliance with the FATF Standards (including the effectiveness of their AML/CFT systems); (iii) apply sufficient peer pressure and accountability; and (iv) better align the FATF and FSAP assessment cycle.

84. Following the discussion and adoption of a MER, the country could be placed in either regular or enhanced follow-up. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up is based on the FATF's traditional policy that deals with members with significant

---

16 If necessary, the staff of the IFIs may supplement the information derived from the ROSC to ensure the accuracy of the AML/CFT input. In instances where a comprehensive assessment or follow-up assessment against the prevailing standard is not available at the time of the FSAP, the staff of the IFIs may need to derive key findings on the basis of other sources of information, such as the most recent assessment report, and follow-up and/or other reports. As necessary, the staff of the IFIs may also seek updates from the authorities or join the FSAP mission for a review of the most significant AML/CFT issues for the country in the context of the prevailing standard and methodology. In such cases, staff would present the key findings in the FSAP documents: however, staff would not prepare a ROSC or ratings.

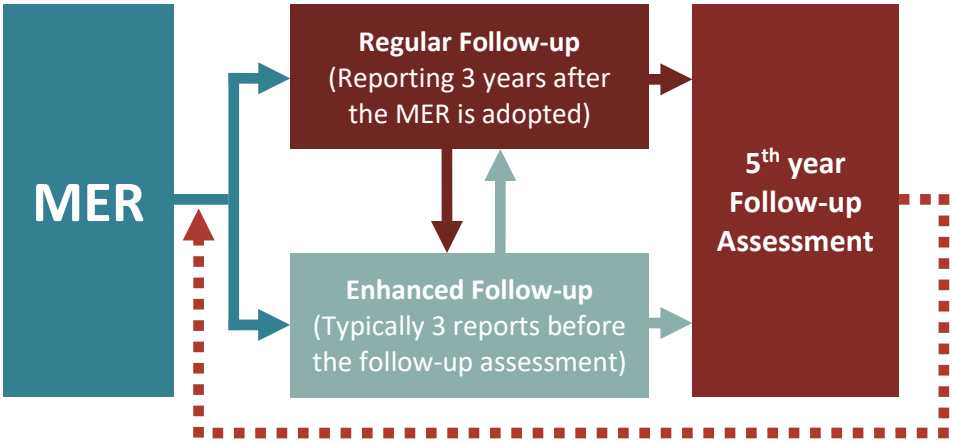
17 The DAR and ROSC use the common agreed template that is annexed to the Methodology and have the same format, although the ROSC remains the responsibility and prerogative of the IMF/World Bank.

18 For ROSCs based on an MER, the word "the" should be used; for ROSCs based on a MER follow-up assessment, the alternative wording "certain" would be used (since the follow-up assessment is not a comprehensive one)

deficiencies (for technical compliance or effectiveness) in their AML/CFT systems, and involves a more intensive process of follow-up.

85. Whether under regular or enhanced follow-up, the country will have a follow-up assessment after five years. This is intended to be a targeted but more comprehensive report on the countries' progress, with the main focus being on areas in which there have been changes, high risk areas identified in the MER or subsequently, on the priority areas for action. A schematic of the 4th round process is included below.

Figure 1. **Process of the 4th Round of Mutual Evaluations**



86. Countries may seek re-ratings for technical compliance with Recommendations rated as NC or PC before or after the 5th year follow-up assessment as part of the follow-up process. The general expectation is for countries to have addressed most if not all of the technical compliance deficiencies by the end of the 3rd year, and the effectiveness shortcomings by the time of the follow-up assessment. Requests for technical compliance re-ratings will not be considered where the expert(s) determines that the legal, institutional, or operational framework has not changed since the country's MER (or previous FUR, if applicable) and there have been no changes to the FATF Standards or their interpretation.[19]

87. If any of the FATF Standards have been revised since the end of the on-site visit (or previous FUR, if applicable), the country will be assessed for compliance with all revised standards at the time its re-rating request is considered (including cases where the revised Recommendation was rated LC or C). In the exceptional case that it comes to the Plenary's attention that a country has significantly lowered its compliance with the FATF Standards, the Plenary may request the country to address any new deficiencies as part of the follow-up process.

[19] Where there is disagreement between the expert(s) and the assessed country in this respect, they should discuss with ECG Co-Chairs to achieve an agreement.

(a) Regular Follow-up

88. Regular follow-up will be the default mechanism to ensure a continuous and on-going system of monitoring. This is the minimum standard that will apply to all members. Countries subject to regular follow-up will report back to the Plenary after three years (10 Plenary meetings) from the adoption of the country's MER, and will be subject to a follow-up assessment after five years.

(b) Enhanced Follow-up

89. The Plenary may decide, at its discretion, that the country should be placed in enhanced follow-up, which would result in the country reporting back more frequently than for regular follow-up. Countries in enhanced follow-up would typically first report back four Plenary meetings after the adoption of the country's MER, and subsequently report twice more at intervals of three Plenary meetings. Plenary retains the discretion to vary the specific frequency of reporting. Minor technical compliance issues remaining after the third follow-up report (or the first report for regular follow-up) will be assessed during the follow-up assessment after the fifth year.

90. In deciding whether to place a country in enhanced follow-up, the Plenary would consider the following factors:

a) After the discussion of the MER: a country will be placed immediately into enhanced follow-up if any one of the following applies:

   (i) it has 8 or more NC/PC ratings for technical compliance, or

   (ii) it is rated NC/PC on any one or more of R.3, 5, 10, 11 and 20, or

   (iii) it has a low or moderate level of effectiveness for 7 or more of the 11 effectiveness outcomes, or

   (iv) it has a low level of effectiveness for 4 or more of the 11 effectiveness outcomes.

b) After the discussion of a regular follow-up report or the 5th year follow-up assessment: the Plenary could decide to place the country into enhanced follow-up at any stage, if a significant number of priority actions have not been adequately addressed on a timely basis.

c) If and when it comes to the Plenary's attention that a country has lowered its compliance with the FATF Standards during the regular follow-up process: a country will be placed into enhanced follow-up if its level of technical compliance changed to a level that the Plenary considers as equivalent to NC/PC on any one or more of R.3, 5, 10, 11 and 20.

91. In addition to more frequent reporting, the Plenary may also apply other enhanced measures to countries placed in enhanced follow–up, particularly if satisfactory progress is not achieved. Possible enhanced measures include:

a) A letter could be sent from the FATF President to the relevant minister(s) in the member jurisdiction drawing attention to the lack of compliance with the FATF Standards.

b) A high-level mission could be arranged to the member jurisdiction to reinforce this message. This mission would meet with Ministers and senior officials.

c) In the context of the application of Recommendation 19 by its members, issuing a formal FATF statement to the effect that the member jurisdiction is insufficiently in compliance with the FATF Standards, and recommending appropriate action, and considering whether additional counter-measures are required.

d) Suspending the jurisdiction's membership of the FATF until the priority actions have been implemented. Suspension would mean that the country would be considered as a non-member of the FATF for the period of the suspension, would not be able to attend FATF meetings or provide input into FATF processes except for the process to determine whether deficiencies have been adequately addressed.

e) Terminate the membership of the jurisdiction.

92. Countries may move to regular follow-up at any time during the enhanced follow-up process in the following situations:

a) Where the country entered enhanced follow-up on the basis of meeting a criterion in paragraph 89(a), the Plenary may decide that the country will be moved from enhanced to regular follow-up following Plenary's decision that the country no longer meets any of those criteria (i.e., after approving a request for re-ratings).

b) The Plenary also has the discretion to decide to move the country to regular follow-up at any time, if it is satisfied that the country has made significant progress against the priority actions in its MER or has taken satisfactory action to address its deficiencies, even if the country still meets a criterion in paragraph 89(a).

93. Where countries in enhanced follow-up move to regular follow-up, the Plenary will decide the timing of the country's next regular follow-up report or of the follow–up assessment.

(c) Follow-up Reports

94. In preparation for the follow-up reports, the country will provide an update to the Secretariat setting out the actions it has taken or is taking to address the priority actions and recommended actions, and deficiencies in its MER.

- **For regular follow-up reports**, as the expectation is that significant progress would have been made in the three year period since the MER was adopted, the report should focus on re-ratings for technical compliance and/or demonstrating progress in addressing the shortcomings in the MER.
- **For enhanced follow-up**, the first follow-up report should at least contain an outline of the country's strategy for addressing the issues identified in their MER and exiting enhanced follow-up, for Plenary's information. If not already contained in the first follow-up report, subsequent reports should focus on re-ratings for technical compliance and/or demonstrating progress in addressing the shortcomings in the MER.

- **For countries subject to review by the International Cooperation Review Group** (on the basis of an agreed action plan), no reporting is expected on the Recommendations that are included in an ongoing action plan. However, overall progress on each Recommendation is still expected to be achieved, including on parts of Recommendations that are not covered by the action plan, under the normal timelines, or as soon as the country has completed its action plan (if this is after the regular timelines).

95. The country will be asked to submit information regarding technical compliance (which may be used to justify re-ratings) and effectiveness (for information only).

- **Technical compliance updates** should be provided in a similar format to the Mutual Evaluation technical compliance questionnaire (see Appendix 3), in relation to the shortcomings identified in the MER.
- **Effectiveness updates** should include any information that goes towards addressing the priority actions or other recommended actions in the MER, such as the lists in the FATF Methodology on the Examples of Information that could support the conclusions on Core Issues for each Immediate Outcome. As with the Mutual Evaluation process, there is no fixed format for the effectiveness update.

96. Although effectiveness will not be re-assessed until the follow-up assessment, updates on effectiveness facilitate a better understanding by the FATF of the progress made over time. Plenary may refer to such updates in determining whether to move a country from enhanced follow-up to regular follow-up (or vice versa), or whether to apply other enhanced measures to countries in enhanced follow–up that do not achieve satisfactory progress.

97. Re-ratings for technical compliance may only be made with Plenary approval, which will be sought by written process. Where a country wishes to seek technical compliance re-ratings, it should indicate on which Recommendations a re-rating will be requested, seven months in advance of Plenary meetings. The update by the country should be submitted to the Secretariat at least six months in advance of Plenary meetings. Only relevant laws, regulations or other AML/CFT measures that are in force and effect by the six-month deadline to submit information for a re-rating request, will be taken into account for a re-rating.[20]

- **Peer review principle**. Assessments of a country's request for technical compliance re-ratings and preparation of the summary report will be undertaken by other members, consistent with the peer review principle of the Mutual Evaluation process.
- **Composition of the group of experts**. The group of experts may include those who were involved in that country's Mutual Evaluation, but may also consist of other experts nominated by their delegation or assigned by the ECG, if necessary. The experts will be chosen from a subgroup of delegations (open to all delegations to participate in) that

[20] This rule may only be relaxed in the exceptional case where the legislation is not yet in force at the six-month deadline, but the text will not change and will be in force by the time of the Plenary. In other words, the legislation has been enacted, but is awaiting the expiry of an implementation or transitional period before it is enforceable. In all other cases, the procedural deadlines should be strictly followed to ensure that experts have sufficient time to do their analysis.

will coordinate the analysis of re-ratings requests and conduct its business in writing. Experts from the subgroup will be assigned by the ECG Co-Chairs to review re-rating requests. The number of experts assigned to a report, and their expertise, will depend on the nature of the particular re-rating request.

- **Reporting of analysis and recommendations**. The group of experts should submit their analysis at least nine weeks before the ECG/Plenary meeting for comments to all members, associate members and observers who have two weeks to comment on the draft. If no comments are received (including from the assessed country), the report will deemed approved and proceed to publication. If comments are received, a revised report will be circulated for adoption six weeks before the ECG/Plenary meeting. If no comments on the revised report are received, the report will be deemed approved and proceed to publication. If two or more delegations (not including the assessed country) raise concerns, regarding the experts' analysis of a particular Recommendation, that Recommendation and the issues raised will be discussed at Plenary.
- Depending on the comments received, the follow-up report may be first discussed at ECG before Plenary. Where there are major disagreements between the expert reviewers and the assessed country on the findings contained in the follow-up report (e.g. re-ratings) and/or major issues raised through the pre-plenary review process, the expert review group and/or secretariat should compile a short list of the most significant issues, and should circulate this to all members, observers and associate members at least two weeks prior to the relevant working group and/or plenary discussion. The relevant working group and/or plenary discussion should prioritise discussion of these issues and should be limited in time and scope. Although follow-up reports may in some instances be first discussed at ECG, Plenary remains the only decision-making body.
- **Consideration of follow-up reports**. Follow-up reports with re-ratings for technical compliance where two or more delegations (not including the assessed country) raise concerns regarding the expert's analysis of a particular Recommendation, the report will be considered by Plenary as a discussion item. Plenary discussions on a follow-up report with technical compliance re-ratings should take, on average, no more than one hour of Plenary time. Plenary will not discuss an individual criterion rating unless it will impact an overall Recommendation rating.
- **Continued involvement of Secretariat**. The Secretariat will assist experts in achieving consistency in the application of the FATF Standards and Methodology, and will equally support the countries in follow-up. The Secretariat will also advise the ECG/Plenary on process and procedural issues (e.g., in cases where no progress has been made).

98. Follow-up reports that do not involve re-ratings should be submitted at least two months in advance of the relevant Plenary meeting. The Secretariat will conduct a desk-based analysis, and prepare a summary report with a cover note solely focusing on the follow-up process and progress. These reports will be considered by Plenary as information items.

99. In preparing the analysis and summary report for Plenary, the original assessors may be consulted, if available. The analysis and summary report will be provided to the country for its

comments before it is sent to delegations. The report will contain a recommendation regarding the next step in the follow-up process.

100. Although most follow-up reports will be considered by written process or as an information item, ECG/Plenary may opt to discuss follow-up reports that receive written comments and/or involve substantive issues. Examples of substantive issues include, but are not limited to:

- Requests for technical compliance re-ratings.
- Significant changes in a country leading to a decline in technical compliance or effectiveness.
- Insufficient progress made by a country against the priority actions in its MER.
- Recommendations to place a country in or out of enhanced follow-up.

(d) 5th Year Follow-up Assessment

101. The follow-up assessment is intended to provide a more comprehensive update on the country's AML/CFT regime. It is intended to serve a similar function as an update that is part of a country's Financial Sector Assessment Programme. This takes place five years after the adoption of the country's MER, and will occur regardless of whether the country has been in regular or enhanced follow-up. Should a country request to undertake its follow-up assessment before or after the fifth year, Plenary may approve the request on a case-by-case basis, considering the FATF's work plan and the available resources of members, ECG/Plenary, and the Secretariat.

102. The scope of the FUAs should primarily target the Immediate Outcomes (IOs) with Low or Moderate Effectiveness (LE/ME) in areas of higher risk and materiality. In principle, there will be flexibility to consider more than 4 Immediate Outcomes (IO), but on a very targeted basis (e.g. focusing only on the most important deficiencies and areas of greatest risk, rather than systematically analysing every aspect of every IO) so as to reduce the resource burden. A scoping exercise, based on a review of the MER and subsequent follow-up reports, will occur about two years before discussion of the report, in coordination with the assessors and the assessed country, and supported by the Secretariat.

103. Each FUA requires up to three assessors (preferably experts that were on the original assessment team). The FUA assessors have the same role as they do in the mutual evaluation process (responsible for analysing countries' level of effectiveness and determining whether a re-rating is appropriate). To ensure quality and consistency, each FUA is supported by one Secretariat staff. The level of the Secretariat's involvement is the same as it is in the mutual evaluation process. The FUA process will be streamlined to limit the resource burden on delegations and the Secretariat. Assessed countries should deliver their effectiveness material to the Secretariat six months before discussion of its FUA and are encouraged to present it using structured formats. As well, to the extent possible, video-/tele-conferencing may be used to narrow the issues. The onsite visit (if one is needed) occurs about 4 months before the discussion of the report. The team would prepare a progress assessment report for Plenary discussion and decision. Re-ratings on both technical compliance and effectiveness are possible, and Plenary will decide whether the country should then be placed in regular or enhanced follow up, with the process continuing as previously.

(e) Publication of Follow-Up Reports

104. The FATF publication policy applies to actions taken under the FATF's follow-up policy. Regular follow-up reports and follow-up assessment reports will be published. The Plenary will retain flexibility on the frequency with which enhanced follow-up reports are published, but they will be published whenever there is a re-rating. After adoption, and prior to publication, final follow-up reports with TC re-ratings should be provided to all assessment bodies for consideration in the post-Plenary Q&C Review described in section V of these Procedures. Follow-up reports where no issues are raised through the pre-plenary review process or during the relevant working group/plenary discussion are not subject to this post Plenary Q&C review process.

105. For follow-up reports, only the technical compliance analysis is published by the FATF, as effectiveness updates are not analysed and discussed by Plenary until the follow-up assessment. The analysis of effectiveness will be included in the publication of the follow-up assessment. If requested by a country, a link will be provided from the FATF website to a website of the country on which it has placed additional updates or other information relevant to the actions it has taken to enhance its AML/CFT system, including for effectiveness.

APPENDIX 1 – TIMELINES FOR THE 4TH ROUND MUTUAL EVALUATION PROCESS

Date[21]	Week	Key Indicative Milestones[22]		
		for Assessment Team	*for the Country*[23]	*for Reviewers*
At least 6 months before the on-site	-26	■ Commence research and desk-based review on technical compliance (TC). ■ Confirm (or find) assessors drawn from countries which had volunteered[24]. President to formally advise country of the assessors once confirmed. ■ Invite delegations to provide information about (a) assessed country's risk situation and any specific issues which should be given additional attention by assessors, (b) their international cooperation experiences with the assessed country.	■ Designate contact point(s) or person(s) and set up an internal coordination mechanisms (as necessary)[25]. ■ Respond to technical compliance update by providing updated information on new laws and regulations, guidance, institutional framework, risk and context.	

21 Differences between the timeline expressed in months and the timeline expressed in weeks are part of the flexibility that assessors and the assessed country have when determining the calendar.

22 Interaction between assessors, secretariat and country is a dynamic and continuous process. The assessment team should engage the assessed country as soon and as much as reasonably possible, and seeking and provision of information will occur throughout the process. Countries should respond to queries raised by assessment team in a timely manner.

23 The country would have to commence preparation and review of its AML/CFT regime for compliance with the FATF Standards more than six months prior to the on-site.

24 The assessment team should comprise at least four assessors, including at least one legal, law enforcement, and financial expert. Depending on the country and risks, additional assessors with the relevant expertise may be sought.

25 Contact person(s) should ideally be familiar or trained in the FATF Standards before the commencement of the process.

Date[21]	Week	Key Indicative Milestones[22]		
		for Assessment Team	*for the Country*[23]	*for Reviewers*
4 months before the on-site	-16	■ Prepare preliminary draft TC annex. ■ Analyse country's assessment of risk and discuss potential areas of increased or reduced focus for on-site[26]. ■ Confirm reviewers (drawn from pool of experts).	■ Provide response on effectiveness based on the 11 Immediate Outcomes and the underlying Core Issues (including as relevant supporting information and data).	
3 months before the on-site visit	-13	■ Send first Draft of TC annex (need not contain ratings or recommended actions) to country for comments.	■ Contact point(s) or person(s) to engage Secretariat to prepare for the on-site.	
2 months before the on-site visit	-9	■ Advise and consult country on preliminary areas of increased or reduced focus for on-site. This could involve preliminary discussions on the assessment team's impressions on the country's ML/TF risks. ■ Send draft scoping note to reviewers. ■ Prepare a preliminary analysis identifying key issues on effectiveness.	■ Provide comments on draft TC assessment. ■ Provide draft programme for on-site visit to the assessment team.[27]	■ Review draft scoping note
1 month before the on-site visit	-4	■ Final date for members and FSRBs to provide specific information on their international co-operation experiences with the country. ■ Finalise areas of increased focus for on-site visit, and key government agencies and private sector to bodies meet.		

26 This may identify a need to request additional experts with other specific expertise for the assessment team.

27 Contact point(s) or person(s) to identify and inform key government agencies and private sector bodies that would be involved for the on-site.

Date[21]	Week	Key Indicative Milestones[22]		
		for Assessment Team	*for the Country*[23]	*for Reviewers*
At least 3 weeks before the on-site	-3	■ Finalise programme and logistics arrangements for on-site.		
At least 2 week before the on-site	-2	■ Assessment team to prepare revised draft TC annex, draft TC text for MER, and outline of initial findings/key issues to discuss on effectiveness. Where possible a working draft MER prepared. Revised draft TC annex sent to country.	■ Country to provide responses to any outstanding questions from the assessment team.	
On-site Visit				
Usually 2 weeks (but may vary)	0	■ Conduct opening and closing meetings with country. A written summary of key findings is to be provided at the closing meeting. ■ Where relevant, assessment team to review the identified areas for greater focus for the on-site. ■ Discuss and draft MER.		
After the on-site visit				
Within 6 weeks of on-site visit	6	■ Assessment team to prepare the complete first draft MER and send to country for comments.		
Within 4 weeks of receipt of draft MER	10	■ Review and provide inputs on queries that country may raise.	■ Respond to first draft MER.	

Date[21]	Week	Key Indicative Milestones[22]		
		for Assessment Team	*for the Country*[23]	*for Reviewers*
Within *4 weeks* of receiving country comments	14	■ Review country's response on first draft of MER. Prepare and send second draft MER to country and reviewers. Send country comments to reviewers.		
Minimum – 10 weeks before the Plenary	17	■ Engage the assessed country to discuss further changes to the draft MER, and identify issues for discussion at the face-to-face meeting. ■ Circulate second set of assessed country comments, reviewers' comments, and assessment team's responses to reviewers, to the ECG team in the FATF secretariat.	■ Respond to second draft MER.	■ Provide comments on second draft MER.
Minimum – 8 weeks before the Plenary	*19*	■ Conduct face-to-face meeting to discuss the second draft MER & ES. ■ Work with country to resolve disagreements and identify potential priority issues for Plenary discussions. ■ If French language assessment, send final draft MER & ES for translation. [Teams may consider starting their assessment process earlier to have additional translation time].		
At least- 5 (ideally 6 weeks) before Plenary	*22*	■ Send final draft MER & ES, together with reviewers' comments, assessed country's views and assessment team response to all delegations for comments (two weeks).		

Date[21]	Week	Key Indicative Milestones[22]		
		for Assessment Team	*for the Country*[23]	*for Reviewers*
Minimum – 3 weeks before Plenary	*24*	■ Deadline for written comments from delegations.		
Two-week period before Plenary	*25*	■ Engage country and assessors on priority key issues, and other comments received on MER or ES. ■ Circulate (a) compilation of delegation comments, and (b) finalised list of priority key issues to be discussed in Plenary. ■ Review and provide inputs on priority key issues, and other comments received on MER or ES.	■ Work with assessment team on priority key issues, and other comments received on MER or ES.	
Plenary Week	*27*	**Discussion of MER**		
Post Plenary – Publication and Finalisation of MER				
The MER adopted by Plenary is to be published as soon as possible, and within six weeks, once the assessment team has reviewed it to take into account additional comments raised in Plenary, and the country confirms that the report is accurate and/or advises of any consistency, typographical or similar errors in the MER. This period to publication is inclusive of any post-Plenary quality and consistency review as required by the Universal Procedures for AML/CFT assessments.				

APPENDIX 2 – AUTHORITIES AND BUSINESSES TYPICALLY INVOLVED FOR ON-SITE VISIT

Ministries:

- Ministry of Finance.
- Ministry of Justice, including central authorities for international co-operation.
- Ministry of Interior.
- Ministry of Foreign Affairs.
- Ministry responsible for the law relating to legal persons, legal arrangements, and non-profit organisations.
- Other bodies or committees to co-ordinate AML/CFT action, including the assessment of the money laundering and terrorist financing risks at the national level.

Criminal justice and operational agencies:

- The FIU.
- Law enforcement agencies including police and other relevant investigative bodies.
- Prosecution authorities including any specialised confiscation agencies.
- Customs service, border agencies, and where relevant, trade promotion and investment agencies.
- If relevant - specialised drug or anti-corruption agencies, tax authorities, intelligence or security services.
- Task forces or commissions on ML, FT or organised crime.

Financial sector bodies:

- Ministries/agencies responsible for licensing, registering or otherwise authorising financial institutions.
- Supervisors of financial institutions, including the supervisors for banking and other credit institutions, insurance, and securities and investment.
- Supervisors or authorities responsible for monitoring and ensuring AML/CFT compliance by other types of financial institutions, in particular bureaux de change and money remittance businesses.
- Exchanges for securities, futures and other traded instruments.
- If relevant, Central Bank.

- The relevant financial sector associations, and a representative sample of financial institutions (including both senior executives and compliance officers, and where appropriate internal auditors).
- A representative sample of external auditors.

DNFBP and other matters:

- Casino supervisory body;
- Supervisor or other authority or Self-Regulatory Body (SRB) responsible for monitoring AML/CFT compliance by other DNFBPs;
- Registry for companies and other legal persons, and for legal arrangements (if applicable);
- Bodies or mechanisms that have oversight of non-profit organisations, for example tax authorities (where relevant);
- A representative sample of professionals involved in non-financial businesses and professions (managers or persons in charge of AML/CFT matters (e.g. compliance officers) in casinos, real estate agencies, precious metals/stones businesses as well as lawyers, notaries, accountants and any person providing trust and company services);
- Any other agencies or bodies that may be relevant (e.g. reputable academics relating to AML/CFT and civil societies).

Efficient use has to be made of the time available on-site, and it is therefore suggested that the meetings with the financial sector and DNFBP associations also have the representative sample of institutions/DNFBP present.

APPENDIX 3 – QUESTIONNAIRE FOR TECHNICAL COMPLIANCE UPDATE

BACKGROUND AND KEY DOCUMENTS

Countries should list the principal laws and regulations in their AML/CFT system, and give a brief, high-level summary of their scope. The (translated) text of these laws should be provided to assessors. It is preferable to assign each document a unique number or name to ensure references are consistent. These numbers should be listed here.

Countries should list the main competent authorities responsible for AML/CFT policy and operations, and summarise their specific AML/CFT responsibilities.

Countries could also briefly note any significant changes to their AML/CFT system which have taken place since the last evaluation or since they exited the follow-up process. This includes new AML/CFT laws, regulations and enforceable means and competent authorities, or significant reallocation of responsibility between competent authorities.

1. [Example –"The principal laws relevant to AML/CFT are:

- *Money Laundering Act (1963) (document L1) – establishes a criminal offence of money laundering*
- *Proceeds of Crime Act (2007) (document L2) – sets a legal framework for confiscation of the proceeds of crime*
- *National Security Act (2005) (document L3) – establishes a criminal offence of terrorist financing and a legal framework for implementing targeted financial sanctions*
- *Financial Sector Act (1999) (document L4) – provides the legal basis for financial sector regulation and supervision and sets out the basic AML/CFT obligations on firms.*

2. [Optional: Example –"Since the last evaluation, Country X has passed the 'Law on Suspicious Transaction Reporting (2009)' and established an FIU. Responsibility for investigating suspicious transactions has been transferred from the Ministry of Interior to the FIU.

RISK AND CONTEXT

Countries should provide assessors with available documents about the ML/TF risks in their country. They should list each document they provide, and briefly describe their scope. Countries should also note any important considerations about risk and context which they wish to bring to the attention of assessors. This should not duplicate information included in the documents provided. If countries wish to highlight specific contextual factors, they should provide documentation on these.

Countries should describe the size and structure of their financial and DNFBP sectors, using the tables in Annex 1.

TECHNICAL COMPLIANCE INFORMATION

Countries should provide information on their technical compliance with each of the Criteria used in the FATF Methodology.

For each criterion, countries should, as a minimum, set out the reference (name of instrument, article or section number) that applies. Countries should always specifically refer to the specific clauses of their laws, enforceable means, or other mechanisms which are relevant to each criterion. If necessary countries should also briefly explain the elements of their laws, enforceable means, or other mechanisms which implement the criterion, (e.g. an outline of the procedures followed, or an explanation of the interaction between two laws). Countries could also note whether the law or enforceable means referred to has changed since the last MER or follow-up report.

The (translated) text of all relevant laws, enforceable means, and other documents should be provided separately (but as early as possible).

Countries should provide brief factual information only – there is no need for lengthy argument or interpretation. There is no need to set out each criterion in full. Information could be provided in the following form:

Recommendation 1

Criterion 1.1

86. [Example – "Country X has conducted separate risk assessments on Money Laundering (attached as document R1) and on Terrorist Financing (edited public version attached as document R2). These risk assessments are both used as the basis for the National Strategic Plan on AML/CFT (attached as document R3) which brings together both ML and TF risks."]

Criterion 1.2

87. [Example – "The Minister of Finance has overall responsibility for AML/CFT. The National Strategic Plan on AML/CFT (document R3) assigns responsibility for ML risk assessment to the National Police Authority (page 54), and for TF risk assessment to the Interior Ministry (page 55). Actions are coordinated through the National AML/CFT Coordinating Committee (terms of reference on page 52)."]

Criterion 1.3

88. [Example – "Both ML and TF risk assessments are required to be updated on an annual basis (document R3, pages 54, 55)"]

Criterion 1.4

89. *[Example – "The ML risk assessment is a public document (document R1). The TF risk assessment is confidential but available to selected staff of all relevant competent authorities. A public version of the TF assessment is prepared which sets out key findings for financial institutions, and DNFBPs (document R2)."]*

etc.

ANNEX 1 TO THE QUESTIONNAIRE FOR TECHNICAL COMPLIANCE UPDATE: SIZE AND STRUCTURE OF THE FINANCIAL AND DNFBP SECTORS

AML/CFT PREVENTIVE MEASURES FOR FINANCIAL INSTITUTIONS AND DNFBPS (R.10 TO R.23)

Type of Entity*	No. Licensed / Regulated / Registered	AML/CFT Laws** / Enforceable Means for Preventive Measures	Date in Force or Last Updated (*where applicable*)	Other additional Information (e.g. highlights of substantive changes etc.)***
Banks				
Life Insurers				
Securities				
MVTS				
Casinos				
Lawyers				
Notaries				
Accountants				
Precious Metals & Stones Dealers				
Trust and Company Service Providers				
Others				

* Additional rows may be added for other type of financial institutions and DNFBPs. Countries may also choose to have more granular and specific classification of the types of financial institutions and DNFBPs.

** Countries should indicate the specific provisions in the AML/CFT laws that set out the CDD, record keeping and STR reporting obligations.

*** Where there have been changes since its last update or where relevant, countries should also set out the specific provisions in the AML/CFT laws or enforceable means and key highlights of the obligations for other preventive measures (e.g. politically exposed persons (PEPs), wire transfers, internal controls and foreign branches and subsidiaries etc.).

LEGAL PERSONS AND ARRANGEMENTS (R.8, R.24 AND R.25)

Type of Legal Persons / Arrangements*	**No. Registered** *(where available)*	**Applicable Laws / Regulations / Requirements**	**Date in Force or Last Updated** *(where applicable)*	**Other additional Information (e.g. highlights of substantive changes etc.)****

* Additional rows may be added for other type of legal persons or arrangements. Countries may also choose to have more granular and specific classification of the types of legal persons or arrangements.

** Countries should indicate the specific provisions in the applicable laws / regulations / requirements and key highlights that set out the obligations to maintain the requisite information in R.24 (e.g. basic and beneficial ownership) and R.25 (e.g. settlors, trustees, protectors (if any), the (class of) beneficiaries, and any other natural person exercising control) respectively.

www.fatf-gafi.org

Appendix H:

FATF, *Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations* (Paris: FATF, 2019)

Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up

"Universal Procedures"

October 2019

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and bounderies and to the name of any territory, city or area.

Citing reference:

FATF (2019), *Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up: "Universal Procedures"*, October 2019, FATF, Paris, France,
www.fatf-gafi.org/publications/mutualevaluations/documents/universal-procedures.html

CONSOLIDATED PROCESSES AND PROCEDURES FOR MUTUAL EVALUATIONS AND FOLLOW-UP

"UNIVERSAL PROCEDURES"

OCTOBER 2019

TABLE OF CONTENTS

CONSOLIDATED PROCESSES AND PROCEDURES FOR MUTUAL EVALUATIONS AND FOLLOW-UP ("UNIVERSAL PROCEDURES")

1. All Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) assessment bodies (i.e. FATF, FATF-style regional bodies (FSRBs), IMF and the World Bank) will conduct the next round of assessments in accordance with the FATF 2013 Methodology. In principle, FSRBs' and International Financial Institutions' (IFI) assessment procedures should be the same as, or close to, those of the FATF. However, as in the previous round, there will be some flexibility in the procedural arrangements. Nevertheless, there will be a set of core elements which should apply to all AML/CFT assessment bodies (as noted in the *High-Level Principles and Objectives for the relationship between the FATF and the FSRBs*[1]).

2. Based on the Procedures for the FATF 4th Round of AML/CFT evaluations, these are the "Universal Procedures" that should form the basis for the evaluations conducted by all assessment bodies. Assessment bodies should periodically review their procedures to identify on-going challenges and update their procedures to address those challenges. When a FSRB's or IFI's evaluation procedure is updated, the changes will be checked against the Universal Procedures. When the Universal Procedures are updated, e.g. after the FATF Procedures are changed, all FSRBs' and IFIs' evaluation procedures should be updated within a reasonable amount of time, and will be checked against the updated Universal Procedures. Before updating the Universal Procedures, the FATF should consider the impact of any changes on the FSRBs. Where any evaluation procedure of an assessment body continues to be inconsistent with the Universal Procedures, the FATF Secretariat would provide a paper to allow for a discussion by FATF's Evaluation and Compliance Group (ECG).

INTERACTION WITH THE EVALUATED COUNTRY

3. The assessment team, facilitated by the FATF/FSRB Secretariat or IFI contact point(s), should engage with and consult the assessed country on an on-going basis throughout the evaluation process. This may include early engagement with higher level authorities to obtain support for and co-ordination of the evaluation for the entirety of the process and training for the assessed country to familiarise stakeholders with the mutual evaluation process. Assessment bodies should review from time to time whether the way in which they engage with assessed jurisdictions is satisfactory.

4. Assessed jurisdictions should consider appointing, at an early stage in the evaluation process, a co-ordinator responsible for the mutual evaluation process to ensure adequate co-ordination and clear channels of communication between the secretariat and the assessed jurisdiction.[2]

---

1 www.fatf-gafi.org/publications/fatfgeneral/documents/high-levelprinciplesfortherelationshipbetweenthefatfandthefatf-styleregionalbodies.html

2 The co-ordinator should have the appropriate seniority to be able to co-ordinate with other authorities effectively and make certain decisions when required to do so. The co-ordinator should also have an understanding of the mutual evaluation process and be able to perform quality control of responses provided by other agencies.

SETTING AND RESPECTING TIMELINES AND OTHER ASPECTS OF THE MUTUAL EVALUATION PROCESS

5. Assessment bodies should develop timelines for the evaluation process, following the FATF approach[3]. Timelines should include key milestones for the process and the relevant responsibilities of the assessment team, the assessed country and the reviewers at each of the various steps, together with remedial action for cases where the timelines are not observed.

6. The assessed countries and assessment teams have the flexibility to extend the overall timeline by up to one or two months in order to plan around plenary meetings, events or holidays or to adjust the date of the on-site visit to the most appropriate time. When translation is needed, assessment bodies should ensure that at least 3 to 4 extra weeks are scheduled for translation purposes. In practice, these extensions may require an earlier start to the evaluation process as there is no scope for reducing the time allocated to the post-onsite stages of the process. Therefore, the assessed country and assessment team should therefore agree on the broad timeline of the evaluation at least 14 months before the plenary discussion.

7. The timelines are intended to provide guidance on what is required if the reports are to be prepared within a reasonable timeframe, and in sufficient time for discussion in Plenary. It is therefore important that both the assessors and the assessed country respect the timelines.

8. Delays may significantly impact the ability of the Plenary to discuss the report in a meaningful way. The draft schedule of evaluations has been prepared so as to allow enough time between the on-site visit and the Plenary discussion. A failure to respect the timetables may mean that this would not be the case. By agreeing to participate in the mutual evaluation process, the country and the assessors undertake to meet the necessary deadlines and to provide full, accurate and timely responses, reports, or other material as required under the agreed procedure. Where there is a failure to comply with the agreed timelines, then the following actions could be taken (depending on the nature of the default):

a) Failure by the country-The assessment body's President/Chair may write to the head of delegation or the relevant Minister in the country. The Plenary will be advised as to the reasons for deferral, and publicity could be given to the deferment (as appropriate) or other additional action considered. In addition, the assessment team may have to finalise and conclude the report based on the information available to them at that time.

b) Failure by the assessors, the reviewers or the Secretariat - the assessment body's President/Chair may write a letter to or liaise with the head of delegation of the assessor or the reviewer, or the assessment body's Executive Secretary (for the Secretariat).

9. The Secretariat will keep the Presidency/Chairmanship advised of any failures so that the President/Chairman can respond in an effective and timely way. The Plenary is also to be advised if the failures result in a request to delay the discussion of the MER.

[3] See Appendix 1 of the FATF Procedures

ASSESSMENT TEAMS AND SECRETARIAT SUPPORT

10. Assessors should be very knowledgeable about the FATF Standards, and are required to attend and successfully complete an assessor training event before they conduct a mutual evaluation. Assessment bodies should implement the criteria for selecting and assessing the level of expertise of persons attending assessor training events, including those criteria approved by the FATF Plenary.[4] To ensure that the mutuality of the peer review process is maintained, members should provide qualified experts. It is also important that assessors are able to devote their time and resources to reviewing all the documents (including the information updates on technical compliance, and information on effectiveness), raising queries prior to the on-site, preparing and conducting the assessment, drafting the MER, attending the meetings (e.g. on-site, face-to-face meeting, and Plenary discussion), and adhere to the deadlines indicated.

11. Assessment teams should have the correct balance of knowledge and skills to ensure a quality mutual evaluation. To the extent possible, the following factors should be considered before confirming an assessor to participate in a mutual evaluation: (i) their relevant operational and assessment experience; (ii) language of the evaluation; (iii) nature of the legal system (civil law or common law) and institutional framework; and (iv) specific characteristics of the jurisdiction (e.g. size and composition of the economy and financial sector, geographical factors, and trading or cultural links).

12. Through the mutual evaluation process, the FATF/FSRB Secretariat or IFI contact point(s) supports the assessment team and the assessed country. This support includes:

- Project-leading the process and undertaking other tasks as indicated in the applicable procedures;
- Focusing on quality and consistency of the MER, including taking steps necessary to ensure that the assessors' analysis is clearly and concisely written, comprehensive, objective and supported by evidence;
- Ensuring compliance with processes and applicable procedures;
- Assisting and guiding the assessors and assessed country in the interpretation of the FATF Standards and Methodology in line with past FATF Plenary decisions; and
- Ensuring that assessors and assessed countries have access to relevant and accurate documentation and that statistics and legislative references are cited correctly.

13. Assessment bodies should review from time to time whether their respective Secretariat is staffed to adequately support the mutual evaluation process, understanding that 2 or 3 staff members should be considered optimal for the majority of evaluations. Where resource issues exist, the assessment body should review its work plan and allocation of resources to other projects to ensure that work on MERs/FURs is adequately prioritised.

PREPARATION FOR THE ON-SITE VISIT

14. The assessment team, supported by the secretariat, will conduct a desk-based review for technical compliance (TC), based on the necessary updates and information (background information

[4] See, e.g. FATF/PLEN/RD(2018)21

on the institutional framework, risks and context and information on the measures taken to meet the criteria for each Recommendation) provided by the assessed country and other reliable sources (e.g. reports from other international organisations). The assessed country should rely on the questionnaire template for the technical compliance update[5] to provide relevant information to the assessment team.

15. A draft of the TC compliance annex, which need not include ratings nor recommendations, will be provided to the assessed country in sufficient time before the on-site visit for it to provide comments.

16. The FATF Methodology requires that in conducting their analysis, assessors should only take into account relevant laws, regulations or other AML/CFT measures that are in force and effect at that time, or will be in force and effect by the end of the on-site. Where relevant bills or other firm proposals to amend the system are made available, these will be referred to in the Mutual Evaluation Report (MER)[6] (including for the purpose of the analysis and recommendations to be made to the assessed country) but should not be taken into account for ratings purposes unless they are in force and effect at the time of the on-site.

17. Countries should provide information on effectiveness. For each of the 11 Immediate Outcomes, they should set out fully how each of the core issues is being addressed. It is important for countries to provide a full and accurate description (including examples of information, data and other factors) that would help to demonstrate the effectiveness of the AML/CFT regime. Other countries which are FATF and FSRB members should be invited to provide information on their experience of international co-operation with the country being evaluated, or any other AML/CFT issues that they would like to see raised and discussed during the on-site visit. In addition, the assessment team and the assessed country may also identify key countries which the assessed country has provided international cooperation to or requested it from, and seek specific feedback. The onus is on the assessed country to provide all relevant and necessary information, both in relation to technical compliance and effectiveness.

18. Based on its preliminary review and analysis of the risks and the assessed country's situation prior to the on-site, the assessment team may identify specific areas which it would pay more attention to during the on-site visit and in the MER. In doing so, the team will consult the assessed country. This will usually relate to effectiveness issues but could also include technical compliance issues. Delegations will be invited to provide any information and comments that they may have that would assist the team to prepare a short scoping note identifying areas of lower and higher risk that need reduced or increased focus. The scoping note should set out briefly the areas for increased and reduced focus, and the rationale. The draft scoping note, along with relevant background information (e.g. the country's risk assessment(s)), should be sent to the reviewers (described in the section on quality and consistency, below) and to the assessed country.

19. There should be adequate confidentiality requirements that apply to the assessment team, Secretariats, reviewers, officials in the assessed country and any other person with access to assessment documents or information.

---

5 See Appendix 3 of the FATF Procedures for an example, or refer to templates that some FSRBs have created.

6 References to MER include detailed assessment reports (DAR) prepared by IFIs.

ON-SITE VISIT

20. The on-site visit will include the following:

- An initial internal preparatory meeting for the assessment team.
- Meetings[7] with representatives of the assessed country, the private sector or other relevant non-government bodies or persons[8], including an opening and closing meeting. The opening meeting should consider including an overview of the country's understanding of risk, to complement the write-ups of the country's national risk assessment(s). The programme of meetings should take into account the areas where the assessment team may want to apply increased and reduced focus. Time may have to be set aside for additional or follow-up meetings, if, in the course of the set schedule, the assessors identify new issues that need to be explored, or if they need further information on an issue already discussed.
- Typically, an onsite programme would also include 1-2 days where the assessors work only on the draft MER (supported by the Secretariat), ensuring that all the major issues that arose during the evaluation are noted in the report, and discusses and agrees ratings and key recommendations.
- The assessment team should provide a written summary of its key findings to the assessed country officials at the closing meeting.

AFTER THE ON-SITE VISIT

21. There should be an adequate amount of time between the end of the on-site visit and the discussion of the MER[9] in Plenary in order to complete all the steps below (noting the timeline set out in Appendix 1 of the FATF *Procedures*).

22. The assessment team will prepare, coordinate and refine a draft MER and the Executive Summary, including the key findings, as well as the preliminary recommendations and ratings. This will then be sent to the assessed country, which should have at least 4 weeks to review and provide its comments on the draft MER to the assessment team.

23. With the aim to facilitate communication between the assessment team and the assessed country, the Secretariat should facilitate regular conference calls between all parties when necessary; in particular after the circulation of an updated draft MER. When writing-up the draft MERs and/or during calls, assessors should aim to clarify in writing or orally as much as possible how information

---

7 The assessment team should also set aside time midway through the on-site to review the progress of the mutual evaluation and where relevant, the identified areas of increased focus for the on-site.

8 Generally, assessors should be given the opportunity to meet with such bodies or persons in private without a government official present, not only if there is concern that the presence of the officials may inhibit the openness of the discussion. The team may also request that meetings with certain government agencies are restricted to those agencies only.

9 The format for the Executive Summary and MER is contained in Annex II of the Methodology. Assessors should also pay attention to the guidance on how to complete the Executive Summary and MER, including with respect to the expected length of the MER (100 pages or less, together with a technical annex of up to 60 pages).

submitted by the assessed country was taken into account[10], if/where additional information is still needed.

24. On receipt of the assessed country's comments on the draft MER and Executive Summary, the assessment team will review the various comments and make further amendments. Every effort should be made to ensure that the revised draft is as close to a final draft MER as possible. The revised draft MER and Executive Summary will then be sent to the reviewers and the assessed country.

QUALITY AND CONSISTENCY REVIEW

25. All assessment bodies will have an effective and robust mechanism in place to ensure the review of the quality and consistency of their own reports that meets the following principles:

a) *Equivalent Purpose and Rigour* – the mechanism for ensuring quality and consistency should have the same objective, and be of equivalent rigour, to the FATF Quality and Consistency review. FSRBs and IFIs should adopt and follow the same quality and consistency procedures as the FATF (set out in section IV (l) of the FATF Procedures), except where the ECG agrees to an alternative procedure.

b) *Scoping* – the mechanism should consider whether the assessors' draft scoping note reflects a reasonable view on the focus of the assessment, and should provide feedback to the assessment team.

c) *External Involvement* – the mechanism should include at least one expert from outside the assessment body (e.g. from the FATF, IFI, or another FSRB).

26. Following the receipt of the reviewers' and assessed country's comments, assessors should respond to all substantive comments by external reviewers and the Secretariat should liaise with external reviewers as needed to facilitate this process. The Secretariat will engage the assessed country to discuss further changes to the draft MER, and identify issues for discussion at the face-to-face meeting or video/teleconference.

INTERACTION WITH THE COUNTRY BEFORE THE PLENARY DISCUSSION

27. The assessment team (including Secretariat) and the assessed country should have a face to face meeting to further discuss the draft MER and Executive Summary. During this session, the assessment team and assessed country should work to resolve any disagreements over technical compliance or effectiveness issues and identify potential priority issues for Plenary discussion. If a meeting is not possible then there should at a minimum be a video or teleconference. Where significant substantive changes are made to the MER after the face-to-face meeting, the FATF/FSRB Secretariat should consider circulating a revised second draft to external reviewers for a targeted review.

PLENARY DISCUSSION

28. The revised Executive Summary and MER, together with the conclusions of the quality and consistency mechanism, and assessors' response, will then be sent to all members, associate members and observers, including FATF (for circulation to FATF members), at least five weeks (ideally six weeks) prior to Plenary for their comments. There should be no further changes to the substance of

[10] Assessors need not include all the information submitted by the assessed country, and should exercise discretion in determining which information are the most relevant to be included.

the draft MER thereafter to allow delegations to provide comments and prepare for the discussion at Plenary (and/or the working group prior to Plenary, if any). Delegations should have sufficient time (ideally two weeks) to provide written comments on the MER and Executive Summary, and in particular, to identify any key issues that they wish to discuss in the relevant working group (if any) and Plenary. The comments should focus on the substantive key issues, or on other high-level or horizontal aspects of the assessment, though other observations may also be made. The comments received will be made available to all delegations. A similar process and timeline should be applied in relation to assessments of countries that are not members of FSRBs, with the documents provided well in advance of finalisation.

29. Ideally three weeks preceding the Plenary, the Secretariat should engage the assessed country and the assessors on priority issues, and other comments received on the MER or Executive Summary and prepare a list of priority and substantive key issues that will be discussed in Plenary and/or Working Group. Key issues should focus on effectiveness, but may include issues related to technical compliance, and should take into account the issues that the assessed country and delegations are most keen to discuss, as well as the assessed country's risk and context. The list of substantive key issues (usually five to seven) will be circulated to all delegations at least two weeks prior to the Plenary discussion.

30. The MER will be discussed in Plenary and/or Working Group (particularly the list of key issues) and should focus on high-level and substantive key issues, primarily concerning effectiveness. Where appropriate, important technical issues would also be discussed.. The President/Chair should manage the discussions and the time for discussion should be limited to a reasonable length (ideally three to four hours). The procedure for the discussion will be as follows:

- Assessment team briefly presents, in high-level terms, the key issues and findings from the report. The team will have the opportunity to intervene/comment on any issue concerning the Executive Summary or MER.
- Assessed country makes a short opening statement.
- The Plenary discusses the list of key issues.
- Time permitting, other issues could be raised from the floor, and discussed by the Plenary.

31. The representative of the FATF Secretariat at the Plenary will be expected to assist and advise on all issues relating to the interpretation of the Recommendations, and the quality and consistency aspects of the draft MERs. The Plenary discussion will provide members and observers adequate opportunity to raise and discuss concerns about the quality and consistency of an MER. At the end of the Plenary discussion, the MER and the Executive Summary will be submitted to the Plenary for adoption.[11]

PUBLICATION AND OTHER PROCEDURES FOLLOWING THE PLENARY

32. Following the Plenary discussion of the report, the Secretariat will work with the assessors to amend all documents as agreed by the Plenary, and will circulate a revised version of the report to

[11] Within an FSRB, the term "the Plenary" refers to the body of senior officials representing member countries.

the assessed country. The assessed country must confirm that the MER is accurate and/or advise of any typographical or similar errors in the MER.

Post plenary quality and consistency review

33. Where an FATF or FSRB member, the FATF Secretariat, FSRB Secretariat or an IFI considers that a FATF or FSRB report has significant problems of quality and consistency (Q&C), it should wherever possible raise such concerns with the body conducting the assessment (the assessment body) prior to adoption. The assessment body, assessment team and assessed country should consider and work to appropriately address the concerns.

34. Nevertheless, highly exceptional situations may arise where significant concerns about the Q&C of a report remain after its adoption. To address such issues, the post-Plenary Q&C process applies to all assessment bodies with a view to preventing the publication of reports with significant Q&C problems and ensuring that poor quality assessments do not damage the FATF brand.

35. The post-Plenary quality and consistency (Q&C) review process applies to all mutual evaluation reports (MERs) (including their executive summaries), detailed assessment reports (DARs)[12] (including their executive summaries), mutual evaluation follow-up reports with technical compliance re-ratings (FURs) and follow-up assessment reports (FUARs), regardless of which assessment body prepared the report.[13] The exception is FURs with technical compliance (TC) re-ratings where no Q&C issues are raised through the pre-plenary review process or during the relevant working group/plenary discussion. Such FURs are not subject to the post-Plenary review process and ordinarily should be published within six weeks after their adoption by Plenary.

Steps in the post-Plenary Q&C process

36. After adoption of the report, the assessment body will amend all documents as necessary and will circulate a revised version of the report to the country within one week of the Plenary. Within two weeks of receiving it from the assessment body, the country must confirm that the report is accurate and/or advise of any typographical or similar errors. Care will be taken to ensure that no confidential information is included in any published report. The assessment body will then forward the final version of the report to the FATF Secretariat.

37. Where an FSRB has a Council of Ministers, or equivalent body, the report should be adopted at the meeting of officials (the Plenary), and there should be no delay in publication due to the need to have the approval or recognition of Ministers regarding the reports.

38. The FATF Secretariat will then circulate the report to all the FATF members, FSRBs and the IFIs, along with a template for referring Q&C issues for consideration. FSRBs should forward the report and template to all of their members for consideration. Parties who identify any serious or major Q&C issues have two weeks to advise the FATF Secretariat (for FATF reports) or both the FATF

12. Where the evaluation is conducted by one of the International Financial Institutions (IFI) (IMF or World Bank).

13 In this section, MERs, DARs, FURs and FUARs are collectively referred to as *reports.*

Secretariat and assessment body (for non-FATF reports)[14] in writing, using the template provided to indicate their specific concerns and how these concerns meet the substantive threshold.

39. To be considered further in this process, a specific concern should be raised by at least two of the following parties: FATF or FSRB members [15]or Secretariats or IFIs, at least one of which should have taken part in the adoption of the report. Otherwise, the post-Plenary Q&C review process is complete, the FATF Secretariat will advise the assessment body and delegations accordingly and the report will be published.[16]

40. If two or more parties identify a specific concern, the Co-Chairs of the FATF Evaluations and Compliance Group (ECG) will review the concern to determine whether *prima facie* it meets the substantive threshold and procedural requirements. To aid in this decision, the FATF Secretariat will liaise with the relevant FATF or FSRB Secretariat team to provide the ECG Co-Chairs with any necessary background information on the issue, including (where relevant and appropriate):

a) information submitted by parties raising the Q&C issue

b) background information on any related comments raised at the pre-Plenary stage

c) the rationale for the relevant rating/issue under discussion based on the facts in the report and/or any relevant co-chairs' report or summary record from the working group/Plenary meeting where the report was discussed (including whether the issue was discussed in detail, what the outcome of the those discussions was and any reasons cited for maintaining or changing the rating or report)

d) objective cross-comparisons with previous FATF reports that have similar issues

e) the report's consistency with the corresponding parts of the Methodology

f) any connection or implications for the ICRG process, and

g) what next steps might be appropriate.

41. If the ECG Co-Chairs conclude that *prima facie* the substantive threshold and procedural requirements are met, the Secretariat will circulate the report to all FATF delegations for consideration by the ECG along with a decision paper prepared by the FATF Secretariat in consultation with the relevant assessment body (FSRB/Secretariat/IFI). On the other hand, if the ECG Co-Chairs conclude that *prima facie* the substantive threshold and procedural requirements are not met, the issue would not be taken forward for discussion, but a short note explaining the Co-Chair's position would be presented to ECG for information.

42. Issues identified less than four to six weeks before the FATF Plenary will be discussed at the next FATF Plenary to ensure sufficient time for consultation among Secretariats and preparation of the decision paper. The decision paper prepared by the FATF Secretariat in consultation with the

14 Where FATF or FSRB members or secretariats consider that an MER which has been adopted by an IFI has or continues to have significant problems of quality or consistency, they should promptly inform the IFI of those concerns (and the FATF Secretariat when the concerns are raised by others).

15 Not including the assessed country.

16 Ordinarily, publication would happen within six weeks of the report being adopted if no further steps in the post-Plenary Q&C process are needed.

relevant assessment body will include the background information listed above in paragraph 35 to the extent that it is relevant and appropriate.

43. The ECG will decide whether the report meets the substantive threshold (serious or major issues of Q&C with the potential to affect the credibility of the FATF brand as a whole). Examples of situations meeting this substantive threshold include:

a) the ratings are clearly inappropriate and not consistent with the analysis

b) there has been a serious misinterpretation of the Standards, Methodology and/or Procedures

c) an important part of the Methodology has been systematically misapplied, or

d) laws that are not in force and effect have been taken into account in the analysis and ratings of a report.

44. If ECG decides that the report meets the substantive threshold, it will refer the matter to the FATF Plenary along with clear recommendations on what action would be appropriate (e.g. requesting that the relevant assessment body reconsiders the report and/or makes appropriate changes before any publication). On the other hand, if ECG decides that the report does not meet the substantive threshold, the FATF Secretariat will advise the assessment body and delegations that the post-Plenary Q&C review is complete, and the report will be published.

45. Where ECG has referred a post-Plenary Q&C issue, the FATF Plenary will discuss the matter and decide on the appropriate action. The Secretariat will advise the assessment body of the FATF Plenary's decision. If the assessment body declines to respond to the action requested by the FATF, the FATF Plenary will consider what further action may be necessary. The assessment body will not publish the report until the issue is resolved within FATF and the assessment body, and the FATF Secretariat advises that the post-Plenary Q&C review process is complete.

46. Following completion of the post-Plenary Q&C review process, the assessment body will publish the report on its website. Additionally, the FATF publishes all reports on its website to give timely publicity to an important part of the work of FATF and the global network.

FOLLOW-UP PROCESS

47. The FATF and FSRBs should have transparent, clear and rules-based follow-up procedures, to which all members commit and which they apply rigorously and consistently. In particular, the procedures should enable FATF and the FSRBs to track progress made by countries in addressing their AML/CFT risks and deficiencies, to focus on countries which do not make sufficient progress in addressing their risks and deficiencies, and to exert pressure on such countries to improve their performance.

48. The FATF and FSRBs' follow-up procedures should include two types of process:

- Regular follow-up as the default monitori ng mechanism, based on a system of regular reporting.
- Enhanced follow-up, involving a more intensive process of follow-up, for countries with significant deficiencies, or countries making insufficient progress. In deciding whether to place a country in enhanced follow-up, the Plenary should consider both the level of technical compliance and of effectiveness reached by the country.
  - As regards technical compliance, a country would be placed into enhanced follow up if it has 8 or more NC/PC ratings for technical compliance, or is rated NC/PC on any one or more of

R.3, 5, 10, 11 and 20. A country would also be placed into enhanced follow-up if, during the regular follow-up process, its level of technical compliance changed to a level that the Plenary considers as equivalent to NC/PC on any one or more of R.3, 5, 10, 11 and 20.

- As regards effectiveness, the assessment body should consider what a reasonable level of effectiveness should be. In principle, FSRBs should aim to apply the same threshold as the FATF, i.e. a country would be placed into enhanced follow-up if it has a low or moderate level of effectiveness for 7 or more of the 11 effectiveness outcomes, or it has a low level of effectiveness for 4 or more of the 11 effectiveness outcomes.

49. Follow-up reports should be analysed by the Secretariat and/or the relevant FATF or FSRB review group, who should highlight both the progress made and the remaining deficiencies, and propose timelines to take remedial actions. Only NC/PC rated Recommendations are eligible for a technical compliance re-rating request. Re-ratings for technical compliance may be allowed if the follow-up report, and other relevant information submitted by the country, provides sufficient justification for the Plenary to come to such a conclusion based on the analyses conducted by the Secretariat/the relevant Review Group. Re-rating requests will not be considered where the Secretariat/the relevant Review Group determines that the legal, institutional, or operational framework has not changed since the country's MER (or previous FUR, if applicable) and there have been no changes to the FATF Standards or their interpretation.[17] The general expectation[18] is for countries to have addressed most if not all of the technical compliance deficiencies by the end of the 3rd year after the adoption of the MER.

50. Countries seeking a technical compliance re-rating should indicate on which Recommendations a re-rating will be requested, seven months in advance of Plenary meetings and submit any information to justify the re-rating ideally six months in advance of Plenary meetings. Only relevant laws, regulations or other AML/CFT measures that are in force and effect by the deadline to submit information for a re-rating request, will be taken into account for a re-rating.

51. Follow-up reports with technical compliance re-ratings should be circulated to all members, associate members and observers, including FATF (for circulation to FATF members), at least five weeks prior to discussion in the relevant working group and/or plenary meeting, who have two weeks to provide written comments on such reports. Where there are major disagreements between the expert reviewers and the assessed country on the findings contained in the follow-up report (e.g. re-ratings) and/or major issues raised through the pre-plenary review process, the expert review group and/or secretariat should compile a short list of the most significant issues, and should circulate this to all members, observers and associate members at least two weeks prior to the relevant working group and/or plenary discussion. The relevant working group and/or plenary discussion should prioritise discussion of these issues and should be limited in time and scope, for example, FSRBs could consider excluding the discussion of an individual criterion rating unless it will have an impact on the overall Recommendation rating. FSRBs can also opt to approve follow-up reports through written process, in line with written process procedures already available in the relevant FSRB. At a minimum, if comments are raised when a report is circulated for approval by written process, Secretariats should work with expert reviewers and the assessed country to amend

17 Where there is disagreement between the expert(s) and the assessed country in this respect, they should discuss with WG Co-Chairs to achieve an agreement.

18 It is up to the Plenary to determine the extent to which its members are subject to this general expectation, depending on the member's context.

the report and address comments received. The report would be then circulated again for approval and be discussed in Plenary if any other comments are raised.

52. In the exceptional case that it comes to the Plenary's attention that a country has significantly lowered its compliance with the FATF Standards, the Plenary may request the country to address any new deficiencies as part of the follow-up process. If any of the FATF Standards have been revised since the end of the on-site visit, the country will be assessed for compliance with all revised standard at the time its re-rating request is considered (including cases where the revised Recommendation was rated LC or C).

53. For countries subject to review by the International Cooperation Review Group (on the basis of an agreed ICRG action plan), no reporting is expected on the Recommendations that are included in an ongoing ICRG action plan. However, overall progress on each Recommendation is still expected to be achieved, including on parts of Recommendations that are not covered by the ICRG action plan, under the normal timelines, or as soon as the country has completed its ICRG action plan (if this is after the regular timelines).

54. The follow-up procedures should include a range of graduated measures (including letters to Ministers, high level visits and public statements regarding the level of compliance) to be taken if countries fail to meet their commitment or make insufficient progress in addressing their priority actions. The follow-up procedures should also include how countries can be moved to regular follow-up from enhanced follow-up if the country no longer meets the criteria for enhanced follow-up.

55. The follow-up procedures should require all countries to be submitted to a follow-up assessment, which should take place within a reasonable timeframe (normally five years) after the initial MER, though this should take into account the total duration of the assessment body's round of MEs.

56. This would focus on the progress made by the country on the priority actions in its MER, and other areas where the country had significant deficiencies. The follow-up assessment could also examine any other elements of the country's AML/CFT regime which have changed significantly as well as high-risk areas identified in the MER or noted subsequently in the follow-up process. The process for the follow-up assessment should include a short on-site visit (2/3 days) to assess improvements in effectiveness and other areas. Re-rating on both TC and effectiveness are possible.

Publication of Follow-up Reports

57. The general publication policy of FATF and FSRBs applies to actions taken under the follow-up policy. Regular follow-up reports and their analysis made by the Secretariat/the relevant Review Group, and the follow-up assessment reports will be published. The Plenary will retain flexibility on the frequency with which enhanced follow-up reports are published, but they will be published whenever there is a re-rating. After adoption, and prior to publication, final follow-up reports with TC re-ratings should be provided to the FATF Secretariat and all other assessment bodies for consideration in the post-Plenary Q&C Review process described in the Post-Plenary Quality and Consistency Review section of these Procedures. Follow-up reports where no issues are raised through the pre-plenary review process or during the relevant working group/plenary discussion are not subject to this post-Plenary Q&C review process.

JOINT MUTUAL EVALUATIONS FATF/FSRBS

58. In line with FATF's policy, FATF members that are also members of FSRB(s) will undergo a joint evaluation by these bodies. Generally, the FATF will be the principal organiser, and will provide three assessors, while one or two assessors could be provided by the participating FSRBs. The assessors will be supported by the FATF and the FSRB(s) Secretariats. The first discussion of the MER should take place in the FATF, and given the additional measures adopted for joint evaluations, the presumption is that the FATF's view would be conclusive.

59. The process (including the FATF procedures for preparing the draft MER and Executive Summary) for joint evaluations would be the same as for other FATF evaluations, with the FSRB and its members having opportunities to participate directly through being part of the assessment team, and also being able to provide comments and input like other delegations. FSRBs should allow reciprocal participation in mutual evaluation discussions for FATF members. Measures for joint evaluations defined in the FATF Procedures will apply.

IFI-LED ASSESSMENTS

60. The FATF and FSRBs are in principle responsible for the mutual evaluation process for all of their members, and there is a presumption that they will conduct the mutual evaluations[19] of all their members as part of this process. The presumption can be overridden on a case by case basis.

61. For the FATF and FSRB assessment schedules to be fixed with appropriate certainty and in a coordinated manner, and for assessment teams to be formed in sufficient time, the process leading to a decision about which countries will have an assessment led by an IFI team should be clear and transparent. The FATF and FSRBs are to be involved at an early stage in the process of determining which countries will be assessed by an IFI (including receiving advice regarding proposals for IFI-led assessments). Where the IMF or World Bank conducts an AML/CFT assessment of an FATF/FSRB member, they should use procedures and a timetable similar to those of the FATF/FSRB, including any procedures that the FATF/FSRB has in addition to what is required by the Universal Procedures.

62. The FATF and/or FSRB Plenary will in all cases have to approve an IFI assessment for it to be accepted as a mutual evaluation.

[19] Including any follow-up that may be required.

Based on the Procedures for the FATF 4th Round of anti-money laundering (AML) and countering the financing of terrorism (CFT) evaluations, these are the "Universal Procedures" that should form the basis for the evaluations conducted by all assessment bodies: FATF, FATF-Style Regional Bodies, IMF and the World Bank.

Contact the FATF

FATF Secretariat
2 rue André Pascal
75775 Paris Cedex 16, France
Tel: +33 (0) 1 45 24 90 90
Fax: + 33 (0) 1 44 30 61 37
contact@fatf-gafi.org
www.fatf-gafi.org

Appendix I:

FATF, *Consolidated Table of Assessment Ratings* (Paris: FATF, 2020)

Updated 30 April 2020

Effectiveness
Ratings that reflect the extent to which a country's measures are effective. The assessment is conducted on the basis of 11 immediate outcomes, which represent key goals that an effective AML/CFT system should achieve. For more information see:

FATF Methodology

Technical Compliance
Ratings which reflect the extent to which a country has implemented the technical requirements of the FATF Recommendations.
For more information see:

FATF Methodology FATF Recommendations

Jurisdiction (click on the country name to go to the report on www.fatf-gafi.org)	Report Type	Report Date	Assessment body/bodies	IO1	IO2	IO3	IO4	IO5	IO6	IO7	IO8	IO9	IO10	IO11	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10	R.11	R.12	R.13	R.14	R.15	R.16	R.17	R.18	R.19	R.20	R.21	R.22	R.23	R.24	R.25	R.26	R.27	R.28	R.29	R.30	R.31	R.32	R.33	R.34	R.35	R.36	R.37	R.38	R.39	R.40	#upgrades	#downgrades
Albania	MER+FUR	Dec/19	MONEYVAL	ME	ME	ME	SE	ME	SE	ME	ME	LE	ME	LE	LC	LC	LC	LC	LC	C	NC	LC	LC	LC	LC	LC	LC	C	LC	LC	N/A	LC	C	LC	C	LC	LC	PC	PC	PC	LC	PC	LC	C	LC	LC	LC	LC	LC	PC	LC	LC		
Albania	MER	Dec/18	MONEYVAL	ME	ME	ME	SE	ME	SE	ME	ME	LE	ME	LE	LC	LC	LC	LC	LC	PC	NC	PC	LC	LC	LC	LC	LC	C	LC	LC	N/A	PC	PC	LC	LC	LC	LC	PC	PC	PC	LC	PC	LC	C	LC	LC	LC	LC	LC	PC	LC	LC		
Albania	FUR1	Dec/19	MONEYVAL	ME	ME	ME	SE	ME	SE	ME	ME	LE	ME	LE	LC	LC	LC	LC	LC	*C*	NC	*LC*	LC	LC	LC	LC	LC	C	LC	LC	N/A	*LC*	*C*	LC	*C*	LC	LC	PC	PC	PC	LC	PC	LC	C	LC	LC	LC	LC	*LC*	LC	LC	PC	LC	LC	6	
Andorra	MER+FUR	Dec/18	MONEYVAL	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME	LC	C	LC	C	LC	LC	C	PC	LC	LC	C	LC	LC	LC	C	LC	LC	C	LC	C	C	C	LC	LC	LC	LC	LC	LC	C	PC	C	LC	LC	LC	PC	LC	LC	LC		
Andorra	MER	Sep/17	MONEYVAL	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME	LC	PC	PC	C	LC	LC	C	PC	LC	LC	LC	PC	LC	LC	PC	PC	LC	LC	C	LC	LC	PC	PC	LC	PC	PC	LC	PC	LC	C	PC	PC	LC	PC	LC	PC	LC	LC	LC		
Andorra	FUR1	Dec/18	MONEYVAL	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME	LC	*C*	*LC*	C	LC	LC	C	PC	LC	LC	*C*	*LC*	LC	LC	*C*	*LC*	LC	LC	C	*C*	*C*	*LC*	*LC*	LC	LC	PC	LC	PC	C	LC	*LC*	LC	LC	LC	LC	LC	LC	LC	LC	12	
Andorra	FUR2	Dec/19	MONEYVAL	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME	LC	C	LC	C	LC	LC	C	PC	LC	LC	C	LC	LC	LC	C	LC	LC	LC	C	C	C	LC	LC	LC	LC	LC	PC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	3	
Antigua & Barbuda	MER	Jul/18	CFATF	ME	ME	LE	ME	ME	ME	LE	ME	ME	LE	LE	LC	LC	LC	LC	C	PC	NC	NC	C	LC	LC	LC	C	LC	C	LC	C	C	C	C	LC	PC	LC	LC	LC	LC	LC	C	PC	LC	PC	LC	LC	LC	C	PC	LC	PC		
Armenia	MER+FUR	Jul/18	MONEYVAL	ME	SE	ME	SE	SE	ME	LE	LE	SE	SE	SE	LC	LC	LC	LC	LC	LC	LC	C	C	LC	C	PC	C	C	C	C	C	C	C	C	C	LC	C	LC	LC	PC	C	C	C	LC	LC	LC	LC	LC	C				
Armenia	MER	Jan/16	MONEYVAL	ME	SE	ME	SE	SE	ME	LE	LE	SE	SE	SE	PC	LC	LC	LC	LC	LC	PC	LC	C	LC	C	PC	C	C	C	C	C	C	C	C	C	LC	C	LC	LC	PC	C	C	C	LC	LC	LC	LC	LC	C				
Armenia	FUR1	Jul/18	MONEYVAL	ME	SE	ME	SE	SE	ME	LE	LE	SE	SE	SE	*LC*	LC	LC	LC	LC	LC	*LC*	*C*	C	LC	C	PC	C	C	C	C	C	C	C	C	C	LC	C	LC	LC	LC	C	PC	C	LC	PC	C	C	C	LC	LC	LC	LC	LC	C	3	
Australia	MER+FUR	Oct/18	FATF/APG	SE	HE	ME	ME	ME	SE	ME	ME	SE	ME	SE	PC	LC	C	C	C	C	C	LC	C	PC	LC	LC	NC	LC	C	PC	PC	PC	LC	C	C	NC	NC	PC	NC	PC	PC	NC	C	C	LC	C	C	LC	LC	PC	C	C	C	C		
Australia	MER	Apr/15	FATF/APG	SE	HE	ME	ME	ME	SE	ME	ME	SE	ME	SE	PC	LC	C	C	LC	C	C	NC	C	PC	LC	LC	NC	LC	LC	PC	PC	PC	PC	C	C	NC	NC	PC	NC	PC	PC	NC	C	LC	LC	LC	LC	LC	PC	LC	C	C	C	C		
Australia	FUR1	Oct/18	FATF/APG	SE	HE	ME	ME	ME	SE	ME	ME	SE	ME	SE	PC	LC	C	C	*C*	C	C	*LC*	C	PC	LC	LC	NC	LC	*C*	PC	PC	PC	*LC*	C	C	NC	NC	PC	NC	PC	PC	NC	C	*C*	LC	LC	PC	*C*	C	C	C	C	7	
Austria	MER+FUR	Nov/18	FATF	ME	SE	ME	ME	ME	LE	LE	ME	SE	ME	SE	LC	LC	LC	C	C	PC	PC	PC	C	C	C	C	LC	C	C	C	LC	C	C	C	C	LC	LC	LC	LC	C	C	LC	LC	C	LC	LC	LC	C	LC	LC		
Austria	MER	Sep/16	FATF	ME	SE	ME	ME	ME	LE	LE	ME	SE	ME	SE	PC	PC	LC	C	C	PC	PC	PC	LC	LC	C	PC	LC	C	PC	PC	LC	PC	C	C	C	PC	LC	PC	PC	C	C	LC	PC	C	LC	LC	LC	LC	C	LC				
Austria	FUR1	Dec/17	FATF	ME	SE	ME	ME	ME	LE	LE	ME	SE	ME	SE	*LC*	*LC*	LC	C	C	PC	PC	PC	*C*	*C*	C	*C*	LC	C	*C*	*C*	LC	*C*	C	C	C	*LC*	LC	PC	PC	C	C	LC	*LC*	C	LC	LC	LC	LC	C	LC	10	
Austria	FUR2	Nov/18	FATF	ME	SE	ME	ME	ME	LE	LE	ME	SE	ME	SE	LC	LC	LC		C	PC	PC	PC	C	C	C	C	LC	C	C	C	LC	C	C	C	C	LC	LC	*LC*	*LC*	C	C	LC	LC	LC	LC	C	LC	LC					2	
Bahamas	MER+FUR	Dec/18	CFATF	LE	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE	LC	C	*C*	C	LC	PC	PC	PC	C	C	LC	C	C	C	LC	LC	C	LC	PC	C	C	PC	LC	PC	LC	PC	PC	PC	C	C	LC	LC	PC	LC	LC	LC	LC	LC		
Bahamas	MER	Aug/17	CFATF	LE	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE	PC	PC	C	C	LC	NC	PC	PC	C	PC	LC	PC	C	C	PC	LC	PC	PC	PC	C	C	PC	PC	PC	PC	PC	PC	C	PC	LC	PC	PC	LC	PC	LC	LC	LC	LC	LC		
Bahamas	FUR1	Dec/18	CFATF	LE	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE	*LC*	C	C	C	LC	*PC*	PC	PC	C	*C*	LC	*C*	C	C	*LC*	LC	*C*	*LC*	PC	C	C	PC	*LC*	PC	PC	PC	C	*C*	LC	*LC*	PC	LC	*LC*	LC	LC	LC	LC	13	
Bahrain	MER	Sep/18	FATF/MENAFATF	ME	SE	SE	ME	ME	SE	ME	ME	ME	ME	ME	PC	LC	LC	C	PC	PC	PC	LC	C	LC	C	LC	LC	LC	C	LC	C	LC	LC	LC	LC	C	C	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC		
Bangladesh	MER+FUR	Aug/19	APG	ME	SE	ME	LE	LE	ME	LE	LE	SE	ME	SE	PC	LC	LC	LC	LC	C	LC	LC	LC	LC	C	LC	LC	LC	C	LC	C	LC	C	C	LC	LC	PC	PC	LC	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC		
Bangladesh	MER	Nov/16	APG	ME	SE	ME	LE	LE	ME	LE	LE	SE	ME	SE	PC	LC	LC	LC	LC	C	LC	LC	PC	LC	C	LC	LC	LC	C	PC	LC	PC	PC	C	C	LC	LC	PC	PC	LC	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC		
Bangladesh	FUR1	Sep/18	APG	ME	SE	ME	LE	LE	ME	LE	LE	SE	ME	SE	PC	LC	LC	LC	LC	C	LC	LC	PC	LC	C	LC	LC	LC	C	PC	LC	PC	PC	C	C	LC	LC	PC	PC	PC	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	1	
Bangladesh	FUR2	Aug/19	APG	ME	SE	ME	LE	LE	ME	LE	LE	SE	ME	SE	PC	LC	LC	LC	LC	C	LC	LC	*LC*	LC	C	LC	LC	LC	C	*C*	LC	*C*	LC	C	C	LC	LC	PC	PC	*LC*	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	5	
Barbados	MER	Feb/18	CFATF	LE	ME	ME	ME	ME	LE	LE	LE	LE	LE	LE	PC	LC	LC	PC	LC	LC	NC	NC	C	LC	C	LC	LC	LC	C	PC	PC	LC	LC	PC	PC	LC	C	C	LC	PC	PC	LC	PC	PC	PC	LC	LC	PC	LC	LC	LC	LC		
Belarus	MER	Dec/19	EAG	SE	SE	ME	ME	LE	SE	ME	ME	SE	ME	SE	LC	LC	C	C	C	LC	LC	PC	C	LC	LC	LC	LC	C	PC	LC	LC	LC	LC	LC	C	C	LC	LC	LC	LC	PC	C	C	C	LC	LC	LC	C	LC	C	LC	LC	LC		
Belgium	MER+FUR	Sep/18	FATF	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME	C	C	C	C	C	PC	PC	LC	C	C	C	C	PC	LC	LC	C	LC	LC	C	C	C	LC	LC	LC	C	C	C	C	C	LC	C	C	LC	LC	LC	LC	LC	LC	LC		
Belgium	MER	Apr/15	FATF	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME	LC	LC	C	C	LC	PC	PC	PC	C	LC	C	PC	PC	LC	LC	PC	PC	PC	LC	C	C	C	C	C	PC	LC	LC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC		
Belgium	FUR1	Sep/18	FATF	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME	*C*	C	C	C	C	PC	PC	*LC*	C	C	C	C	PC	LC	LC	C	*LC*	*LC*	C	C	C	C	C	LC	LC	LC	C	C	C	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	15	
Bermuda	MER	Jan/20	CFATF	HE	SE	SE	ME	SE	SE	ME	LE	SE	SE	ME	C	C	C	LC	C	LC	LC	C	C	C	C	LC	C	C	C	C	C	C	C	C	C	C	C	LC	LC	C	LC	LC	C	LC	LC	C	C	LC	LC	C	LC	LC	C	C		
Bhutan	MER+FUR	Sep/18	APG	LE	ME	LE	LE	LE	LE	LE	LE	ME	LE	LE	LC	LC	PC	PC	LC	PC	PC	PC	C	C	C	C	C	LC	C	LC	LC	LC	LC	PC	LC	C	LC	PC	LC	PC	PC	LC	PC	PC	LC	PC	PC	LC	PC	NC	LC	LC	PC		
Bhutan	MER	Oct/16	APG	LE	ME	LE	LE	LE	LE	LE	LE	ME	LE	LE	NC	PC	PC	PC	NC	NC	NC	PC	LC	C	C	C	C	PC	C	LC	LC	LC	LC	PC	NC	C	PC	PC	LC	PC	C	NC	NC	PC	PC	PC	PC	PC	NC	NC	LC	PC		
Bhutan	FUR1	Sep/18	APG	LE	ME	LE	LE	LE	LE	LE	LE	ME	LE	LE	*LC*	LC	PC	PC	*LC*	PC	PC	NC	C	C	C	C	C	PC	C	LC	LC	LC	LC	PC	*LC*	C	LC	PC	PC	LC	PC	C	PC	LC	PC	PC	LC	PC	NC	LC	LC	PC	14	
Botswana	MER+FUR	Aug/19	ESAAMLG	LE	ME	LE	LE	LE	ME	LE	LE	LE	LE	LE	LC	PC	C	LC	C	PC	PC	NC	PC	PC	LC	LC	PC	NC	PC	PC	N/A	PC	NC	C	LC	NC	LC	PC	PC	PC	C	PC	LC	LC	LC	LC	PC	PC	PC	C	LC	C	LC	LC		
Botswana	MER	May/17	ESAAMLG	LE	ME	LE	LE	LE	ME	LE	LE	LE	LE	LE	NC	NC	PC	PC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	N/A	PC	NC	PC	NC	NC	PC	NC	NC	NC	LC	NC	NC	PC	PC	PC	NC	PC	NC	PC	LC	PC	PC		
Botswana	FUR1	Aug/19	ESAAMLG	LE	ME	LE	LE	LE	ME	LE	LE	LE	LE	LE	*LC*	PC	*C*	*LC*	*C*	*PC*	*PC*	NC	*PC*	*PC*	*LC*	*LC*	*PC*	NC	*PC*	*PC*	N/A	PC	NC	*C*	*LC*	NC	*LC*	*PC*	*PC*	*PC*	*C*	*PC*	*LC*	*LC*	*LC*	*LC*	*PC*	PC	*PC*	*C*	LC	*C*	*LC*	*LC*	31	
Burkina Faso	MER	May/19	GIABA	LE	ME	LE	LE	LE	ME	LE	LE	LE	LE	LE	LC	PC	C	LC	PC	PC	PC	PC	C	LC	LC	LC	LC	PC	C	LC	LC	PC	PC	C	NC	C	C	C	PC	LC	PC	LC	C	LC	LC	LC	C	LC	LC	LC	LC	LC		
Cabo Verde	MER	May/19	GIABA	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	PC	PC	C	C	LC	PC	LC	PC	C	PC	LC	LC	LC	LC	PC	PC	PC	PC	PC	PC	C	PC	LC	C	C	C	PC	C	LC	LC	LC	C	LC	LC	C	LC	LC	LC		
Cambodia	MER+FUR	Aug/19	APG	ME	ME	LE	LE	LE	LE	LE	LE	SE	ME	LE	PC	LC	LC	LC	LC	LC	NC	PC	C	LC	LC	PC	PC	LC	C	PC	LC	PC	LC	PC	LC	PC	LC	LC	LC	LC	PC	LC	PC	LC	PC	PC	LC	PC	LC	PC	PC	LC		
Cambodia	MER	Sep/17	APG	ME	ME	LE	LE	LE	LE	LE	LE	SE	ME	LE	PC	PC	LC	LC	LC	LC	NC	PC	C	LC	LC	PC	PC	LC	C	PC	LC	PC	PC	PC	LC	PC	LC	LC	LC	LC	PC	LC	PC	LC	LC	LC	LC	PC	LC	PC	LC	LC		
Cambodia	FUR1	Sep/18	APG	ME	ME	LE	LE	LE	LE	LE	LE	SE	ME	LE	PC	PC	LC	LC	LC	LC	NC	PC	C	LC	LC	PC	PC	LC	C	PC	LC	PC	*LC*	LC	LC	PC	LC	LC	LC	LC	PC	*LC*	PC	LC	PC	PC	LC	PC	*LC*	PC	LC	LC	2	
Cambodia	FUR2	Aug/19	APG	ME	ME	LE	LE	LE	LE	LE	LE	SE	ME	LE	PC	*LC*	LC	LC	LC	LC	NC	PC	C	LC	LC	PC	PC	LC	C	PC	LC	PC	*LC*	LC	LC	PC	LC	LC	LC	LC	PC	*LC*	PC	LC	PC	PC	LC	PC	LC	PC	LC	LC	1	
Canada	MER	Sep/16	IMF/FATF/APG	SE	SE	SE	ME	LE	ME	ME	ME	SE	SE	ME	LC	C	C	LC	LC	LC	LC	C	C	LC	LC	NC	LC	C	NC	PC	PC	LC	C	PC	LC	NC	NC	PC	NC	LC	C	PC	PC	C	LC	LC	C	LC	LC	C	LC	LC		
Cayman Islands	MER	Mar/19	CFATF	ME	ME	LE	LE	ME	LE	LE	ME	LE	ME	ME	PC	PC	C	LC	C	LC	LC	LC	C	LC	C	C	C	LC	LC	LC	C	PC	C	PC	PC	PC	PC	C	PC	PC	LC	C	LC	C	LC	LC								
China	MER	Apr/19	FATF/IMF/APG/EAG	SE	ME	ME	LE	LE	ME	ME	SE	SE	LE	LE	LC	C	PC	C	LC	PC	NC	PC	C	LC	C	PC	LC	LC	PC	PC	LC	PC	C	LC	LC	NC	NC	NC	NC	PC	LC	NC	PC	C	C	LC	LC	PC	PC	LC	LC			
Colombia	MER	Nov/18	GAFILAT	SE	SE	SE	ME	ME	SE	LE	SE	LE	ME	LE	LC	LC	LC	C	LC	PC	NC	PC	C	PC	C	PC	PC	C	PC	PC	N/A	C	PC	LC	C	PC	PC	PC	LC	LC	LC	PC	LC	C	LC	C	LC	LC						
Cook Islands	MER	Sep/18	APG	SE	SE	SE	ME	SE	ME	LE	LE	ME	SE	ME	LC	C	LC	LC	LC	LC	PC	LC	C	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC							
Costa Rica	MER+FUR	Oct/18	GAFILAT	ME	SE	ME	ME	LE	ME	ME	ME	ME	LE	LE	LC	C	C	LC	C	LC	C	PC	C	LC	C	LC	LC	C	C	LC	PC	LC	C	C	C	PC	LC	LC	LC	LC	LC	NC	C	LC	LC	LC	LC	C	C	LC	C	C		
Costa Rica	MER	Dec/15	GAFILAT	ME	SE	ME	ME	LE	ME	ME	ME	ME	LE	LE	PC	PC	LC	LC	PC	PC	NC	NC	C	LC	C	LC	LC	C	NC	PC	NC	LC	PC	PC	LC	LC	NC	PC	LC	LC	C	LC	LC	PC	C	C	LC	C	C					
Costa Rica	FUR1	Oct/16	GAFILAT	ME	SE	ME	ME	LE	ME	ME	ME	ME	LE	LE	*LC*	*C*	*C*	LC	*C*	*PC*	*PC*	NC	C	LC	C	LC	LC	C	*C*	*LC*	*PC*	LC	*C*	*C*	*C*	PC	PC	PC	LC	C	LC	NC	PC	LC	LC	C	C	LC	C	C	11		
Costa Rica	FUR2	Oct/17	GAFILAT	ME	SE	ME	ME	LE	ME	ME	ME	ME	LE	LE	LC	C	C	LC	C	*LC*	*C*	*PC*	C	LC	C	LC	LC	C	C	LC	PC	LC	C	C	C	PC	PC	*LC*	*LC*	LC	LC	NC	PC	LC	LC	C	C	LC	C	C	5		
Costa Rica	FUR3	Oct/18	GAFILAT	ME	SE	ME	ME	LE	ME	ME	ME	ME	LE	LE	LC	C	LC	LC	C	LC	C	PC	C	LC	C	LC	LC	C	C	LC	PC	LC	C	C	C	PC	*LC*	LC	LC	LC	LC	NC	*C*	LC	LC	C	C	LC	C	C	2		
Cuba	MER+FUR	Oct/17	GAFILAT	ME	ME	SE	ME	SE	ME	ME	SE	SE	SE	ME	LC	C	LC	LC	C	C	LC	PC	C	LC	C	C	C	C	C	C	C	C	C	C	C	LC	LC	LC	C	LC	LC	PC	C	LC	LC	PC	LC	LC	LC	LC	LC		
Cuba	MER	Dec/15	GAFILAT	ME	ME	SE	ME	SE	ME	ME	SE	SE	SE	ME	LC	C	LC	LC	C	C	LC	PC	C	LC	C	C	C	LC	C	C	C	C	C	C	C	LC	LC	LC	C	LC	LC	PC	C	LC	LC	PC	LC	LC	LC	LC	LC		
Cuba	FUR1	Oct/17	GAFILAT	ME	ME	SE	ME	SE	ME	ME	SE	SE	SE	ME	LC	C	LC	LC	C	C	LC	PC	C	LC	C	C	C	*C*	C	C	C	C	C	C	C	LC	LC	LC	C	LC	LC	PC	C	LC	LC	PC	LC	LC	LC	LC	LC	1	
Cyprus	MER	Dec/19	MONEYVAL	SE	SE	ME	ME	ME	ME	ME	ME	SE	ME	ME	LC	LC	C	C	LC	LC	LC	PC	C	LC	C	LC	PC	C	LC	LC	C	LC	LC	LC	LC	C	LC	C	LC	PC	LC	C	C	LC	C	C	C						
Czech Republic	MER	Feb/19	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	SE	SE	ME	LC	LC	LC	LC	LC	PC	PC	PC	C	LC	C	LC	LC	PC	PC	PC	PC	PC	LC	LC	LC	LC	LC	C	PC	PC	LC	PC	LC	LC	LC	LC	LC	LC					
Denmark	MER+FUR	Nov/19	FATF	ME	SE	LE	LE	ME	ME	ME	ME	SE	ME	SE	LC	LC	LC	LC	C	PC	PC	PC	LC	LC	LC	C	PC	LC	LC	LC	LC	LC	LC	C	C	LC	LC	LC	LC	C	PC	LC	LC	LC	LC	LC	LC					
Denmark	MER	Aug/17	FATF	ME	SE	LE	LE	ME	ME	ME	ME	SE	ME	SE	PC	PC	LC	LC	C	PC	PC	PC	LC	PC	LC	C	PC	LC	LC	LC	LC	LC	LC	C	C	PC	LC	PC	PC	PC	LC	LC	LC	C	LC	LC	LC	LC	LC				
Denmark	FUR1	Nov/18	FATF	ME	SE	LE	LE	ME	ME	ME	ME	SE	ME	SE	PC	*LC*	LC	LC	C	PC	PC	PC	LC	*LC*	LC	*C*	PC	LC	*LC*	*LC*	*LC*	*LC*	LC	C	C	*LC*	LC	*LC*	PC	PC	LC	LC	LC	LC	LC	LC	LC	LC	10				
Denmark	FUR2	Nov/19	FATF	ME	SE	LE	LE	ME	ME	ME	ME	SE	ME	SE	*LC*	LC	LC	LC	C	PC	PC	PC	LC	LC	LC	C	PC	LC	LC	LC	LC	LC	LC	C	C	LC	LC	LC	LC	*C*	*LC*	LC	LC	LC	LC	LC	LC	3				
Dominican Republic	MER+FUR	Sep/19	GAFILAT	ME	SE	LE	ME	ME	ME	ME	ME	SE	ME	ME	LC	C	C	C	C	LC	LC	PC	C	LC	LC	LC	LC	C	PC	C	LC	LC	LC	*LC*	PC	C	LC	C	LC	LC	PC	C	LC	C	C	LC	LC	LC	PC	LC				
Dominican Republic	MER	Sep/18	GAFILAT	ME	SE	LE	ME	ME	ME	ME	ME	SE	ME	ME	LC	C	C	C	C	LC	LC	PC	C	LC	LC	LC	C	PC	C	LC	LC	PC	PC	C	LC	C	LC	LC	LC	PC	C	LC	C	C	LC	LC	LC	PC	LC				
Dominican Republic	FUR1	Sep/19	GAFILAT	ME	SE	LE	ME	ME	ME	ME	ME	SE	ME	ME	LC	C	C	C	C	LC	LC	PC	C	LC	LC	LC	C	PC	C	LC	LC	*LC*	PC	C	LC	C	LC	LC	LC	PC	C	LC	C	C	LC	LC	LC	PC	LC	1				
Ethiopia	MER+FUR	Sep/19	ESAAMLG/WB	LE	ME	LE	LE	ME	LE	LE	LE	LE	LE	LE	C	LC	LC	LC	LC	PC	PC	C	LC	C	C	C	C	LC	C	C	LC	LC	LC	PC	N/A	LC	C	LC	LC	LC	PC	LC	PC	LC	C	LC	LC	LC	PC				
Ethiopia	MER	Jun/15	ESAAMLG/WB	LE	ME	LE	LE	ME	LE	LE	LE	LE	LE	LE	NC	PC	LC	LC	LC	NC	NC	PC	C	LC	C	C	C	PC	LC	C	C	LC	PC	C	LC	C	LC	LC	LC	PC	PC	PC	LC	PC	LC	LC	LC	LC	NC				
Ethiopia	FUR1	Nov/18	ESAAMLG	LE	ME	LE	LE	ME	LE	LE	LE	LE	LE	LE	*C*	PC	LC	LC	LC	*LC*	NC	PC	C	LC	C	C	C	*C*	LC	C	C	LC	*LC*	C	LC	LC	LC	PC	N/A	LC	C	*LC*	LC	LC	LC	PC	*LC*	PC	LC	PC	LC	LC	NC	6	
Ethiopia	FUR2	Sep/19	ESSAMLG	LE	ME	LE	LE	ME	LE	LE	LE	LE	LE	LE	C	*LC*	LC	LC	C	C	LC	*PC*	*LC*	C	LC	C	C	C	LC	LC	C	LC	LC	C	LC	LC	LC	PC	N/A	LC	C	LC	LC	LC	LC	PC	LC	PC	LC	LC	LC	LC	*PC*	5	
Fiji	MER+FUR	Aug-19	APG	ME	ME	ME	ME	LE	ME	ME	LE	LE	LE	LE	LC	LC	LC	C	C	PC	PC	PC	C	LC	C	C	C	C	C	LC	LC	LC	C	LC	LC	LC	LC	PC	PC	LC	LC	LC	C	C	LC	LC	*C*	LC	LC	LC	LC	C	PC	LC		
Fiji	MER	Nov/16	APG	ME	ME	ME	ME	LE	ME	ME	LE	LE	LE	LE	PC	PC	LC	C	PC	NC	NC	PC	C	PC	PC	PC	C	C	PC	PC	PC	PC	NC	LC	LC	NC	PC	PC	PC	PC	LC	LC	PC	C	C	LC	LC	PC	LC	LC	PC	LC		
Fiji	FUR1	Oct/17	APG	ME	ME	ME	ME	LE	ME	ME	LE	LE	LE	LE	*LC*	PC	LC	C	*C*	*PC*	*PC*	PC	C	*LC*	*C*	PC	C	C	PC	*LC*	*LC*	*LC*	NC	LC	LC	*PC*	PC	PC	PC	LC	LC	PC	C	C	LC	LC	PC	*LC*	PC	LC	C	PC	LC	11	
Fiji	FUR2	Sep/18	APG	ME	ME	ME	ME	LE	ME	ME	LE	LE	LE	LE	*LC*	*LC*	LC	C	C	*PC*	PC	PC	C	LC	C	C	C	C	C	*LC*	LC	*LC*	LC	LC	LC	*LC*	*LC*	PC	PC	LC	LC	PC	LC	C	PC	LC	*LC*	LC	C	PC	LC	8	
Fiji	FUR3	Aug/19	APG	ME	ME	ME	ME	LE	ME	ME	LE	LE	LE	LE	LC	LC	LC	C	C	PC	PC	PC	C	LC	C	C	C	C	C	LC	LC	LC	C	LC	LC	LC	LC	PC	PC	LC	LC	LC	C	C	LC	LC	*C*	LC	LC	LC	LC	C	PC	LC	1	
Finland	MER	Apr/19	FATF	SE	HE	LE	ME	ME	SE	SE	ME	ME	ME	ME	LC	PC	LC	LC	LC	LC	LC	PC	C	LC	C	LC	PC	C	LC	C	LC	LC	PC	LC	C	C	LC	LC	PC	PC	LC	LC	LC	PC	LC	LC	LC	LC	LC	LC				
Ghana	MER+FUR	Jun/18	GIABA	ME	SE	ME	LE	LE	ME	ME	LE	LE	LE	LE	LC	LC	C	LC	LC	LC	LC	NC	C	LC	C	C	C	C	C	LC	LC	LC	C	C	C	LC	LC	PC	PC	C	C	C	LC	C	LC	LC	LC	PC	LC				
Ghana	MER	Apr/18	GIABA	ME	SE	ME	LE	LE	ME	ME	LE	LE	LE	LE	LC	LC	C	LC	LC	LC	LC	NC	C	LC	C	C	C	C	C	PC	PC	LC	C	C	C	LC	LC	LC	PC	C	C	C	LC	PC	LC	LC	LC	PC	LC				
Ghana	FUR1	Jun/18	GIABA	ME	SE	ME	LE	LE	ME	ME	LE	LE	LE	LE	LC	LC	C	LC	LC	LC	LC	NC	C	LC	C	C	C	C	C	*LC*	*LC*	LC	C	C	C	LC	LC	LC	PC	C	C	C	LC	C	LC	LC	LC	PC	LC	2				
Gibraltar	MER	Dec/19	MONEYVAL	ME	SE	ME	ME	ME	LE	LE	LE	ME	ME	ME	PC	LC	C	LC	C	LC	LC	LC	C	C	PC	PC	PC	LC	C	C	C	C	C	C	C	C	LC	LC	C	C	C	LC	PC	C	C	C	LC	LC					
Greece	MER	Sep/19	FATF	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	SE	LC	LC	C	LC	LC	LC	LC	PC	C	C	C	C	PC	C	LC	LC	LC	C	LC	C	C	LC	LC	LC	C	C	PC	LC	LC	LC	LC	LC	C	C	LC					
Guatemala	MER+FUR	Oct/18	CFATF/ GAFILAT	ME	SE	ME	ME	ME	SE	SE	SE	ME	ME	ME	LC	C	LC	LC	PC	PC	PC	LC	C	LC	C	LC	C	PC	C	LC	PC	LC	C	C	LC	C	C	C	C	C	C	C	PC	C	LC	LC	LC	LC					
Guatemala	MER	Feb/17	CFATF/ GAFILAT	ME	SE	ME	ME	ME	SE	SE	SE	ME	ME	ME	LC	C	LC	LC	PC	PC	PC	LC	C	LC	C	LC	C	PC	PC	PC	PC	C	C	LC	C	PC	PC	LC	LC	C	LC	PC	C	C	C	C	C	C	PC	C	LC	LC	LC		
Guatemala	FUR1	Oct/18	GAFILAT	ME	SE	ME	ME	ME	SE	SE	SE	ME	ME	ME	LC	C	LC	LC	PC	PC	PC	LC	C	LC	C	LC	C	PC	*C*	*LC*	PC	C	C	LC	C	C	PC	LC	LC	C	LC	C	C	C	C	C	C	C	PC	C	LC	LC	LC	2	
Haiti	MER	Jul/19	CFATF	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	NC	PC	PC	PC	PC	NC	NC	NC	LC	PC	PC	PC	PC	PC	NC	NC	NC	NC	PC	PC	NC	NC	NC	NC	NC	PC	PC	NC	NC	PC	LC	PC	PC	PC	NC					
Honduras	MER	Jan/17	GAFILAT	ME	SE	ME	ME	LE	ME	ME	HE	SE	ME	LE	PC	LC	LC	C	LC	LC	PC	LC	C	LC	C	LC	C	C	C	PC	PC	LC	C	C	C	LC	PC	NC	LC	LC	C	PC	LC	LC	LC	LC	LC						
Hong Kong, China	MER	Sep/19	FATF	SE	SE	ME	ME	ME	SE	ME	SE	SE	SE	ME	LC	LC	LC	LC	LC	C	C	C	C	LC	LC	PC	C	LC	LC	LC	LC	LC	C	C	C	C	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC					
Hungary	MER+FUR	Dec/19	MONEYVAL	LE	SE	ME	ME	LE	SE	LE	LE	ME	ME	ME	LC	LC	LC	C	LC	LC	LC	PC	C	LC	LC	PC	PC	LC	C	LC	LC	PC	LC	C	LC	C	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC					
Hungary	MER	Sep/16	MONEYVAL	LE	SE	ME	ME	LE	SE	LE	LE	ME	ME	ME	PC	PC	LC	C	LC	PC	PC	PC	C	PC	LC	PC	PC	LC	PC	PC	LC	PC	PC	LC	LC	PC	PC	PC	PC	LC	LC	LC	LC	LC	LC	LC	LC						
Hungary	FUR1	Mar/18	MONEYVAL	LE	SE	ME	ME	LE	SE	LE	LE	ME	ME	ME	*LC*	*LC*	LC	C	PC	*LC*	*LC*	PC	C	*LC*	LC	PC	PC	LC	*C*	*LC*	LC	PC	*LC*	C	LC	C	LC	PC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	13	

Jurisdiction (click on the country name to go to the report on www.fatf-gafi.org)	Report Type	Report Date	Assessment body/bodies	IO1	IO2	IO3	IO4	IO5	IO6	IO7	IO8	IO9	IO10	IO11	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10	R.11	R.12	R.13	R.14	R.15	R.16	R.17	R.18	R.19	R.20	R.21	R.22	R.23	R.24	R.25	R.26	R.27	R.28	R.29	R.30	R.31	R.32	R.33	R.34	R.35	R.36	R.37	R.38	R.39	R.40	#upgrades	#downgrades
Hungary	FUR2	Dec/18	MONEYVAL	LE	SE	ME	ME	LE	SE	LE	LE	ME	ME	ME	LC	LC	LC	C	LC	LC	LC	PC	C	LC	LC	PC	PC	LC	C	LC	LC	PC	LC	C	LC	LC	LC	PC	LC	LC	LC	LC	C	C	LC	PC	PC	LC	LC	LC	LC	LC	LC	LC	2	
Hungary	FUR3	Dec/19	MONEYVAL	LE	SE	ME	ME	LE	SE	LE	LE	ME	ME	ME	LC	LC	LC	C	LC	LC	LC	PC	C	LC	LC	PC	PC	LC	C	LC	LC	PC	LC	C	LC	LC	LC	PC	LC	LC	LC	LC	C	C	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	1	
Iceland	MER+FUR	Sep/19	FATF	LE	SE	LE	LE	LE	ME	ME	ME	ME	LE	LE	PC	PC	C	LC	LC	PC	PC	NC	C	C	C	C	PC	LC	LC	C	C	LC	C	C	C	C	LC	PC	PC	PC	C	PC	LC	C	C	PC	LC	PC	LC	LC	LC	LC	LC	LC		
Iceland	MER	Apr/18	FATF	LE	SE	LE	LE	LE	ME	ME	ME	ME	LE	LE	PC	PC	C	LC	LC	PC	PC	NC	LC	PC	C	PC	PC	LC	PC	PC	PC	PC	PC	LC	C	PC	PC	PC	PC	PC	LC	NC	LC	C	C	PC	LC	PC	PC	LC	LC	LC	LC	LC		
Iceland	FUR1	Sep/19	FATF	LE	SE	LE	LE	LE	ME	ME	ME	ME	LE	LE	PC	PC	C	LC	LC	PC	PC	NC	C	C	C	C	PC	LC	PC	C	C	LC	PC	C	C	C	LC	PC	PC	PC	C	PC	LC	C	C	PC	LC	PC	LC	LC	LC	LC	LC	LC	14	
Indonesia	MER	Sep/18	APG	SE	SE	ME	ME	ME	SE	ME	SE	SE	ME	LE	LC	LC	LC	LC	LC	PC	NC	LC	C	LC	LC	LC	C	C	LC	LC	LC	C	LC	C	LC	LC	LC	PC	PC	LC	LC	PC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC		
Ireland	MER+FUR	Nov/19	FATF	SE	SE	SE	ME	ME	SE	ME	ME	ME	ME	SE	LC	C	C	C	LC	PC	PC	PC	C	LC	LC	C	PC	LC	LC	C	LC	LC	LC	C	C	PC	LC	LC	LC	C	C	LC	C	C	C	PC	PC	C	LC	C	C	LC	C	LC		
Ireland	FUR1	Nov/19	FATF	SE	SE	SE	ME	ME	SE	ME	ME	ME	ME	SE	LC	C	C	C	LC	PC	PC	PC	C	LC	LC	C	PC	LC	LC	C	LC	LC	LC	C	C	PC	LC	LC	LC	C	C	LC	C	C	C	PC	PC	C	LC	C	C	LC	C	LC	11	
Isle of Man	MER+FUR	Jul/18	MONEYVAL	SE	SE	ME	ME	ME	LE	LE	LE	ME	ME	ME	LC	C	C	LC	C	C	LC	LC	C	LC	C	C	C	LC	C	C	C	LC	C	C	LC	LC	PC	LC	C	LC	LC	LC	C	C	C	C	C	LC	LC	LC	LC	LC	C	LC		
Isle of Man	MER	Dec/16	MONEYVAL	SE	SE	ME	ME	ME	LE	LE	LE	ME	ME	ME	LC	C	C	LC	LC	LC	LC	LC	C	LC	LC	LC	C	LC	C	PC	LC	LC	C	C	LC	LC	PC	PC	PC	LC	LC	LC	LC	C	C	LC	LC	LC	PC	LC	LC	LC	C	LC		
Isle of Man	FUR1	Jul/18	MONEYVAL	SE	SE	ME	ME	ME	LE	LE	LE	ME	ME	ME	LC	C	C	LC	C	C	LC	LC	C	LC	LC	LC	C	LC	C	C	LC	LC	C	C	LC	LC	PC	LC	PC	LC	LC	LC	C	C	C	C	C	LC	LC	LC	LC	LC	C	LC	8	
Isle of Man	FUR2	Jul/19	MONEYVAL	SE	SE	ME	ME	ME	LE	LE	LE	ME	ME	ME	LC	C	C	LC	C	C	LC	LC	C	LC	C	C	C	LC	C	C	C	LC	C	C	LC	LC	PC	LC	C	LC	LC	LC	C	C	C	C	C	LC	LC	LC	LC	LC	C	LC	4	
Israel	MER	Dec/18	FATF/MONEYVAL	SE	SE	ME	ME	SE	HE	SE	HE	HE	SE	ME	LC	C	LC	LC	C	LC	LC	LC	C	LC	LC	LC	C	C	C	PC	N/A	PC	LC	C	C	PC	PC	LC	LC	LC	C	PC	C	C	C	C	C	C	LC	C	LC	LC	C	LC		
Italy	MER+FUR	Mar/19	IMF/FATF	SE	SE	ME	ME	SE	SE	SE	SE	SE	ME	SE	C	LC	LC	C	C	LC	PC	LC	C	LC	C	LC	PC	C	LC	C	LC	LC	C	C	LC	LC	LC	LC	LC	C	C	LC	C	C	C	LC	LC	LC	C	C	LC	LC	C	C		
Italy	MER	Feb/16	FATF	SE	SE	ME	ME	SE	SE	SE	SE	SE	ME	SE	LC	LC	LC	C	C	LC	PC	LC	C	LC	C	LC	PC	C	LC	PC	LC	LC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	C	LC	LC	LC	PC	C	LC	LC	C	LC		
Italy	FUR1	Mar/19	FATF	SE	SE	ME	ME	SE	SE	SE	SE	SE	ME	SE	C	LC	LC	C	C	LC	PC	LC	C	LC	C	LC	PC	C	LC	C	LC	LC	C	C	LC	LC	LC	LC	LC	C	C	LC	C	C	C	LC	LC	LC	C	C	LC	LC	C	C	8	
Jamaica	MER	Jan/17	CFATF	ME	ME	ME	LE	LE	ME	LE	SE	LE	LE	LE	PC	PC	LC	LC	LC	NC	PC	NC	C	PC	PC	PC	C	PC	C	LC	PC	PC	PC	C	PC	PC	PC	PC	PC	PC	PC	PC	LC	LC	LC	LC	PC	LC	PC	LC	C	LC	C	PC		
Jordan	MER	Jan/20	MENAFATF	ME	SE	ME	ME	LE	ME	LE	ME	SE	LE	LE	PC	LC	LC	PC	LC	PC	NC	NC	C	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	PC	PC	NC	NC	PC	NC	PC	LC	PC	LC	C	C	PC	PC	PC	PC	LC	PC	NC	PC	PC		
Korea	MER	Apr/20	FATF/EAG	SE	SE	ME	ME	ME	SE	ME	SE	SE	ME	ME	LC	LC	LC	C	LC	PC	PC	PC	LC	LC	C	PC	C	C	C	LC	C	LC	LC	C	C	PC	PC	PC	LC	LC	C	PC	C	C	LC	LC	C	LC	LC	LC	LC	C	LC	LC		
Kyrgyzstan	MER+FUR	Dec/19	EAG	LE	ME	ME	ME	ME	ME	ME	LE	ME	ME	ME	LC	LC	C	LC	LC	C	C	NC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC		
Kyrgyzstan	MER	Sep/18	EAG	LE	ME	ME	ME	ME	ME	ME	LE	ME	ME	ME	PC	PC	C	LC	LC	LC	PC	NC	LC	LC	LC	NC	LC	LC	LC	PC	NC	LC	LC	LC	LC	PC	PC	PC	LC	LC	LC	NC	LC	C	LC	LC	LC	PC	LC	LC	LC	PC	LC	LC		
Kyrgyzstan	FUR1	Dec/19	EAG	LE	ME	ME	ME	ME	ME	ME	LE	ME	ME	ME	LC	LC	C	LC	LC	C	C	NC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	14	
Latvia	MER+FUR	Dec/19	MONEYVAL	ME	SE	ME	ME	LE	ME	ME	ME	ME	ME	LE	C	C	LC	C	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC		
Latvia	MER	Jul/18	MONEYVAL	ME	SE	ME	ME	LE	ME	ME	ME	ME	ME	LE	C	LC	LC	C	LC	PC	PC	PC	C	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	PC	LC	LC	LC	PC	C	PC	LC	LC	LC	PC	LC	C	LC	LC	LC	LC	PC	PC		
Latvia	FUR1	Dec/19	MONEYVAL	ME	SE	ME	ME	LE	ME	ME	ME	ME	ME	LE	C	C	LC	C	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	11	
Lithuania	MER	Feb/19	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME	PC	PC	LC	LC	LC	PC	PC	LC	C	LC	C	C	LC	LC	C	LC	C	LC	LC	LC	C	LC	LC	PC	LC	PC	C	PC	LC	C	LC	PC	LC	LC	LC	C	LC	LC	LC	LC		
Macao, China	MER+FUR	Oct/19	APG	ME	SE	SE	ME	SE	SE	LE	LE	ME	SE	SE	LC	LC	LC	C	LC	C	C	LC	C	C	C	C	C	C	C	LC	C	C	C	C	C	LC	LC	LC	LC	C	C	LC	C	LC	C	LC	LC	C	C	LC	C	LC	LC	LC		
Macao, China	MER	Dec/17	APG	ME	SE	SE	ME	SE	SE	LE	LE	ME	SE	SE	LC	LC	LC	C	LC	C	C	LC	C	C	C	C	C	C	C	LC	C	C	C	C	C	PC	PC	LC	LC	C	C	LC	C	LC	C	NC	LC	C	C	LC	C	LC	LC	LC		
Macao, China	FUR1	Oct/19	APG	ME	SE	SE	ME	SE	SE	LE	LE	ME	SE	SE	LC	LC	LC	C	LC	C	C	LC	C	C	C	C	C	C	C	LC	C	C	C	C	C	LC	LC	LC	LC	C	C	LC	C	LC	C	LC	LC	C	C	LC	C	LC	LC	LC		
Madagascar	MER	Sep/18	ESAAMLG/WB	LE	LE	LE	LE	LE	ME	LE	LE	LE	LE	LE	NC	PC	LC	LC	PC	NC	NC	PC	C	NC	PC	PC	PC	PC	NC	NC	PC	LC	PC	LC	C	NC	NC	PC	NC	PC	LC	NC	LC	C	C	PC	PC	NC	NC	PC	LC	LC	LC	PC		
Malawi	MER	Sep/19	ESAAMLG	ME	ME	ME	ME	LE	ME	ME	ME	LE	LE	LE	LC	PC	PC	C	PC	LC	PC	NC	C	LC	C	C	C	C	PC	PC	C	C	C	LC	C	LC	LC	PC	PC	C	C	C	C	C	LC	LC	PC	PC	LC	C	LC	C	LC	LC		
Malaysia	MER+FUR	Oct/18	APG/FATF	SE	ME	SE	ME	ME	SE	ME	ME	ME	SE	ME	LC	C	LC	LC	C	C	C	LC	LC	C	LC	LC	LC	C	C	C	LC	C	C	C	C	LC	LC	PC	PC	C	C	LC	C	C	C	C	C	C	LC	LC	LC	LC	LC	LC		
Malaysia	MER	Sep/15	APG/FATF	SE	ME	SE	ME	ME	SE	ME	ME	ME	SE	ME	LC	C	LC	LC	LC	C	PC	LC	LC	C	LC	LC	LC	C	C	C	LC	C	C	C	C	LC	LC	PC	PC	C	C	LC	C	C	C	LC	C	LC	LC	LC	LC	LC	LC	LC		
Malaysia	FUR1	Oct/18	APG/FATF	SE	ME	SE	ME	ME	SE	ME	ME	ME	SE	ME	LC	C	LC	LC	C	C	C	LC	LC	C	LC	LC	LC	C	C	C	LC	C	C	C	C	LC	LC	PC	PC	C	C	LC	C	C	C	C	C	C	LC	LC	LC	LC	LC	LC	4	
Mali	MER	Mar/20	GIABA	LE	ME	LE	LE	LE	LE	LE	LE	LE	LE	LE	LC	PC	LC	LC	PC	PC	PC	NC	C	LC	LC	LC	LC	PC	C	PC	LC	LC	NC	PC	C	PC	PC	PC	PC	PC	C	NC	LC	C	C	PC	PC	PC	LC	LC	LC	PC	LC	LC		
Malta	MER	Jul/19	MONEYVAL	ME	SE	LE	ME	ME	ME	LE	LE	ME	ME	SE	LC	C	C	C	LC	LC	C	PC	C	LC	C	LC	PC	LC	PC	LC	LC	LC	C	PC	C	LC	LC	PC	LC	PC	LC	PC	LC	LC	LC	LC	C	LC	LC	PC	LC	PC	C	LC		
Mauritania	MER+FUR	Apr/19	MENAFATF	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	NC	NC	LC	PC	PC	PC	NC	NC	LC	NC	PC	PC	LC	PC	NC	PC	PC	PC	NC	PC	PC	PC	PC	NC	NC	PC	PC	NC	LC	PC	PC	PC	PC	PC	PC	LC	LC	NC	PC	PC		
Mauritania	MER	Nov/18	MENAFATF	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	NC	NC	LC	PC	PC	PC	NC	NC	LC	NC	PC	PC	PC	PC	NC	PC	NC	NC	NC	PC	PC	PC	PC	NC	NC	PC	PC	NC	LC	PC	PC	PC	PC	PC	PC	LC	LC	NC	PC	PC		
Mauritania	FUR1	Apr/19	MENAFATF	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	NC	NC	LC	PC	PC	PC	NC	NC	LC	NC	PC	PC	LC	PC	NC	PC	PC	PC	NC	PC	PC	PC	PC	NC	NC	PC	PC	NC	LC	PC	PC	PC	PC	PC	PC	LC	LC	NC	PC	PC	3	
Mauritius	MER+FUR	Sep/19	ESAAMLG	LE	ME	LE	ME	LE	ME	ME	LE	LE	LE	LE	C	C	C	C	C	C	C	NC	C	C	LC	C	C	C	C	C	C	C	C	C	C	C	C	PC	LC	PC	C	LC	C	C	C	PC	PC	LC	C	LC	LC	LC	LC	LC		
Mauritius	MER	Jul/18	ESAAMLG	LE	ME	LE	ME	LE	ME	ME	LE	LE	LE	LE	NC	PC	LC	LC	PC	NC	NC	NC	PC	NC	LC	PC	NC	PC	NC	NC	NC	PC	PC	C	PC	NC	NC	NC	PC	PC	LC	NC	LC	C	C	PC	PC	LC	PC	LC	LC	LC	LC	LC		
Mauritius	FUR1	Apr/19	ESAAMLG	LE	ME	LE	ME	LE	ME	ME	LE	LE	LE	LE	NC	PC	LC	LC	PC	NC	NC	NC	C	LC	LC	C	C	C	PC	LC	C	C	PC	C	PC	LC	NC	NC	PC	PC	C	NC	LC	C	C	PC	PC	LC	PC	LC	LC	LC	LC	LC	11	
Mauritius	FUR2	Sep/19	ESAAMLG	LE	ME	LE	ME	LE	ME	ME	LE	LE	LE	LE	C	C	C	C	C	C	C	NC	C	C	LC	C	C	C	C	C	C	C	C	C	C	C	C	PC	LC	PC	C	LC	C	C	C	PC	PC	LC	C	LC	LC	LC	LC	LC	19	
Mexico	MER	Jan/18	IMF/FATF/GAFILAT	SE	SE	ME	LE	ME	ME	LE	LE	ME	SE	SE	LC	LC	C	LC	LC	C	C	PC	C	PC	LC	PC	LC	LC	PC	PC	PC	PC	LC	PC	LC	PC	NC	PC	LC	LC	LC	PC	C	LC	LC	PC	PC	LC	LC	LC	PC	PC	LC	LC		
Moldova	MER	Jul/19	MONEYVAL	SE	SE	ME	ME	ME	ME	ME	ME	SE	ME	LE	LC	LC	LC	C	LC	PC	PC	PC	LC	PC	LC	PC	LC	C	LC	LC	LC	LC	PC	C	C	PC	PC	PC	PC	C	LC	LC	C	C	LC	LC	LC	C	C	LC	LC	PC	LC	LC		
Mongolia	MER+FUR	Oct/19	APG	LE	ME	LE	LE	LE	LE	LE	ME	LE	LE	LE	PC	LC	LC	LC	LC	LC	LC	PC	LC	LC	C	LC	LC	PC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	PC	C	C	C	LC	LC	LC	PC	C	C	LC	LC	LC		
Mongolia	MER	Sep/17	APG	LE	ME	LE	LE	LE	LE	LE	ME	LE	LE	LE	PC	PC	LC	LC	LC	PC	NC	PC	LC	LC	C	LC	LC	PC	LC	LC	NC	LC	PC	LC	PC	NC	NC	PC	PC	PC	LC	NC	PC	C	C	PC	PC	PC	PC	C	C	LC	LC	LC		
Mongolia	FUR1	Oct/19	APG	LE	ME	LE	LE	LE	LE	LE	ME	LE	LE	LE	PC	LC	LC	LC	LC	LC	LC	PC	LC	LC	C	LC	LC	PC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	LC	LC	PC	C	C	C	LC	LC	LC	PC	C	C	LC	LC	LC	16	
Morocco	MER	Jun/19	MENAFATF	ME	ME	ME	ME	LE	ME	LE	ME	SE	ME	LE	PC	PC	LC	PC	LC	PC	NC	NC	C	PC	LC	PC	PC	LC	PC	LC	PC	PC	PC	PC	C	PC	PC	PC	NC	PC	LC	PC	LC	PC	PC	NC	PC	PC	PC	LC	LC	PC	LC	PC		
Myanmar	MER+FUR	Aug/19	APG	LE	LE	LE	LE	LE	ME	LE	LE	LE	LE	LE	LC	LC	C	LC	LC	LC	NC	PC	C	PC	C	PC	PC	NC	LC	LC	C	LC	PC	C	LC	PC	PC	NC	NC	PC	C	NC	PC	LC	LC	PC	PC	PC	PC	PC	PC	PC	PC	LC		
Myanmar	MER	Sep/18	APG	LE	LE	LE	LE	LE	ME	LE	LE	LE	LE	LE	PC	LC	C	LC	LC	LC	NC	PC	C	PC	C	PC	PC	NC	LC	LC	C	C	NC	C	LC	PC	PC	NC	NC	PC	C	NC	PC	LC	LC	PC	PC	PC	PC	PC	PC	PC	PC	LC		
Myanmar	FUR1	Aug/19	APG	LE	LE	LE	LE	LE	ME	LE	LE	LE	LE	LE	LC	LC	C	LC	LC	LC	NC	PC	C	PC	C	PC	PC	NC	LC	LC	C	LC	PC	C	LC	PC	PC	NC	NC	PC	C	NC	PC	LC	LC	PC	PC	PC	PC	PC	PC	PC	PC	LC	2	1
Nicaragua	MER+FUR	Jan/19	GAFILAT	ME	ME	LE	ME	LE	ME	ME	SE	ME	ME	LE	PC	LC	LC	LC	LC	LC	LC	PC	LC	C	C	C	C	PC	PC	LC	LC	LC	LC	LC	LC	PC	PC	PC	LC	LC	LC	PC	C	C	LC	LC	LC	LC	PC	LC	LC	LC	LC	LC		
Nicaragua	MER	Oct/17	GAFILAT	ME	ME	LE	ME	LE	ME	ME	SE	ME	ME	LE	PC	LC	LC	LC	PC	LC	NC	PC	LC	PC	PC	PC	C	PC	PC	LC	LC	LC	LC	PC	PC	NC	NC	NC	NC	PC	LC	NC	C	C	LC	LC	LC	LC	PC	LC	LC	LC	LC	LC		
Nicaragua	FUR1	Jan/19	GAFILAT	ME	ME	LE	ME	LE	ME	ME	SE	ME	ME	LE	PC	LC	LC	LC	LC	LC	NC	PC	LC	PC	C	PC	C	PC	PC	LC	LC	LC	LC	LC	LC	PC	PC	PC	NC	LC	LC	PC	C	C	LC	LC	LC	LC	PC	LC	LC	LC	LC	LC	9	
Nicaragua	FUR2	Aug/19	GAFILAT	ME	ME	LE	ME	LE	ME	ME	SE	ME	ME	LE	PC	LC	LC	LC	LC	LC	LC	PC	LC	C	C	C	C	PC	PC	LC	LC	LC	LC	LC	LC	PC	PC	PC	LC	LC	LC	PC	C	C	LC	LC	LC	LC	PC	LC	LC	LC	LC	LC	4	
Norway	MER+FUR+FU	Dec/19	FATF	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	SE	LC	LC	C	C	C	PC	C	LC	C	LC	C	C	PC	C	C	PC	LC	LC	LC	C	C	LC	LC	PC	C	C	C	C	LC	C	LC	C	PC	LC	C	C	LC	LC	LC	LC		
Norway	MER	Dec/14	FATF	ME	SE	ME	ME	ME	ME	ME	ME	SE	ME	ME	PC	PC	C	LC	LC	PC	PC	LC	LC	PC	LC	PC	PC	LC	PC	PC	PC	PC	LC	C	LC	PC	LC	PC	PC	PC	LC	PC	LC	C	LC	C	PC	LC	PC	C	LC	LC	LC	LC		
Norway	FUR1	Mar/18	FATF	ME	SE	ME	ME	ME	ME	ME	ME	SE	ME	ME	LC	LC	C	C	C	PC	C	LC	LC	PC	LC	PC	PC	LC	LC	PC	PC	PC	LC	C	LC	PC	LC	PC	PC	LC	LC	LC	LC	C	LC	C	PC	LC	PC	C	LC	LC	LC	LC	8	
Norway	FUR2	Mar/19	FATF	ME	SE	ME	ME	ME	ME	ME	ME	SE	ME	ME	LC	LC	C	C	C	PC	C	LC	C	LC	C	C	PC	C	C	PC	LC	LC	LC	C	C	LC	LC	PC	C	C	C	C	LC	C	LC	C	PC	LC	C	C	LC	LC	LC	LC	15	
Norway	FUAR	Dec/19	FATF	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	SE	LC	LC	C	C	C	PC	C	LC	C	LC	C	C	PC	C	C	PC	LC	LC	LC	C	C	LC	LC	PC	C	C	C	C	LC	C	LC	C	PC	LC	C	C	LC	LC	LC	LC	15	
Pakistan	MER	Oct/19	APG	LE	ME	LE	LE	LE	LE	LE	LE	LE	LE	LE	PC	LC	LC	LC	LC	PC	PC	PC	C	PC	LC	PC	LC	PC	PC	LC	PC	PC	PC	PC	PC	NC	PC	PC	NC	PC	PC	NC	PC	PC	PC	PC	PC	PC	PC	LC	PC	NC	LC	PC		
Palau	MER	Sep/18	APG	ME	SE	ME	ME	LE	ME	ME	ME	LE	ME	LE	PC	LC	LC	LC	LC	LC	NC	NC	C	PC	C	PC	PC	NC	PC	PC	PC	C	PC	LC	C	NC	PC	NC	PC	PC	C	NC	LC	LC	LC	LC	LC	PC	PC	NC	LC	LC	LC	LC		
Panama	MER+FUR	Aug/19	GAFILAT	LE	ME	ME	ME	LE	LE	ME	ME	ME	SE	SE	LC	LC	LC	C	LC	LC	LC	LC	C	LC	LC	C	C	C	C	LC	LC	C	LC	C	C	LC	LC	PC	PC	LC	LC	LC	C	C	LC	C	C	C	LC	C	LC	LC	LC	LC		
Panama	MER	Jan/18	GAFILAT	LE	ME	ME	ME	LE	LE	ME	ME	ME	SE	SE	LC	LC	PC	C	LC	LC	LC	LC	C	LC	LC	C	C	PC	C	LC	LC	C	PC	PC	C	LC	LC	NC	PC	LC	LC	LC	C	PC	LC	LC	PC	C	LC	C	LC	LC	LC	LC		
Panama	FUR1	Jan/19	GAFILAT	LE	ME	ME	ME	LE	LE	ME	ME	ME	SE	SE	LC	LC	PC	C	LC	LC	LC	LC	C	LC	LC	C	C	C	C	LC	LC	C	LC	PC	C	LC	LC	NC	PC	LC	LC	LC	C	PC	LC	C	C	C	LC	C	LC	LC	LC	LC	4	
Panama	FUR2	Aug/19	GAFILAT	LE	ME	ME	ME	LE	LE	ME	ME	ME	SE	SE	LC	LC	LC	C	LC	LC	LC	LC	C	LC	LC	C	C	C	C	LC	LC	C	LC	C	C	LC	LC	PC	PC	LC	LC	LC	C	C	LC	C	C	C	LC	C	LC	LC	LC	LC	4	
Peru	MER	Feb/19	GAFILAT	ME	SE	ME	ME	LE	SE	LE	ME	ME	SE	SE	LC	C	C	C	C	LC	LC	PC	LC	LC	LC	LC	C	C	C	LC	PC	C	PC	C	C	LC	LC	PC	PC	LC	C	LC	C	LC	LC	LC	C	LC	PC	C	LC	C	C	LC		
Philippines	MER	Oct/19	APG	SE	ME	ME	ME	LE	ME	LE	LE	LE	LE	LE	LC	C	LC	PC	LC	PC	NC	LC	LC	LC	C	LC	LC	LC	LC	LC	C	LC	PC	C	C	PC	PC	PC	PC	LC	LC	PC	PC	C	LC	PC	LC	LC	LC	LC	LC	C	PC	LC		
Portugal	MER	Dec/17	FATF	SE	SE	ME	ME	ME	ME	SE	ME	SE	SE	SE	LC	LC	LC	C	LC	C	C	PC	LC	LC	C	LC	PC	C	LC	PC	LC	LC	LC	LC	C	PC	LC	PC	PC	LC	C	LC	LC	C	C	LC	LC	LC	LC	C	LC	C	C	LC		
Russian Federation	MER	Dec/19	FATF/EAG/MONEYV	SE	SE	ME	ME	SE	HE	ME	SE	HE	ME	ME	LC	C	LC	LC	LC	PC	PC	LC	C	LC	LC	PC	LC	LC	C	PC	LC	LC	LC	C	LC	LC	LC	LC	PC	LC	LC	LC	C	LC	C	LC	C	LC	LC	LC	LC	LC	LC	LC		
Samoa	MER+FUR	Sep/18	APG	ME	SE	LE	ME	ME	LE	LE	ME	ME	ME	LE	PC	LC	LC	LC	LC	PC	NC	PC	C	LC	C	PC	PC	C	PC	PC	PC	LC	NC	LC	C	PC	PC	PC	PC	PC	PC	PC	LC	C	LC	LC	LC	PC	PC	PC	LC	LC	LC	LC		
Samoa	MER	Oct/15	APG	ME	SE	LE	ME	ME	LE	LE	ME	ME	ME	LE	PC	PC	PC	LC	PC	PC	NC	PC	C	PC	C	PC	PC	C	PC	PC	PC	LC	NC	LC	C	PC	PC	PC	PC	PC	PC	PC	LC	C	LC	LC	LC	PC	PC	PC	LC	LC	LC	LC		
Samoa	FUR1	Oct/17	APG	ME	SE	LE	ME	ME	LE	LE	ME	ME	ME	LE	PC	LC	PC	LC	PC	PC	NC	PC	C	PC	C	PC	PC	C	PC	PC	PC	LC	NC	LC	C	PC	PC	PC	PC	PC	PC	PC	LC	C	LC	LC	LC	PC	PC	PC	LC	LC	LC	LC	1	
Samoa	FUR2	Sep/18	APG	ME	SE	LE	ME	ME	LE	LE	ME	ME	ME	LE	PC	LC	LC	LC	LC	PC	NC	PC	C	LC	C	PC	PC	C	PC	PC	PC	LC	NC	LC	C	PC	PC	PC	PC	PC	PC	PC	LC	C	LC	LC	LC	PC	PC	PC	LC	LC	LC	LC	3	
Saudi Arabia	MER	Sep/18	FATF/MENAFATF	SE	ME	SE	ME	ME	ME	LE	LE	SE	SE	LE	LC	LC	C	LC	C	PC	PC	LC	C	C	C	C	C	C	LC	LC	C	C	C	C	C	LC	C	LC	LC	C	C	C	LC	LC	LC	LC	PC	C	C	PC	LC	LC	LC	LC		
Senegal	MER	May/18	GIABA	LE	LE	LE	LE	LE	ME	LE	LE	LE	LE	LE	PC	LC	LC	PC	PC	NC	NC	PC	C	PC	LC	NC	NC	LC	PC	PC	PC	PC	NC	C	C	PC	PC	PC	NC	PC	C	NC	LC	LC	PC	LC	PC	PC	PC	PC	C	PC	LC	LC		
Serbia	MER+FUR	Dec/19	MONEYVAL	ME	ME	ME	ME	ME	ME	LE	ME	ME	LE	LE	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	C	C	LC	C	C	PC	PC	LC	LC	LC	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	PC		
Serbia	MER	Jun/16	MONEYVAL	ME	ME	ME	ME	ME	ME	LE	ME	ME	LE	LE	PC	LC	LC	LC	LC	PC	NC	PC	LC	PC	LC	PC	PC	LC	LC	PC	C	PC	PC	C	C	PC	PC	LC	PC	PC	LC	PC	LC	LC	LC	LC	LC	LC	PC	LC	LC	LC	LC	PC		
Serbia	FUR2	Dec/18	MONEYVAL	ME	ME	ME	ME	ME	ME	LE	ME	ME	LE	LE	LC	LC	LC	LC	LC	PC	LC	PC	LC	LC	LC	C	LC	LC	LC	LC	C	PC	LC	C	C	PC	PC	LC	LC	LC	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	PC	10	
Serbia	FUR3	Dec/19	MONEYVAL	ME	ME	ME	ME	ME	ME	LE	ME	ME	LE	LE	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC	LC	LC	LC	C	C	LC	C	C	PC	PC	LC	LC	LC	LC	PC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	PC	3	
Seychelles	MER	Sep/18	ESAAMLG	LE	LE	LE	ME	LE	LE	LE	LE	LE	LE	LE	PC	PC	LC	PC	PC	PC	NC	NC	C	LC	C	LC	C	C	NC	PC	LC	C	PC	C	C	LC	LC	LC	PC	PC	LC	PC	PC	C	C	LC	PC	PC	PC	C	PC	NC	PC	LC		
Singapore	MER+FUR	Nov/19	FATF/APG	SE	SE	ME	ME	ME	SE	ME	ME	LE	ME	SE	LC	C	C	C	LC	LC	LC	LC	C	C	C	C	C	LC	C	C	C	C	LC	LC	C	PC	LC	LC	C	LC	C	PC	C	C	C	C	LC	LC	PC	C	LC	LC	LC	LC		
Singapore	MER	Sep/16	FATF/APG	SE	SE	ME	ME	ME	SE	ME	ME	LE	ME	SE	LC	C	LC	C	LC	LC	LC	LC	C	C	C	C	C	LC	C	C	C	C	LC	LC	C	PC	PC	PC	PC	LC	C	PC	C	C	C	C	LC	LC	PC	C	LC	LC	LC	LC		
Singapore	FUR1	Nov/19	FATF/APG	SE	SE	ME	ME	ME	SE	ME	ME	LE	ME	SE	LC	C	C	C	LC	LC	LC	LC	C	C	C	C	C	LC	C	C	C	C	LC	LC	C	PC	LC	LC	C	LC	C	PC	C	C	C	C	LC	LC	PC	C	LC	LC	LC	LC	4	
Slovenia	MER+FUR	Dec/18	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME	PC	LC	LC	LC	PC	PC	PC	PC	LC	LC	C	PC	PC	C	C	C	LC	LC	LC	C	C	LC	LC	LC	LC	PC	C	PC	C	C	LC	PC	LC	C	C	LC	LC	LC	LC	LC		
Slovenia	MER	Aug/17	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME	PC	LC	LC	LC	PC	PC	PC	PC	LC	LC	C	PC	PC	C	C	PC	LC	LC	LC	C	C	LC	LC	LC	LC	PC	C	PC	C	C	LC	PC	LC	C	C	LC	LC	LC	LC	LC		
Slovenia	FUR1	Dec/18	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME	PC	LC	LC	LC	PC	PC	PC	PC	LC	LC	C	PC	PC	C	C	C	LC	LC	LC	C	C	LC	LC	LC	LC	PC	C	PC	C	C	LC	PC	LC	C	C	LC	LC	LC	LC	LC	1	
Slovenia	FUR2	Dec/19	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME	PC	LC	LC	LC	PC	PC	PC	PC	LC	LC	C	PC	PC	C	C	C	LC	LC	LC	C	C	LC	LC	LC	LC	PC	C	PC	C	C	LC	PC	LC	C	C	LC	LC	LC	LC	LC		
Solomon Islands	MER	Oct/19	APG	ME	ME	LE	LE	LE	ME	LE	LE	LE	LE	LE	PC	PC	LC	LC	LC	NC	NC	NC	C	NC	PC	PC	NC	PC	NC	NC	PC	NC	NC	C	C	NC	PC	PC	NC	PC	LC	PC	LC	C	LC	LC	PC	PC	PC	PC	PC	PC	LC	PC		
Spain	MER+FUR+F	Dec/19	FATF	SE	SE	SE	SE	SE	HE	SE	SE	SE	ME	SE	C	LC	LC	C	C	PC	PC	LC	C	LC	C	C	C	C	C	C	LC	C	C	C	C	LC	C	LC	LC	LC	C	LC	C	C	C	C	C	C	C	C	C	C	C	C		
Spain	MER	Dec/14	FATF	SE	SE	SE	ME	SE	HE	SE	SE	SE	ME	ME	C	LC	LC	C	LC	PC	PC	LC	C	LC	C	C	C	C	C	PC	LC	C	C	C	C	LC	C	LC	LC	LC	C	LC	C	C	C	C	C	C	C	C	C	C	LC	C		
Spain	FUR1	Mar/18	FATF	SE	SE	SE	ME	SE	HE	SE	SE	SE	ME	ME	C	LC	LC	C	C	PC	PC	LC	C	LC	C	C	C	C	C	C	LC	C	C	C	C	LC	C	LC	LC	LC	C	LC	C	C	C	C	C	C	C	C	C	C	C	C	3	
Spain	FUAR	Dec/19	FATF	SE	SE	SE	SE	SE	HE	SE	SE	SE	ME	SE	C	LC	LC	C	C	PC	PC	LC	C	LC	C	C	C	C	C	C	LC	C	C	C	C	LC	C	LC	LC	LC	C	LC	C	C	C	C	C	C	C	C	C	C	C	C		
Sri Lanka	MER+FUR	Oct/19	APG	ME	LE	LE	LE	LE	LE	LE	LE	SE	LE	LE	LC	LC	LC	PC	C	LC	LC	PC	LC	LC	LC	LC	LC	NC	LC	LC	LC	LC	LC	C	C	LC	C	NC	LC	PC	C	PC	LC	C	LC	PC	LC	LC	PC	LC	C	LC	LC	PC		
Sri Lanka	MER	Oct/15	APG	ME	LE	LE	LE	LE	LE	LE	LE	SE	LE	LE	PC	PC	LC	PC	C	LC	NC	PC	LC	NC	LC	NC	NC	NC	PC	NC	NC	PC	NC	C	C	NC	PC	NC	NC	PC	C	NC	PC	C	LC	PC	PC	PC	PC	LC	PC	PC	LC	PC		
Sri Lanka	FUR1	Jul/16	APG	ME	LE	LE	LE	LE	LE	LE	LE	SE	LE	LE	PC	LC	LC	PC	C	LC	NC	PC	LC	LC	LC	LC	LC	NC	LC	LC	LC	LC	LC	C	C	NC	PC	NC	NC	PC	C	NC	PC	C	LC	PC	PC	PC	PC	LC	PC	PC	LC	PC	9	

Jurisdiction (click on the country name to go to the report on www.fatf-gafi.org)	Report Type	Report Date	Assessment body/bodies	IO1	IO2	IO3	IO4	IO5	IO6	IO7	IO8	IO9	IO10	IO11	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10	R.11	R.12	R.13	R.14	R.15	R.16	R.17	R.18	R.19	R.20	R.21	R.22	R.23	R.24	R.25	R.26	R.27	R.28	R.29	R.30	R.31	R.32	R.33	R.34	R.35	R.36	R.37	R.38	R.39	R.40	#upgrades	#downgrades
Sri Lanka	FUR2	Sep/18	APG	ME	LE	LE	LE	LE	LE	LE	LE	SE	LE	LE	*LC*	LC	LC	PC	C	LC	NC	PC	LC	LC	LC	LC	LC	NC	LC	LC	LC	LC	LC	C	C	*LC*	C	NC	NC	PC	C	NC	*LC*	C	LC	PC	*LC*	*LC*	PC	LC	PC	PC	LC	PC	6	
Sri Lanka	FUR3	Oct/19	APG	ME	LE	LE	LE	LE	LE	LE	LE	SE	LE	LE	LC	LC	LC	PC	C	LC	***LC***	PC	LC	LC	LC	LC	LC	NC	LC	LC	LC	LC	LC	C	C	LC	C	NC	***LC***	PC	C	***PC***	LC	C	LC	PC	LC	LC	PC	LC	***C***	***LC***	LC	PC	5	
Sweden	MER+FUR	Jul/18	FATF	ME	HE	ME	ME	ME	ME	SE	SE	SE	ME	SE	LC	C	LC	LC	LC	PC	PC	LC	C	LC	C	C	LC	C	C	C	LC	LC	LC	LC	C	C	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	LC	C	LC	C	C		
Sweden	MER	Apr/17	FATF	ME	HE	ME	ME	ME	ME	SE	SE	SE	ME	SE	LC	PC	LC	LC	LC	PC	PC	LC	LC	LC	C	LC	LC	C	C	PC	PC	PC	LC	LC	LC	C	C	LC	PC	LC	LC	LC	C	LC	LC	C	C							
Sweden	FUR1	Jul/18	FATF	ME	HE	ME	ME	ME	ME	SE	SE	SE	ME	SE	LC	C	LC	LC	LC	PC	PC	LC	C	LC	C	C	LC	C	C	C	*LC*	*LC*	C	C	C	LC	LC	*LC*	*LC*	PC	LC	LC	LC	C	LC	LC	C	LC	C	C		10	
Switzerland	MER+FUR	Jan/20	FATF	SE	ME	ME	ME	ME	SE	SE	SE	SE	SE	SE	LC	LC	LC	LC	LC	LC	C	PC	C	PC	C	LC	LC	C	LC	LC	LC	LC	C	LC	LC	PC	PC	LC	LC	LC	LC	C	C	LC	LC	C	LC	LC	LC	LC	LC	PC		
Switzerland	MER	Dec/16	FATF	SE	ME	ME	ME	ME	SE	SE	SE	SE	SE	SE	LC	LC	LC	LC	LC	LC	C	PC	C	PC	C	LC	LC	C	LC	PC	LC	LC	PC	LC	LC	PC	PC	LC	LC	LC	LC	C	C	LC	LC	PC	LC	LC	LC	LC	LC	PC		
Switzerland	FUR	Jan/20	FATF	SE	ME	ME	ME	ME	SE	SE	SE	SE	SE	SE	LC	LC	LC	LC	LC	LC	C	PC	C	PC	C	LC	LC	C	LC	***LC***	LC	LC	***C***	LC	LC	PC	PC	LC	LC	LC	LC	C	C	LC	LC	***C***	LC	PC	LC	LC	LC	LC	PC	3	
Chinese Taipei	MER	Oct/19	APG	SE	SE	ME	ME	ME	SE	ME	SE	SE	SE	SE	LC	LC	LC	LC	LC	LC	LC	C	LC	LC	C	C	C	C	C	C	LC	C	LC	LC	LC	PC	LC	C	LC	LC	LC	C	PC	LC	LC	LC	LC	LC	LC	LC	LC			
Tajikistan	MER	Dec/18	EAG	SE	SE	ME	ME	ME	ME	LE	ME	SE	ME	LE	LC	C	LC	LC	LC	PC	NC	PC	C	LC	LC	PC	LC	LC	PC	PC	NA	LC	LC	C	C	PC	LC	LC	PC	PC	LC	PC	C	LC	PC	LC	C	LC	LC	LC	LC	PC	C	LC	PC	LC	LC		
Thailand	MER+FUR	Sep/18	APG	SE	SE	ME	LE	LE	SE	ME	SE	ME	ME	LE	PC	LC	LC	LC	LC	LC	LC	PC	LC	LC	LC	LC	PC	LC	LC	PC	C	LC	PC	PC	LC	NC	PC	PC	PC	PC	LC	PC	LC	C	LC	LC	LC	LC	PC	LC	LC	C	LC	LC		
Thailand	MER	Dec/17	APG	SE	SE	ME	LE	LE	SE	ME	SE	ME	ME	LE	PC	LC	LC	LC	LC	LC	NC	PC	LC	LC	LC	LC	PC	LC	LC	PC	C	LC	PC	PC	LC	NC	PC	PC	PC	PC	LC	PC	LC	C	LC	PC	LC	LC	PC	LC	LC	C	LC	LC		
Thailand	FUR1	Sep/18	APG	SE	SE	ME	LE	LE	SE	ME	SE	ME	ME	LE	PC	LC	LC	LC	LC	LC	*LC*	PC	LC	LC	LC	LC	PC	LC	LC	PC	C	LC	PC	PC	LC	NC	PC	PC	PC	PC	LC	PC	LC	C	LC	*LC*	LC	LC	PC	LC	LC	C	LC	LC	2	
Trinidad and Tobago	MER+FUR	Jun/19	CFATF	ME	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE	LC	LC	LC	LC	C	C	LC	PC	C	C	C	C	C	C	C	C	C	C	C	C	C	C	PC	C	PC	C	LC	C	C	PC	C	LC							
Trinidad and Tobago	MER	Jun/16	CFATF	ME	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE	PC	LC	LC	LC	C	PC	NC	NC	C	LC	C	C	C	C	C	LC	C	C	PC	C	LC	C	LC	C	LC	PC	PC	C	PC	LC	PC	LC	PC						
Trinidad and Tobago	FUR1	Jun/19	CFATF	ME	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE	*LC*	LC	LC	LC	C	*C*	*LC*	PC	C	*C*	C	C	C	C	C	C	C	C	C	C	C	C	C	PC	C	LC	C	C	PC	C	*LC*	18	
Tunisia	MER+FUR	Dec/17	MENAFATF	ME	ME	LE	LE	LE	ME	ME	ME	LE	LE	LE	LC	PC	C	LC	LC	LC	NC	LC	C	LC	C	LC	LC	LC	LC	LC	C	C	C	PC	PC	PC	PC	LC	LC	PC	C	LC	PC	C	LC							
Tunisia	MER	Jun/16	MENAFATF/ WB	ME	ME	LE	LE	LE	ME	ME	ME	LE	LE	LE	PC	PC	C	LC	C	PC	NC	LC	C	PC	C	PC	LC	LC	PC	NC	PC	PC	PC	C	C	PC	PC	PC	NC	NC	LC	PC	C	PC	C	LC						
Tunisia	FUR1	Dec/17	MENAFATF	ME	ME	LE	LE	LE	ME	ME	ME	LE	LE	LE	***LC***	PC	C	LC	***LC***	PC	NC	***PC***	C	***LC***	C	***LC***	LC	LC	***LC***	***LC***	***LC***	***LC***	***LC***	C	C	PC	PC	PC	***PC***	***PC***	LC	PC	LC	C	PC	C	LC	12	2
Tunisia	FUR2	Jan/19	MENAFATF	ME	ME	LE	LE	LE	ME	ME	ME	LE	LE	LE	LC	PC	C	LC	LC	***LC***	NC	***LC***	C	LC	C	LC	LC	LC	LC	LC	C	***PC***	LC	C	C	PC	PC	PC	PC	LC	C	PC	LC	C	PC	LC	***LC***	LC	C	PC	C	LC	4	2
Turkey	MER	Dec/19	FATF	SE	SE	ME	ME	ME	ME	ME	ME	ME	LE	LE	LC	LC	LC	C	LC	PC	NC	PC	C	LC	C	NC	LC	LC	LC	LC	C	PC	LC	C	C	PC	PC	PC	PC	PC	LC	C	C	LC	C	C	C	LC						
Turks&Caicos	MER	Jan/20	CFATF	ME	ME	LE	LE	ME	ME	LE	LE	LE	ME	ME	PC	LC	C	C	C	LC	LC	PC	C	PC	C	PC	PC	PC	PC	PC	C	PC	C	C	PC	PC	LC	C	PC	C	PC	C	C	LC	C	LC	C	LC	PC	LC	LC	C	PC		
Uganda	MER+FUR	Nov/18	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	PC	PC	C	LC	C	C	NC	NC	C	PC	C	PC	C	LC	PC	C	C	C	PC	C	C	PC	PC	NC	NC	NC	PC	NC	PC	PC	PC	NC	NC	PC	PC	C	PC	PC	NC	PC		
Uganda	MER	Sep/16	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	NC	PC	PC	LC	NC	NC	NC	NC	C	PC	NC	NC	C	PC	NC	NC	C	NC	NC	NC	NC	NC	PC	PC	PC	NC	NC	PC	PC	C	PC	PC	NC	NC	PC	PC	C	PC	PC	NC	PC		
Uganda	FUR1	Nov/18	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	***PC***	PC	***C***	LC	***C***	***C***	NC	NC	C	PC	***C***	***PC***	C	PC	***PC***	***C***	***C***	***C***	***PC***	C	C	PC	PC	PC	NC	NC	***PC***	NC	PC	PC	PC	NC	NC	PC	PC	C	PC	PC	NC	PC	13	
Ukraine	MER+FUR	Jul/19	MONEYVAL	SE	ME	ME	ME	ME	SE	LE	ME	ME	ME	ME	LC	C	LC	LC	PC	PC	PC	LC	C	LC	C	LC	C	LC	LC	C	N/A	LC	C	C	***LC***	LC	LC	PC	C	C	C	LC	LC	LC	LC	LC	LC	LC	LC	LC			
Ukraine	MER	Jan/18	MONEYVAL	SE	ME	ME	ME	ME	SE	LE	ME	ME	ME	ME	LC	C	LC	LC	PC	PC	PC	LC	C	LC	C	LC	C	LC	LC	C	N/A	LC	C	C	C	LC	LC	PC	C	C	C	LC	PC	C	PC	LC	LC	LC	LC	LC			
Ukraine	FUR1	Jul/19	MONEYVAL	SE	ME	ME	ME	ME	SE	LE	ME	ME	ME	ME	LC	C	LC	LC	PC	PC	PC	LC	C	LC	C	LC	C	LC	LC	C	N/A	LC	C	C	***LC***	LC	LC	PC	C	C	C	LC	LC	LC	LC	LC	LC	LC	LC	LC			1
United Arab Emirates	MER	Apr/20	FATF/MENAFATF	ME	LE	ME	ME	LE	ME	LE	ME	SE	ME	LE	PC	LC	LC	LC	LC	PC	PC	LC	C	LC	LC	C	LC	LC	C	LC	LC	PC	C	C	LC	PC	C	C	C	LC	LC	LC	C	LC	LC	LC	C	LC				
United Kingdom	MER	Dec/18	FATF	HE	SE	ME	ME	SE	ME	SE	SE	HE	HE	HE	LC	C	C	C	C	LC	LC	C	C	LC	C	PC	C	LC	LC	C	C	LC	LC	C	C	LC	C	C	C	C	LC	C	C	C	LC	C	C	C	C	LC	C	C		
United States	MER+FUR	Mar/20	FATF	SE	SE	ME	ME	LE	SE	SE	HE	HE	HE	HE	PC	C	LC	LC	C	LC	LC	LC	C	LC	LC	PC	LC	LC	PC	LC	LC	LC	PC	C	NC	NC	NC	PC	LC	C	NC	C	C	LC	C	LC	LC	LC	LC	LC	LC	LC	C		
United States	MER	Dec/16	FATF/APG	SE	SE	ME	ME	LE	SE	SE	HE	HE	HE	HE	PC	C	LC	LC	C	LC	LC	LC	C	PC	LC	PC	LC	LC	LC	PC	LC	LC	LC	PC	C	NC	NC	NC	PC	LC	C	NC	C	C	LC	C	LC	LC	LC	LC	LC	LC	LC	C		
United States	FUR1	Mar/20	FATF	SE	SE	ME	ME	LE	SE	SE	HE	HE	HE	HE	PC	C	LC	LC	C	LC	LC	LC	C	***LC***	LC	PC	LC	LC	LC	PC	LC	LC	LC	PC	C	NC	NC	NC	PC	LC	C	NC	C	C	LC	C	LC	LC	LC	LC	LC	LC	LC	C	1	
Uruguay	MER	Jan/20	GAFILAT	ME	ME	ME	ME	ME	ME	ME	ME	ME	ME	ME	LC	C	LC	LC	LC	LC	LC	C	C	LC	C	C	LC	LC	LC	LC	NA	C	C	LC	C	C	LC	LC	C	C	C	C	C	LC	C	LC	LC	LC	LC	LC	LC			
Vanuatu	MER+FUR	Nov/17	APG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	C	C	C	C	C	C	C	LC	LC	LC	LC	LC	C	C	LC	PC	LC	LC	C	C	C	LC	C	C	C	LC	C	C	C	LC	C	C	LC	C	LC				
Vanuatu	MER	Oct/15	APG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	NC	NC	NC	PC	PC	PC	NC	NC	LC	PC	LC	LC	LC	PC	LC	NC	NC	NC	PC	LC	C	PC	LC	NC	PC	PC	PC	PC	NC	PC	NC							
Vanuatu	FUR1	Nov/17	APG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	NC	NC	NC	PC	PC	PC	NC	NC	LC	PC	LC	LC	LC	PC	LC	NC	NC	NC	PC	LC	C	PC	LC	NC	PC	PC	PC	PC	NC	PC	NC	2	
Vanuatu	FUR2	Sep/18	APG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	*C*	*C*	*C*	*C*	*C*	*C*	*C*	*LC*	LC	*LC*	LC	LC	*C*	LC	*C*	*C*	*LC*	PC	LC	LC	*LC*	*LC*	*LC*	*LC*	*LC*	C	C	C	*C*	*LC*	C	*LC*	27	
Zambia	MER	Jun/19	ESAAMLG	ME	ME	ME	ME	LE	ME	ME	ME	ME	ME	LE	LC	LC	C	C	LC	PC	NC	PC	C	PC	LC	LC	C	LC	PC	PC	LC	LC	LC	C	C	PC	LC	C	C	PC	C	LC	C	C	PC	LC	LC	LC	LC	LC			
Zimbabwe	MER+FUR	Sep/19	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	ME	ME	LE	PC	LC	C	C	C	C	PC	PC	C	C	C	C	LC	C	C	C	LC	C	C	C	C	C	C	NC	LC	PC	LC	C	PC	PC	C	LC	C	LC	C	LC	LC			
Zimbabwe	MER	Jan/17	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	ME	ME	LE	PC	LC	C	PC	C	C	NC	NC	C	PC	C	PC	LC	PC	NC	C	C	PC	C	C	PC	C	C	NC	NC	PC	LC	PC	PC	LC	C	C	LC	C	LC				
Zimbabwe	FUR1	Apr/19	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	ME	ME	LE	PC	LC	C	C	C	C	NC	NC	C	LC	C	C	LC	C	C	LC	C	C	C	C	C	LC	C	NC	NC	PC	LC	C	PC	PC	LC	C	C	LC	C	LC	10		
Zimbabwe	FUR2	Sep/19	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	ME	ME	LE	PC	LC	C	C	C	C	***PC***	***PC***	C	***C***	C	C	LC	C	C	***C***	LC	C	C	C	C	***C***	C	NC	***LC***	PC	LC	PC	PC	C	LC	LC	***C***	PC	LC	C	C	LC	C	LC	6	

	MER	Mutual Evaluation Report	
	FUR	Follow-Up Report	
HE	large extent. Minor improvements needed.	C	Compliant
SE	large extent. Moderate improvements needed.	LC	Largely compliant - There are only minor shortcomings
ME	some extent. Major improvements needed.	PC	Partially compliant - There are moderate shortcomings
LE	Low level of effectiveness - The Immediate Outcome is not achieved or	NC	Non-compliant - There are major shortcomings.
		NA	Not applicable - A requirement does not apply, due to

Assessment Bodies

The body or bodies who conducted the mutual evaluation. Click on the links for more information.

APG	Asia/Pacific Group on Money Laundering
CFATF	Caribbean Financial Action Task Force
EAG	Eurasian Group
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
GABAC	Task Force on Money Laundering in Central Africa
GAFILAT	Financial Action Task Force of Latin America
GIABA	Inter Governmental Action Group against Money Laundering in West Africa
MENAFATF	Middle East and North Africa Financial Action Task Force
MONEYVAL	Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
IMF	International Monetary Fund
WB	World Bank

Effectiveness

Ratings that reflect the extent to which a country's measures are effective. The assessment is conducted on the basis of 11 immediate outcomes, which represent key goals that an effective AML/CFT system should achieve. See the FATF Methodology for more information.

HE	High level of effectiveness - The Immediate Outcome is achieved to a very large extent. Minor improvements needed.
SE	Substantial level of effectiveness - The Immediate Outcome is achieved to a large extent. Moderate improvements needed.
ME	Moderate level of effectiveness - The Immediate Outcome is achieved to some extent. Major improvements needed.
LE	Low level of effectiveness - The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements needed.

Immediate Outcomes

IO1	Money laundering and terrorist financing risks are understood and, where appropriate, actions co-ordinated domestically to combat money laundering and the financing of terrorism and proliferation.
IO2	International co-operation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.
IO3	Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.
IO4	Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.
IO5	Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.
IO6	Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.
IO7	Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.
IO8	Proceeds and instrumentalities of crime are confiscated.
IO9	Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.
IO10	Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.
IO11	Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

Technical Compliance

Ratings which reflect the extent to which a country has implemented the technical requirements of the FATF Recommendations. See the FATF Recommendations and the FATF Methodology for more information.

C	Compliant
LC	Largely compliant - There are only minor shortcomings.
PC	Partially compliant - There are moderate shortcomings.
NC	Non-compliant - There are major shortcomings.
NA	Not applicable - A requirement does not apply, due to the structural, legal or institutional features of the country.

Recommendations	
	AML/CFT Policies and Coordination
R.1	Assessing Risks and Applying a Risk-Based Approach
R.2	National cooperation and coordination
	Money Laundering and Confiscation
R.3	Money laundering offence
R.4	Confiscation and provisional measures
	Terrorist Financing and Financing of Proliferation
R.5	Terrorist financing offence
R.6	Targeted financial sanctions related to terrorism & terrorist financing
R.7	Targeted financial sanctions related to proliferation
R.8	Non-profit organisations
	Preventive Measures
R.9	Financial institution secrecy laws
R.10	Customer due diligence
R.11	Record keeping
R.12	Politically exposed persons
R.13	Correspondent banking
R.14	Money or value transfer services
R.15	New technologies
R.16	Wire transfers
R.17	Reliance on third parties
R.18	Internal controls and foreign branches and subsidiaries
R.19	Higher-risk countries
R.20	Reporting of suspicious transactions
R.21	Tipping-off and confidentiality
R.22	DNFBPs: Customer due diligence
R.23	DNFBPs: Other measures
	Transparency and Beneficial Ownership of Legal Persons and Arrangements
R.24	Transparency and beneficial ownership of legal persons
R.25	Transparency and beneficial ownership of legal arrangements
	Powers and Responsibilities of Competent Authorities and Other Institutional Measures
R.26	Regulation and supervision of financial institutions
R.27	Powers of supervisors
R.28	Regulation and supervision of DNFBPs
R.29	Financial intelligence units
R.30	Responsibilities of law enforcement and investigative authorities
R.31	Powers of law enforcement and investigative authorities
R.32	Cash couriers
R.33	Statistics
R.34	Guidance and feedback
R.35	Sanctions
	International Cooperation
R.36	International instruments
R.37	Mutual legal assistance
R.38	Mutual legal assistance: freezing and confiscation
R.39	Extradition
R.40	Other forms of international cooperation

Appendix J:

FATF, *Financial Action Task Force on Money Laundering: Annual Report 1992-1993* (Paris: FATF, 1993)

FATF-IV

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

ANNUAL REPORT 1992-1993

June 29, 1993

TABLE OF CONTENTS

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

ANNUAL REPORT 1992-1993

SUMMARY

1. The fourth round of the Task Force, which was chaired by Australia, continued to focus on three priorities:

(i) monitoring the implementation by FATF members of the forty recommendations for combating money laundering set out in its first report;

(ii) keeping track of developments in money laundering methods and examining appropriate counter-measures;

(iii) carrying out its external relations programme to promote world-wide action against money laundering.

2. The monitoring of members' implementation of the Recommendations has been undertaken on the basis of the self-assessment and mutual evaluation procedures developed in the previous round. Further refinements were made to the annual self-assessment exercise and this now provides a comprehensive and objective analysis of the state of implementation of the Recommendations across the membership. The 1992-93 exercise showed that members were making significant progress in this area. In particular, nearly all members have now made drug money laundering a criminal offence or are in the process of doing so.

3. The mutual evaluations of FATF members, which provide a more detailed examination of the measures to combat money laundering, are well under way. The number of evaluations doubled in 1992-1993 and nearly half of the FATF member jurisdictions have now been evaluated. Summaries of the 8 evaluations carried out in FATF-IV (Denmark, the United States, Belgium, Canada, Italy, Austria, Luxembourg and Switzerland) are contained in the report. The evaluation process has proved to be a particularly effective monitoring mechanism which is of benefit not only to the country examined but to all members. The remaining evaluations are expected to be completed by the end of 1994.

4. The assessment carried out in 1992-1993 of developments in money laundering techniques confirmed the trend towards greater use of non-bank financial institutions for money laundering purposes. It also showed that businesses outside the financial sector were being used to an increasing extent.

5. As regards development of countermeasures, no new Recommendations were drawn up during FATF-IV. However, Interpretative Notes were agreed on the law enforcement technique known as "controlled delivery"; and on clarifying the application of certain existing Recommendations to insurance business. The FATF also continued its work on two initiatives begun in earlier rounds: preventive measures in the non-bank financial sector; and on the audit trail for fund transfers on electronic payment and message systems. On the latter issue, the FATF has established good

co-operation with SWIFT, the leading international funds transfer messages system, and substantial progress has been achieved in this field.

6. Two further policy initiatives were launched during the round. A major study was carried out on the use of shell corporations for money laundering. Active consideration is being given to ways of applying Recommendation 13 (which requires financial institutions to take reasonable measures to obtain information on beneficial customers) in this area. Work has also begun on measures to counteract money laundering through non-financial businesses. Both these initiatives will be pursued in FATF-V.

7. In the external relations field, the FATF has intensified its efforts to encourage non-member countries to take effective action against money laundering. The programmes undertaken in 1992-93 have involved contacts with countries from every continent, with a particular emphasis on the Caribbean, Central and Eastern Europe and Asia.

8. FATF members participated in the work of the Caribbean Financial Action Task Force which, in November 1992, endorsed the FATF Recommendations and agreed to establish its own process to monitor their implementation by its members. In Central and Eastern Europe, the FATF held seminars in Budapest (attended by officials from a number of states from the region) and Warsaw. A seminar for Asian and Pacific states was held during the FATF's September 1992 meeting in Sydney, Australia, and was followed by a major money laundering symposium for Asian countries in Singapore in April this year. Further initiatives are planned in various parts of the world in 1993-1994.

9. In carrying out its external relations mission the FATF has worked in close co-operation with other international bodies involved in the fight against money laundering, such as the Commonwealth Secretariat, the Council of Europe, the United Nations International Drug Control Programme, the Customs Co-operation Council and INTERPOL.

10. During its 1993-1994 round, which will be chaired by the United Kingdom, the FATF will carry out the review of its statute and future work which was agreed when its mandate was renewed by Ministers in June 1991. However, it has already been decided that the group will continue until at least the end of 1994 to complete the mutual evaluations of FATF members.

11. At its 2-3 June meeting, the Council of OECD Ministers reaffirmed "the importance of co-operative global action to combat money laundering". They also welcomed "the substantial progress made by members of the Financial Action Task Force in implementing effective counter-measures in their countries and look forward to the greater application of these measures in the non-bank financial sector".

INTRODUCTION

12. The Financial Action Task Force was established by the G7 Economic Summit in Paris in 1989 to examine measures to combat money laundering. In April 1990, it issued a report with a programme of forty Recommendations. Following a second round of the Task Force, Member governments decided in June 1991 that it should continue its work for a further period. The Task Force has twenty eight member jurisdictions and regional organisations, including all OECD countries and other major financial centres.

13. Australia succeeded Switzerland as the Presidency of the Task Force for the fourth round of its work. Six series of meetings were held in 1992-1993, the first in Sydney and the remainder at the OECD headquarters in Paris. As agreed in the previous round, membership of the FATF has not been expanded. The Task Force continued to draw together experts from a wide range of disciplines, including finance, justice and external affairs ministries, law enforcement authorities and financial supervisory and regulatory agencies. Meetings of the Task Force were also attended, on an ad hoc basis, by representatives from the Council of Europe, the Customs Co-operation Council, the International Monetary Fund, the International Organisation of Securities Commissions, Interpol, the United Nations International Drug Control Programme and the World Bank.

14. In addition to holding plenary meetings, the FATF has also continued to operate through three Working Groups, dealing respectively with legal issues (Working Group I, Chairman: Italy); financial matters (Working Group II, Chairman: the Netherlands and, for the last part of the round, France); and external relations (Working Group III, Chairman: the USA). Working Groups I and II met jointly on several occasions to discuss the draft mutual evaluation reports on FATF members and policy issues of mutual interest.

15. In line with the remit for the FATF agreed in June 1991, the Task Force has focused on three main areas of work:

(i) evaluating the progress made by FATF members in implementing the forty Recommendations for countering money laundering set out in the first FATF report;

(ii) monitoring developments in money laundering techniques and pursuing appropriate refinements to the counter measures; and

(iii) implementing an external relations programme to promote the widest possible international action against money laundering.

I. MONITORING THE PROGRESS OF FATF MEMBERS IN IMPLEMENTING THE FORTY RECOMMENDATIONS

16. The Task Force monitors the performance of its members using the two methods agreed in 1991: an annual self-assessment exercise; and the more detailed mutual evaluation process under which each member jurisdiction is examined once over the period 1991-1994.

(i) Self Assessment

17. The self-assessment process continued on the basis of separate questionnaires relating to the legal and financial Recommendations. Drawing on the experience of the 1991-1992 exercise, various improvements were made to the questionnaires to elicit more precise information from members and to ensure that all aspects of the Recommendations were covered. In particular, the questionnaire dealing with financial issues was substantially revised so that the state of the application of the relevant Recommendations in the various sectors of non-bank financial institutions (securities, insurance, etc.) could be more accurately assessed. As before, members were invited to supply any appropriate narrative information as well as answering the questions. Most took the opportunity to do so.

18. When all member jurisdictions had completed the questionnaires, the FATF Secretariat drew up two grids of the responses showing the state of implementation of the Recommendations across the membership. These were then discussed in the respective Working Groups. Although there inevitably remain some differences in interpretation of some of the questions, the exercise now provides a generally objective analysis of the performance of members.

(ii) State of Implementation

(a) Legal Matters

19. The responses to the questionnaire showed that members have made substantial progress in putting into place the necessary legal measures, although there is still some way to go before all members are in full compliance with the Recommendations.

20. Nearly all members have now made drug money laundering a criminal offence or are taking steps to enable them to do so within the next twelve months. In addition, whereas in the survey carried out in FATF-III, very few members had criminalised money laundering other than for drugs proceeds, ten members have now introduced measures making it an offence to launder the proceeds of any serious crime or any crime which generates significant proceeds and another eight are in the process of doing so. In addition to the ten members who have ratified the Vienna Convention, another eight expect to have done so within the next twelve months and another four have partially implemented its provisions.

21. Nearly all members have laws enabling the confiscation of the proceeds from, and instrumentalities of, criminal offences. Such laws almost uniformly provide for law enforcement authorities to freeze and seize assets subject to confiscation and most include measures for identification, tracing and evaluation of assets. In addition, three FATF members have now ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, which will come into force on 1 September 1993. The majority of the European members of the FATF expect to have ratified the Convention within the next twelve months.

22. There has also been encouraging progress in promoting mutual legal assistance between members on money laundering issues. The domestic law of most FATF members allows them to conduct

co-operative investigations with other jurisdictions regarding money laundering and asset seizure/confiscation. Nearly all these members have conducted such investigations, although statistics are not generally available. Similarly, the great majority of FATF members can provide legal assistance in relation to drug money laundering offences either under bilateral or multilateral legal assistance treaties or general provisions. However, so far only a minority of members have such arrangements for non-drug money laundering cases.

(b) Financial Issues

23. There was also continued progress in implementing the financial Recommendations, particularly in the case of several European Task Force Member governments who are required to comply with the provisions of the EC Money Laundering Directive. But, as with the legal Recommendations, full compliance has not yet been achieved. In particular, there is a considerable disparity in the state of implementation of the various recommendations between the banking sector and non-bank financial institutions.

24. The vast majority of members are in full or partial compliance with customer identification and record-keeping rules, although there are still important exceptions, in particular for fiduciary transactions and requirements for non-bank financial institutions to take reasonable measures to obtain information about the true identity of persons on whose behalf an account is opened or a transaction is conducted.

25. While a majority of FATF Member governments requires banks to pay special attention to complex, unusual, large transactions, only a quarter of them currently oblige non-bank financial institutions to do so. Most FATF members either permit or require financial institutions to report promptly their suspicions to the competent authorities, although many still allow these institutions to warn their customers that reports are being made. Some two thirds of FATF member governments require banks to pay special attention to business relations and transactions with persons from countries with insufficient anti-money laundering measures. In a large majority of members, banks fully or partially ensure that the FATF principles are also applied to their branches and majority-owned subsidiaries located abroad. Similar measures are applied by non-bank financial institutions only in a minority of FATF members.

26. Most members require banks to develop specific programmes against money laundering and, in the majority, the regulatory authorities ensure that the supervised institutions have adequate programmes in place. In nearly all members, the competent authorities supervising banks and other financial institutions co-operate with law enforcement authorities in money laundering investigations and prosecutions. Some member governments have designated competent authorities to deal with the implementation of the FATF Recommendations as far as other professions dealing with cash are concerned. Guidelines have already been established by half of the Member governments to assist banks in detecting suspicious patterns of behaviour. Some members have done so for non-bank financial institutions as well. A large majority of members have also taken measures to guard against the control or acquisition of financial institutions by criminals.

(iii) Mutual Evaluation

27. The mutual evaluation process is now well under way. The number of evaluations carried out doubled in the 1992-1993 round. Nearly half the FATF member jurisdictions have now been subject to this process. The procedures established in FATF-III, which involve on-site visits by a team of experts followed by the preparation of detailed reports for discussion and endorsement by the FATF, have proved to be a particularly effective monitoring mechanism.

28. The evaluations provide a very thorough scrutiny of the action taken against money laundering by the members concerned and identify possible improvements to their anti-money laundering systems. The process produces a consistent and analytical assessment across the FATF membership while taking into account the particular circumstances of each individual FATF member (such as the scale and nature of the money laundering problem; the degree of development of the financial system; and the state of advancement of the anti-money laundering framework). The evaluation reports and the discussions in FATF meetings have proved to be of benefit to the FATF membership as a whole as well as to the individual member examined.

29. Eight mutual evaluations were carried out in FATF-IV: Denmark, the USA, Belgium, Canada, Italy, Austria, Luxembourg and Switzerland. The summaries of the reports are as follows:

Denmark

30. Denmark does not have a major drug consumption problem, nor is it a major centre for money laundering activity. Nevertheless, the fact that Denmark is not free of criminal activity, including the sales of drugs, means that criminal proceeds are generated within the country. However, the requirement for Danish banks to report accounts to the taxation authorities and the high level of income and capital taxation in Denmark act as powerful deterrents to resident criminals using the financial system for money laundering.

31. Denmark has adopted a clear political attitude towards the philosophy of the FATF. However, Denmark has, until now, not separated money laundering as a problem which differs from other kinds of serious crime. In addition, there is no Danish law enforcement agency specialised in the fight against money laundering. Despite the lack of legislation specifically criminalising money laundering, the combination of existing laws with respect to a wide range of predicate offences together with the confiscation provisions provides a legal framework which the authorities have used on a number of occasions to punish the laundering of criminal proceeds.

32. The bulk of the anti-money laundering requirements for the financial sector is introduced in the Danish legislation by Act 348 of 9 June 1993 on measures to prevent money laundering. This Act implements the EC Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

33. With a view to preventing money laundering, the legislation requires the financial institutions to adopt internal rules of adequate control, communications procedures, training and institutions programmes for their employees. Financial institutions will ask their customers to provide proof of identity when establishing business relations with them. The requirement concerning proof of identity will also apply to occasional customers for every transaction above the equivalent value of ECU 15,000 and to transactions carried out on behalf of a third party. When there is a suspicion that a transaction is associated with money laundering, the financial institutions will have to investigate it closely, and at that same time, report it to the police only if the suspicion cannot be disproved. Information from the banks and the financial institutions passed on to the police in good faith will not be treated as a breach of confidentiality and will not involve these institutions in any liability.

34. An effective and complete implementation of the EC Directive is crucial to strengthen the Danish approach to money laundering. Concentrating on areas for enhancement, efforts should focus on the role of the Financial Supervisory Financial Authority which needs to be clearly defined in the anti-money laundering process. While the legislation to implement the EC Directive is comprehensive

with regard to banks and traditional financial institutions, the question remains as to how to address the use of non-traditional financial institutions for money laundering.

United States

35. The US has the most serious drug consumption problem and drug-related social problems of any industrialised country in the world. Money laundering takes place on a huge scale and the laundering of drug proceeds has increased enormously since the early 1980's. However, very large amounts of the proceeds of non-drug crimes are also laundered - in total almost as much (if not more) than drug funds. The US is also notable for the size and diversity of its financial system, which complicates the task of combating laundering. The scale of the informal financial sector, which is largely unregulated, is a particular problem since the launderers are increasingly using such institutions.

36. The US conducts a very vigorous programme against money laundering. Its strategy is based on aggressive prosecution of money laundering offences, a concentrated effort to prevent the use of financial institutions for laundering, with a particular emphasis on reporting of large currency transactions, and determined efforts to locate, seize and forfeit the proceeds of money laundering. The US is also very active in bilateral and multilateral initiatives in this field.

37. The US has had anti-money laundering legislation since 1970 and this is regularly revised and updated to respond to changes in the money laundering threat, most recently in an Act of October 1992. The key elements are the Bank Secrecy Act and the Money Laundering Control Act. The former, which applies to all deposit-taking institutions and other specified categories of activity, provides for the reporting of large cash transactions (which is mandatory for all businesses whether or not in the financial sector); identification of customers; and record-keeping requirements. Depository institutions are also required to report suspicious transactions and have anti-money laundering compliance programmes. These requirements are now in the process of being extended to other institutions. The money laundering offence itself is notable for the very wide range of predicate crimes which are specified in the legislation.

38. The US is very substantially in compliance with the forty FATF Recommendations, the main area of weakness being the non-bank financial sector where application of anti-money laundering measures is as yet far from comprehensive. There is a generally commendable legal framework for dealing with money laundering. Both the US authorities and the mainstream financial institutions are without question very strongly committed to the fight against money laundering. The dedication and professionalism of the agencies merits high respect, although the number of agencies involved in this field presents its own challenges.

39. Given the scale and nature of the money laundering problem faced by the US, there is clearly a need to ensure that the regulatory and law enforcement resources and systems available are organised and targeted to maximum effect. Reinforcement of the resources directed towards the informal financial sector would be consistent with the increased use of this sector by launderers. Concerns have also been expressed about the burdens imposed by the large currency reporting system in its present form and potential problems in running both this and suspicions reporting in tandem. The recently announced review by the US Treasury of the burdens and efficiency of the currency reporting system is therefore welcome.

Belgium

40. Belgium does not differ significantly from other European countries with regard to drug manufacturing, dealing and consumption. However, there is a risk that the Belgian financial system will, like others, find itself confronted with attempts at money laundering. This risk is accentuated by the fact that neighbouring countries have stiffened their legislation and that Brussels has consolidated its position as a financial centre. For this reason Belgium considered it necessary to adopt a certain number of measures aimed at combating money laundering in conformity with its international obligations.

41. Before the Act of 11 January 1993 on preventing the financial system being used for money laundering purposes, Belgium had already adopted anti-money laundering measures. First, the Act of 17 July 1990 made money laundering a criminal offence and provided for rules regarding confiscation. Second, on 17 July 1991, the Banking and Finance Commission issued a circular that requires credit institutions to observe certain requirements regarding the identification of customers, recordkeeping and internal procedures and increased diligence for unusual transactions. These measures were extended to stock brokerage companies as from September 1992.

42. The Act of 11 January 1993 on preventing the financial system from being used for money laundering went a long way towards completing Belgium's anti-money laundering machinery. The Act implements the provisions of EC Directive of 10 June 1991 in Belgium. It contains a set of preventive measures to be implemented by financial bodies. The Act also organises the collaboration of the financial bodies in the fight against money laundering by introducing a system for channeling information to an administrative unit called the "Financial Information Processing Unit". Financial bodies report suspicious operations to this Unit. The task assigned to the Unit is to collect reports from financial bodies and analyse them in the light of its own investigations. The Unit is empowered to ask the financial bodies to suspend an operation and, under certain circumstances, it can also inform the Crown Prosecutor.

43. The banking sector has made noteworthy efforts to combine its own action with those of the supervisory authorities. In particular, the Belgian Banking Federation and most credit institutions have set up remarkable training programmes. With regard to law enforcement matters, the Belgian anti-money laundering system will be reinforced by the creation of the Central Organised Economic and Financial Crime Enforcement Bureau.

44. The objectives defined in the FATF's Recommendations are being seriously and correctly pursued. While Belgium has recently acquired a coherent set of anti-money laundering measures, thanks to the Acts of 17 July 1990 and 11 January 1993, there is room for supplementary measures. Belgium should ensure that, in practice, rules against money laundering are implemented as fully as possible, especially in the case of individual currency agents and the non-financial professions.

Canada

45. Canada is primarily a drug consuming rather than producing country and the drugs situation is considered to be a serious social problem. It is estimated that drugs trafficking could generate several billion dollars a year. Like other financial centre countries, Canada's financial system has been used to launder foreign (particularly US), as well as domestically generated illicit funds. As legislation and programs were developed to combat money laundering within the sphere of traditional regulated financial institutions, the informal financial sector, particularly currency exchanges, has become a focus of concern.

46. Canada was quick to take action against money laundering. It was made a criminal offence in legislation enacted in 1988 and goes beyond drug trafficking to embrace a wide range of "enterprise crime" predicates. The legislation also enhanced the ability of the authorities to investigate, seize and obtain forfeiture of the proceeds of crime and provided for immunity from liability for reporting of suspicions. This was supplemented by new legislation and regulations brought into force earlier this year regarding record-keeping and customer identification by financial institutions and others. The federal Canadian financial services supervisor also took early action and issued money laundering guidelines which apply to all deposit-taking institutions it supervises. The Canadian banks have very active programmes of their own, although, as in other FATF members, the position in the non-bank sector is less well-developed. At the operational level, the Royal Canadian Mounted Police have had an anti-drug profiteering programme since 1981 and special integrated anti-drug profiteering units have recently been set up. Internationally, Canada has been very active in negotiating mutual legal assistance treaties.

47. Canada is substantially in compliance with the FATF Recommendations and is to be commended for the extensive list of money laundering predicates, although consideration might be given to extending this to cover all serious crimes or those generating substantial proceeds. Canadian law deals comprehensively at the domestic level with provisional measures against, and confiscation of proceeds of crime, although the requirement for the prosecution to give undertakings regarding payment of damages or costs in relation to restraint orders and freezing of assets does seem to be a constraint in practice. It would also be desirable if the authorities could act directly on requests from foreign countries to freeze and seize assets.

48. Full acknowledgement needs to be given to the Canadian authorities' willingness to keep their anti-money laundering measures under review and to make improvements to the system. For example, legislation providing for the sharing of confiscated assets domestically and internationally, was enacted in June 1993. Two additional changes - the introduction of mandatory suspicions reporting and the establishment of more effective powers to deal with suspicious currency at the border - are currently under consideration. The evaluation supported the introduction of such measures, which would further strengthen the Canadian system.

Italy

49. Located at the crossroads between the Middle East, the Mediterranean and northern Europe, Italy is the focus of a very large-scale narcotics traffic. However, the amount of laundered funds does not derive exclusively from the volume of narcotics trafficking in Italy, but also comes from the proceeds of the illicit activities of the organised crime in Italy - based on associations (clans, families) that control the traffic of drugs, arms, smuggling, etc. This means that a large part of the illicit money is channeled into and retained in financial and/or commercial activities. Therefore, the fight against money laundering is centered on this phenomenon.

50. The Penal Code provides for the repression of money laundering in its various forms, in conformity with the relevant international instruments. In order to refine and extend the scope of the repressive legislation, a Bill is under discussion in Parliament. With regard to confiscation, the provisions of the Penal Code and other criminal laws allow for the seizure of the proceeds of crime with respect to all types of crimes.

51. The key element of the Italian financial legislation to combat money laundering is Act 197 of 5 July 1991. The aim of this Act is to control cash transactions and flows, through the requirement that cash (or cash equivalent) transactions above 20 million lire (the equivalent of roughly US$ 13,000) must be carried out only through authorised financial intermediaries. Act 197 also extends the obligation of

identifying and recording the identity of the customers to all financial institutions, and broadens the requirement of recording to all means of payment. In addition, financial intermediaries are obliged to report suspicious transactions to the police. Finally, financial companies are required to be registered with the Italian Foreign Exchange Office. In parallel, the Act 227 of 1990 introduces the requirement that cross-border movements of cash or cash equivalents above 20 million lire must be channeled through authorised financial intermediaries.

52. The Italian system deserves to be characterised as a coherent and comprehensive money laundering control scheme. From a legal and administrative point of view, Italy has implemented the FATF Recommendations. However, it seems too early to offer any kind of substantive judgement as to how the legislation is working or will work in practice. Indeed, some aspects of the Italian system, i.e. the intelligence task dedicated to the UIC, will only produce results in the future.

53. As numerous authorities are involved in the anti-money laundering programme, the necessity for strong co-ordination seems to be of paramount importance. This is crucial to the achievement of the best results in money laundering investigations. The situation is different when an organised crime aspect is involved. Recent cases ("Green Ice", "Seaport") in this latter field have shown excellent efficiency both at the Italian level and at the international co-operation level between law enforcement agencies. For purely money laundering enquiries, the most important organisational problem is to determine the co-ordinating point. The latter is represented by the magistrate in charge of the investigation, who may co-ordinate his work with that of other magistrates involved in the same investigation. With regard to police investigations, the Central Investigation Office is responsible for the co-ordination of the work carried out by provincial officers.

Austria

54. Austria is not a major drug consuming country, although it does have a growing drug problem. It is one of the transit points for the supply of drugs to markets further west in Europe and to North America. Cocaine and heroin smuggling is increasing and there is growing activity by trafficking gangs from Central and Eastern European states. Although some domestic money laundering takes place, at present the problem is mainly seen in terms of the misuse of the Austrian financial system to launder the proceeds of foreign crimes, with indications that Austrian financial institutions have been used by Colombian cartels among others.

55. Measures to combat money laundering are currently limited to two main instruments: a decree of the Austrian National Bank, issued in 1991, establishing specific identification procedures for clients of banks who are not Austrian residents, although these do not fully apply to security deposit accounts; and a due diligence agreement by the Austrian banking industry, which contains various provisions, including a requirement to sever business relations in cases where there is well-founded suspicion that the funds stem from crime. Tight banking secrecy means that suspicions cannot be reported to the authorities. To date, there is no money laundering offence per se and two categories of anonymous accounts are permitted.

56. The new system being drawn up will provide a much more comprehensive and potentially effective framework. Legislation has been introduced to create a specific money laundering offence, covering the proceeds of all serious crimes. This is to be welcomed, although, in addition to actual knowledge that proceeds derive from crime, it would be desirable if the offence covered cases of wilful blindness or even those where the person should have known the criminal origin of the funds. Legislation is also being drafted to amend the Penal Code concerning confiscation of proceeds from crime, extradition and mutual legal assistance. The Banking Law will be amended to introduce a

mandatory suspicions reporting system (with a central reporting point); provide for immunity from liability for reports made in good faith; and prohibit institutions from warning customers that reports have been made. There will also be enhanced customer identification and record-keeping requirements. Nonetheless, on current proposals, identification would still not be required for passbook and security deposit Schilling accounts held by Austrian residents - a very sensitive issue in Austria and the subject of much ongoing discussion and public debate.

57. It is too soon to make a final evaluation of the Austrian anti-money laundering system, given that the new measures have yet to be implemented. However, whilst acknowledging the progress represented by the proposed laws, the retention of the two classes of anonymous accounts is a matter of concern, running directly counter to a very important FATF Recommendation. Failure to take action in this area would compromise efforts to combat money laundering in Austria and overshadow what should otherwise be a generally commendable system.

Luxembourg

58. Luxembourg does not have a significant drug problem. However, like all international financial centers, it runs the risk of being used by money launderers, as is shown by past money laundering cases, which all had an international dimension, with Luxembourg being used at the intermediary stage of the laundering process.

59. Luxembourg has implemented most of the forty Recommendations of the FATF. It has criminalized narcotics money laundering; and has required banks and other financial institutions to know and record the identity of their customers engaging in significant transactions, including recording sizeable currency transactions at thresholds appropriate to that country's economic situation (client identity must be verified for transactions exceeding 500,000 FLux, roughly US$15,000). It has required banks and other financial institutions to maintain, for an adequate time, records necessary to reconstruct large transactions through financial institutions in order to be in a position to respond rapidly to requests for information from the appropriate authorities in drug-related money laundering cases.

60. Luxembourg has also created systems for identifying, tracing, freezing, seizing and forfeiting narcotics-related assets; and has co-operated, when requested, with the appropriate law enforcement agencies of other governments investigating financial crimes related to narcotics.

61. Luxembourg introduced specific anti-money laundering regulations as early as 1989, in particular the Luxembourg Monetary Institutes's circular 89/57. The Act of 5 April 1993 on the financial sector raised the legal status of these regulations to a single coherent text, applicable to the whole financial sector, thus codifying the requirements imposed on the financial sector by the FATF Recommendations and the 1991 EC Directive. A key point of the new law, central to the FATF Recommendations, is that it obliges financial professionals to take the initiative to inform the public prosecutor of any suspicion of a laundering offence. No professional secrecy obligation inhibits this obligation to inform the authorities and a financial professional who, in good faith, provides such information is protected from criminal and civil liability. A potential problem for Luxembourg is that, as controls discourage the use of the regulated financial institutions, money launderers might be attracted to other less regulated businesses. Another problem concerns the limitation of the predicate offences to those connected to drug trafficking. Efforts are therefore underway to impose on other vulnerable sectors obligations similar to those prevailing for the financial sector, and to extend the incrimination of money laundering to other criminal offences.

62. The concept of money laundering and the role of the financial institutions have undergone an important evolution in Luxembourg. To its credit, the local financial community acknowledges that to

maintain the Grand Duchy's reputation as a safe and sound banking environment, money laundering schemes do little to enhance the center's reputation. At the same time, the enactment of the Act of 5 April 1993 remains an important element in demonstrating Luxembourg's commitment to fighting money laundering and its desire to comply fully with the forty Recommendations of the FATF.

Switzerland

63. The domestic consumption and trafficking of drugs in Switzerland produces only a low level of laundering. On the other hand, as an international financial center, Switzerland is likely to be used for money laundering purposes. The authorities and the banking sector were consequently induced to take significant measures for fighting against this phenomenon.

64. Since 1990, the Swiss Penal Code contains the specific offence of money laundering. Every serious offence, not only drug trafficking, is considered as a predicate offence. The Penal Code also contains a general obligation, which applies to all intermediaries in the financial sector, to identify the customer as well as any possible beneficial owner of the funds. Moreover, the competent authorities are entitled to freeze, seize and confiscate the proceeds of all offences. The Swiss penal law is thus in full compliance with FATF Recommendations 4 and 5, and goes even further than the mere letter of the measures recommended.

65. The banking sector takes advantage of a notable experience in the fight against money laundering. Since 1977, the obligation to identify the contracting partners and beneficial owners of funds is anchored in a private law agreement, the Agreement on the banks' code of conduct with regard to the exercise of due diligence (CDB). This latter has been periodically reinforced, and it is considered as a minimum requirement for the application of penal measures and prudential supervision. The other requirements for banks are set out in a circular of the Federal Banking Commission, the bank supervisory authority. The Swiss banking sector thus applies the great majority of the FATF Recommendations on financial matters. In addition, a Bill introducing the right for financial sector professionals to pass on their money laundering suspicions to the penal prosecution authorities, will soon be submitted to Parliament. However, with regard to the non-banking financial sector, additional efforts will be necessary to implement the FATF Recommendations. In this context, the adoption of the draft Bill on the fight against money laundering in the financial sector, which is still confidential, in a shorter time limit than anticipated, appears as a necessity.

66. While Switzerland has not yet ratified the UN Convention, it already applies its provisions related to international assistance. Its very broad definition of money laundering has furthermore enabled Switzerland to ratify without difficulty, Convention No. 141 of the Council of Europe. With its Federal law of 1983 on International Mutual Assistance in Criminal Matters, Switzerland is finally equipped with a domestic law which allows it to co-operate in this field with all requesting States, even those to whom it is not bound by a bilateral treaty.

67. The progress acccomplished by Switzerland in the fight against money laundering deserves recognition and many aspects of the Swiss system could serve as an example to other Member governments in their own implementation of the FATF's Recommendations.

Assessment

68. No final conclusions on the state of play across the FATF membership revealed by the mutual evaluation exercise can be drawn until all the examinations have been completed. However, some provisional observations can be made. The members examined during FATF-IV were at different stages in the development of their anti-money laundering framework. For example, some had had laws in the area for some years, while others were still in the process of enacting measures. But all were making generally good progress in their implementation of or were already substantially in compliance with the FATF Recommendations.

69. Most already had, or were proposing to enact, a money laundering offence which went wider than just the proceeds of drugs trafficking. All fully recognised the importance of enlisting the support of the financial community in the fight against money laundering and the banking sector was already well aware of the problem, although the position was more variable in the case of non-bank financial institutions. In all cases, the reports pointed to some areas where the anti-money laundering framework could be strengthened with a view to maximising the effectiveness of the counter-measures and preventing the exploitation of any weak links in the system by money launderers.

II. MONITORING DEVELOPMENTS ON MONEY LAUNDERING TECHNIQUES AND REFINEMENT OF THE FATF RECOMMENDATIONS

70. Money laundering is a dynamic activity. The criminals are constantly searching for new points of vulnerability and adjusting their laundering techniques as FATF members and other countries apply counter-measures. An essential element of the FATF's work is therefore to collect and share information on the latest developments and trends in money laundering methods and consider appropriate responses.

1992-1993 Survey of Laundering Trends and Techniques

71. It is rare for a genuinely new technique to be developed - and none were discernible in the monitoring exercise carried out in FATF-IV. But the exercise did reveal important trends in the pattern of money laundering and the increased utilisation of more sophisticated methods. Many methods mentioned in earlier exercises, such as the use of wire transfers, structuring of transactions ("smurfing"), were emphasised as subjects of continuing concern. However, it was noted that there was an increasing amount of laundering of the proceeds of non-drugs crimes, for example, arms smuggling and "white-collar" crime.

72. The trend towards greater use of non-bank financial institutions as a means of getting the proceeds of crime into the financial system ("placement") was confirmed. The use of bureaux de change, casinos, financial brokers, life insurance and postal money orders were all mentioned in cases submitted by FATF members.

73. Evidence was also presented of the increasing use of legitimate non-financial businesses, such as retail shops and import-export companies. (This was a major feature of the famous "Green Ice" operation against the Colombian cocaine cartels.) These businesses were used not only for the investment of the proceeds of crime (the final "integration" phase of a laundering operation) but also in earlier phases of placement and "layering" (conducting a series of transactions to hide the illicit origin of the money). Control over well-established existing businesses by money launderers provides a continuing means of facilitating their operations. The proceeds of crime can be commingled with those of the legitimate commercial activities of the company and false invoicing used to disguise the illicit origin of funds. Such businesses can also be used in drug trafficking operations themselves: shipments of drugs being sent together with the legitimate goods in which the companies were dealing.

74. Shell corporations continue to be widely used by money launderers, mainly, though not exclusively, those registered in offshore havens. Finally, the renewed recourse to physical movement of cash across international borders, using increasingly sophisticated methods of concealment, was noted.

Refinement of Countermeasures

75. In response to the findings from this exercise, the FATF launched various new studies of appropriate counter-measures as well as continuing the policy development work begun in early rounds, notably on the use of non-bank financial institutions for money laundering. As in FATF-III, it was decided not to add to, or modify, the original forty Recommendations for the time being. But FATF-IV agreed to adopt three further Interpretative Notes to the existing Recommendations and also carried out substantial work on other issues.

Interpretative Notes

(i) Controlled Delivery

76. FATF-III agreed an Interpretative Note stating that members should consider taking measures to postpone or waive the arrest of suspected persons and/or seizure of suspect funds to enable the identification of those engaged in suspected money laundering operations and gather evidence. In 1992-1993, the FATF looked further at the technique of controlled delivery - allowing shipments of or transactions involving items of a suspect origin to proceed under the surveillance of the authorities to identify and gather evidence against as many as possible of the criminals involved. The use of this technique in international drugs trafficking cases has been accepted for many years but it is equally applicable in those involving suspected money laundering. To promote the use of this technique, the FATF therefore adopted the following Interpretative Note to Recommendations 32, 33, 36 and 38 (which deal with exchange of information and co-operation between legal authorities):

" The controlled delivery of funds known or suspected to be the proceeds of crime is a valid and effective law enforcement technique for obtaining information and evidence in particular on international money laundering operations. It can be of great value in pursuing particular criminal investigations and can also help in obtaining more general intelligence on money laundering activities. The use of these techniques should be strongly encouraged. The appropriate steps should therefore be taken so that no obstacles exist in legal systems preventing the use of controlled delivery techniques, subject to any legal requisites, including judicial authorisation for the conduct of such operations. The FATF welcomes and supports the undertakings by the Customs Co-operation Council and INTERPOL to encourage their members to take all appropriate steps to further the use of these techniques."

(ii) Insurance

77. During 1992-1993, the FATF discussed modalities for implementing its Recommendations on financial matters (Recommendations 9-32) in specific sectors of non-bank financial institutions, particularly in the insurance industry.

78. With regard to the scope of application of the Recommendations, it was recognised that, while life insurance can be an instrument for laundering illicit funds, money laundering through non-life insurance or insurance products other than investment products, is rare. To take account of this, the following Interpretative Note was adopted to Recommendation 9:

> "The FATF Recommendations should be applied in particular to life insurance and other investment products offered by insurance companies, whereas Recommendation 29 applies to the whole of the insurance sector."

79. As far as the increased diligence of financial institutions is concerned, the following Interpretative Note to Recommendation 15 was agreed to clarify what was meant by the term "transactions" in relation to insurance:

> "The word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits."

Shell Corporations

80. It was agreed in FATF-III that FATF members should take notice of the potential for abuse by money launderers of shell corporations and should consider measures to prohibit unlawful use of such entities. The further work carried out on this issue in FATF-IV has focused on studying the ways in which shell corporations (and similar entities such as ghost or front corporations) can be employed in money laundering operations; and in discussing appropriate steps which would counter these abuses without prejudicing the legitimate use of such bodies. A survey of FATF members and a sample of non-FATF jurisdictions was carried out to obtain information on the form of beneficial ownership and conditions for incorporation of shell corporations; and the ability to find out who owns such bodies and provide this information to foreign and domestic law enforcement authorities. The legislation of the various FATF members differs significantly in this field of commercial law.

81. A key factor which makes shell corporations attractive to money launderers is the ability in many jurisdictions to conceal or obfuscate the true beneficial ownership of the entity. The FATF has therefore concentrated on the issue of transparency of ownership. The FATF Recommendations already place responsibilities on financial institutions to identify their clients and take reasonable measures to obtain information about beneficial customers, particularly in the case of domiciliary companies. Active consideration is being given to a possible Interpretative Note to these Recommendations or further guidance which would clarify the measures to be taken by financial institutions in obtaining identification information in respect of such clients. Consideration has also begun of the feasibility of specific methods to ensure that adequate records of owners of shell corporations are maintained and can be accessed by law enforcement authorities.

Use of Non-Financial Businesses for Money Laundering

82. The range of businesses which can be used - whether wittingly or unwittingly - by money launderers is a wide one. Those which deal with large amounts of cash or conduct some form of financial services activity in addition to their mainstream operations are potential targets. Work has begun on identifying businesses which carry out quasi-financial activities and will consider where application of the FATF Recommendations is appropriate and which are the relevant Recommendations. However, this is obviously a major and complex area which will need to be the subject of a long-term study.

Non-Bank Financial Institutions

83. The Task Force reviewed the tendencies of the use of the non-banking financial sector by money launderers. Bureaux de change, intermediaries in investment businesses and insurance companies were identified as having been used, or particularly vulnerable to being used, for money laundering. The results of this study will provide the basis for further work during FATF-V. In parallel, modalities for implementing the FATF financial Recommendations in the non-bank financial sector were discussed on several occasions.

Customer Identification

84. Work was also carried out on the specific problem of how best to conduct identification in cases where there is no face-to-face contact between the institution and its customer. In such cases, the provision of identifying documents poses real difficulties or is impractical and runs counter to the way in which transactions or business relations are conducted. It was agreed that further work should be done on this important issue in 1993-1994, bearing in mind the need to ensure both a level playing field for the various categories of financial institutions and a proper balance between flexibility and security.

Electronic Fund Transfers

85. In 1992-1993, the FATF addressed the issue of how to deal with money laundering cases that involve use of domestic and/or international electronic funds transfers. FATF members took note of the increased use of electronic payment and message systems in the money laundering process. They held meetings with SWIFT (the Society for Worldwide Interbank Financial Telecommunications) in order to discuss their concern that international funds transfers can be used to dissimulate the identity of the original ordering customer or the beneficiary. As a result, SWIFT responded to this concern by broadcasting a message to all the users of its system asking them to include these details in the messages they send. In turn, national authorities have also taken steps to encourage the users of the SWIFT system, within their respective jurisdictions, to follow the advice contained in the SWIFT broadcast. SWIFT and the FATF have also co-operated in studying what further improvements might be made to the audit trail left by electronic payment and message instructions.

III. EXTERNAL RELATIONS

86. In 1992-1993, the FATF intensified its efforts to promote the widest possible world-wide action against money laundering, based on the external relations plan agreed in the previous round. A series of initiatives were mounted in different parts of the world to disseminate the FATF programme and respond to requests from particular countries for provision of training and technical assistance. The Task Force has also continued to monitor progress by dependent, associate or otherwise connected territories of FATF members in adopting and implementing the forty Recommendations.

87. In carrying out its external relations programme, the FATF collaborates closely with other international and regional organisations with an interest in combating money laundering. These links have been strengthened and diversified during the past year and the FATF aims to develop an increasingly co-ordinated approach in the future.

(i) Disseminating the FATF Programme

88. An essential feature of the FATF's external relations strategy is its multi-disciplinary approach. Great emphasis is placed on gathering together all the relevant interests concerned - financial and regulatory; legal and judicial; and law enforcement - and promoting co-operation between them. As far as possible, the FATF also seeks to involve financial institutions as well as government agencies in its contacts with non-member countries.

89. Geographically, the FATF has concentrated its efforts on three regions during 1992-1993: the Caribbean area; Central and Eastern Europe; and Asia.

a) The Caribbean

90. FATF members have worked closely with the Caribbean Islands and Central American States since 1990 when a drug money laundering conference was held in Aruba. Subsequently a Caribbean Financial Action Task Force (CFATF) was formed. The CFATF process has gathered pace in 1992-1993 and major progress has been made in promulgating the FATF message in the region. A Ministerial Conference of the CFATF held in Jamaica in November 1992 formally endorsed and undertook to implement the forty FATF Recommendations and the nineteen Recommendations drawn up at the Aruba Conference in 1990. The CFATF also agreed on the need for a mechanism to monitor and encourage progress in this work, including a self-assessment and evaluation process. To further this aim and to facilitate the provision of training and technical assistance in the region, the meeting proposed the creation of a small CFATF Secretariat to be based in Trinidad and Tobago, which is taking over the Presidency of this body. A further meeting of the CFATF will be held in 1994 to evaluate progress.

b) Central and Eastern Europe

91. Central and Eastern Europe has been a particular focus for the FATF's external relations work during 1992-1993. The countries present an increasingly attractive target for money launderers as they liberalise their economic and financial systems. With the increasing presence of organised crime in the area, there is also a growing risk of domestic money laundering operations. The FATF has therefore been encouraging these states to implement effective anti-money laundering measures in the process of reforming their laws and financial systems.

92. At the occasion of the Council of Europe's money laundering conference in September 1992, FATF members held meetings with delegates from most Central and Eastern European countries to find

out more about the money laundering situations within these countries and discuss how the FATF might assist them. These contacts resulted in the FATF's organising two seminars in Hungary and Poland.

93. The first took place in Budapest in early February. In addition to representatives from Hungarian government agencies and commercial banks, delegations from Albania, Bulgaria, the Czech Republic, Poland, Romania and Slovakia attended as observers. In preparation for the seminar, FATF members held detailed discussions with Hungarian officials and bankers on the money laundering situation in Hungary and progress in developing counter-measures. The symposium covered all aspects of the anti-money laundering framework and resulted in the preparation of a set of recommendations to the Hungarian authorities on their next steps in this area.

94. A similar symposium took place in Warsaw in early March for officials from Polish government agencies and financial institutions. Again, the FATF held discussions with the relevant Polish agencies beforehand, including the Governor of the National Bank of Poland and other high-level officials, and produced recommendations for the Government of Poland.

95. Individual FATF members took part in other missions to particular Central and Eastern European countries and both the European Community and the Council of Europe have ongoing initiatives in the region.

96. The FATF and UNDCP are now initiating a dialogue with relevant policy makers in Russia. The FATF will also be following up the links established with Hungary and Poland to evaluate progress and provide further assistance as necessary.

c) Asia and the Pacific

97. Preliminary contacts with Asian and Pacific countries had been made in earlier FATF rounds. However, given the importance of this region, both in terms of the numbers of developed or emerging financial centres as well as drug producing countries, the FATF undertook two initiatives in the area during 1992-1993.

98. The Sydney meeting of the FATF in September included a programme for selected Asian and Pacific states. Representatives from Fiji, Indonesia, Malaysia, Nauru, Papua New Guinea, the Philippines, the Solomon Islands, Tonga and Taiwan took part in presentations and discussions on the money laundering situation in the region.

99. This was followed in April 1993 by the Asia Money Laundering Symposium. This was organised jointly by the FATF and the Commonwealth Secretariat, with the support of the UNDCP, and hosted by the Government of Singapore. The Symposium was attended by participants from fourteen non-FATF countries/regions and SEACEN, as well as nine FATF members, the UNDCP and INTERPOL. The Symposium concentrated on raising awareness of the money laundering problem and explaining countermeasures. The non-FATF members were asked to give serious consideration to implementing the forty FATF Recommendations, and interest was expressed in holding a follow-up Symposium in about a year's time.

d) Other Areas

100. In November 1992, FATF members met representatives of the Central African Republic, the Ivory Coast, Kenya, Morocco, Nigeria and Zimbabwe for discussions on the best way of pursuing anti-money laundering initiatives in Africa. Consultations are also taking place with selected regional organisations. The FATF is now drawing up proposals for a programme of action in Africa during the 1993-1994 Round of the Task Force.

101. In the Middle East, a conference on money laundering, organised jointly by the FATF, the Gulf Co-operation Council and the Saudi Arabian Monetary Authority, is planned for October 1993. In South America the FATF is continuing to follow the progress of the Organisation of American States' anti-money laundering initiative.

(ii) Implementation of FATF Recommendations by Dependent, Associate or Otherwise Connected Territories of FATF Members.

102. The FATF has continued to oversee the action taken by these non-member territories in implementing anti-money laundering measures. The reports provided by the FATF members who have links with these territories indicate that good progress is being made in a number of areas. Most are in the process either of enacting or implementing laws to make money laundering a criminal offence. However, it was agreed that the sponsoring FATF members should maintain their efforts to encourage these territories to put in place a comprehensive anti-money laundering system as soon as possible.

103. The FATF has begun consideration of how to evaluate progress by these territories. Some already take part in the FATF self-assessment survey or will be covered by the Caribbean FATF evaluation process. But these arrangements are not systematic or comprehensive at present.

Co-operation with Regional and International Organisations

104. While the Task Force is the only international body which specialises in and concentrates solely on the fight against money laundering, it works in close co-operation with other international organisations in this field. Representatives from the Council of Europe, INTERPOL, the UNDCP and the Customs Co-operation Council have regularly attended FATF meetings and participated in the planning and execution of the various initiatives carried out in 1992-1993 and contacts have also been maintained with the IMF and the World Bank. Close links have been established with the Commercial Crime Unit of the Commonwealth Secretariat and the FATF is also having discussions with the European Bank for Reconstruction and Development regarding anti-money laundering initiatives in Eastern Europe.

105. It is clearly important that the international community avoids overlap and duplication and draws strength from collective action. In conjunction with the other major organisations, FATF is therefore taking steps to promote a more co-ordinated approach in this area.

Assessment

106. The FATF has made substantial progress in its external relations agenda during round IV. Promoting money laundering awareness remains an important element of its work. But, in addition to seeking a firm commitment to implementation of the forty Recommendations, the FATF also wants to secure agreements by third countries to be evaluated on their progress in applying anti-money laundering measures. Clearly, results cannot be expected immediately and the FATF is at different stages in its dialogue with various regions. However, the Caribbean FATF process has shown that, over time,

substantive commitments can be achieved. The challenge for the future is to give substance to the contacts which have already been made, whilst spreading the FATF message to those parts of the world where even awareness of the money laundering problem remains at a very low level.

CONCLUSIONS

107. The FATF has made substantial progress in its work in 1992-1993 and last year's experience confirmed that it remains an effective and flexible forum for combating money laundering. Implementation of the forty Recommendations by FATF members is gathering pace and the monitoring mechanisms devised in round III provide a searching scrutiny of performance. The FATF's external relations efforts have been intensified and, as the Caribbean FATF process shows, have now started to produce firm commitments in important areas to action against money laundering. The FATF has also continued to undertake valuable work in refining and developing anti-money laundering counter-measures.

108. Nevertheless, there can be no cause for complacency nor any let up in the efforts of the Task Force to carry out its programme. There is still some way to go before all the Recommendations are implemented and it is essential that all members complete the process without further delay. There is also a need to be constantly on guard against new money laundering techniques and take prompt action to remedy any weaknesses revealed. In its external relations work, the Task Force, in co-operation with other international bodies, must maintain the momentum of its efforts to persuade all financial centres to join the fight against money laundering. There are still some areas where the FATF's message has not penetrated and others where further work is needed to reinforce the process. The more widespread the action against money laundering, the more effective it will be.

109. The 1993-1994 round of FATF, which will be chaired by the United Kingdom, will therefore have a full agenda. This will include the review of the future of the FATF, which will examine the statute and future operations of the Task Force.

FATF-IV

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

ANNEXES TO THE ANNUAL REPORT 1992-1993

June 29, 1993

CONTENTS

REPORT TO THE FATF FROM WORKING GROUP I (LEGAL MATTERS)
1992-93

I. Introduction

On 9-11 September 1992, FATF IV established the following mandate for Working Group I:

1. In consultation with Working Group II, continuation, updating and improvement of the balanced monitoring mechanism for:

a) self assessment:

i) questionnaire
ii) compilation and analysis of answers

b) mutual evaluation:

i) questionnaire;
ii) participation in discussion of the draft reports.

Working Group I covers Recommendations 1-8 and 33-40 and, jointly with Working Group II, Recommendation 32.

2. Monitoring of new money laundering techniques ("typology"), in cooperation with Working Groups II & III, including general lessons to be learnt from specific cases.

3. Complements and/or Interpretative Notes to the 40 Recommendations as necessary.

4. Further study of legal issues, including, inter alia, "predicate offences", "shelf corporations", corporate liability and controlled delivery; and discussion of practical aspects of legal cooperation between FATF members, (in particular, extradition and cooperation in the prosecution of defendants).

5. Input as necessary into WG II work (for example on electronic fund transfers)

In FATF IV Working Group I concentrated on four main areas:

(a) reviewing the progress of FATF members in implementing the 40 FATF Recommendations through analysis of the self-assessment questionnaires and participation in discussion of the eight mutual evaluation reports completed during the Round;
(b) monitoring of new money laundering techniques and counter-measures;
(c) further studies of the issues of shell corporations and controlled delivery;
(d) launching a study of ways of countering money laundering by non-financial businesses.

During 1992-93 the Group met 5 times (9 September 1992, 20 January 1993, 30 - 31 March 1993, 12-13 May 1993 and, in conjunction with Working Group II 28 June 1993). A sub-group meeting on money laundering typologies was also held on 16 November 1992.

II. Reviewing Progress in Implementing Anti-Money Laundering Measures

At the 9 September meeting the Working group agreed to make various revisions to the legal matters self-assessment questionnaire so that it now covers all the relevant FATF Recommendations. All member governments completed the questionnaire. The Secretariat then produced a compilation of the answers which was discussed at the meeting of the Group on 31 March. A revised compilation, incorporating amendments proposed by FATF members, was then re-circulated at the meeting on 12 May. This compilation was approved by all members.

The analysis of responses indicated that FATF members have continued to make substantial progress in implementing the legal Recommendations. For example, 10 members have now fully implemented the Vienna Convention and another 8 expect to have done so within the next 12 months. A further 4 members have partially implemented the Convention. Similarly, nearly all members have criminalised drug money laundering or expect to do so over the next year. Moreover, an increasing number of members have decided to go beyond a purely narcotics-based offence and to criminalise the laundering of the proceeds of all serious crimes or offences which generate a significant amount of proceeds. 10 members have already introduced such measures and another 8 are in the process of doing so. There has also been encouraging progress in promoting mutual legal assistance between members on money laundering issues.

The Group also participated jointly with Working Group II in the discussion of the draft mutual evaluation reports on Denmark, US, Belgium, Canada, Italy, Austria, Luxembourg and Switzerland. These reports were endorsed, subject to amendment, and forwarded to the plenary.

III. Monitoring New Money Laundering Techniques and Countermeasures

As in previous FATF Rounds, a major element in FATF IV was the refinement and updating of assessments of money laundering techniques.All members were invited to submit written case histories or synthetic analyses illustrating developments in this area. 20 members contributed to this exercise. An expert sub-group, attended by representatives from most FATF members together with INTERPOL, UNDCP and the CCC, was convened on 16 November 1992 to discuss this material and present othercases. A typology paper, incorporating these examples and the conclusions of the sub-group, was then prepared and discussed at a joint meeting of Working Groups I and II on 19 January. The paper was endorsed subject to minor changes.

The exercise revealed no genuinely new money laundering techniques. However, it indicated various significant trends. The use of shell corporations and wire transfers as methods of laundering money were emphasised as a subject of continuing concern. The trend towards increasing use of non-bank financial institutions for placement activity also appeared to be continuing. There was also increased evidence of the use of non-financial businesses for the placement and layering as well as the integration of the proceeds of crime, and in drug-trafficking operations themselves. Finally, the renewed recourse to the physical movement of cash across international borders was noted. As regarded law enforcement counter-measures, the use of controlled delivery and other types of undercover operations were emphasised as valuable and important techniques.

IV. Shell Corporations

The use of offshore shell corporations in money laundering schemes had been noted in FATF III and it had been agreed that FATF members should take notice of the potential for abuse by money launderers of these bodies and should consider measures to prohibit unlawful use of such entities. Further work on this subject was carried out in FATF IV. The US delegation presented a detailed study on the ways in which shell corporations (and similar entities such as ghost and front companies) could be used to facilitate laundering. Working Group I also carried out a survey in FATF members and a sample of non-FATF jurisdictions of the conditions of ownership and incorporation for shell corporations; and of the ability to obtain information about such ownership and provide it to foreign and domestic law enforcement.

In the discussion of ways to counter the use of shell corporations for money laundering, the importance of transparency regarding the beneficial ownership of these bodies was highlighted. It was noted that the FATF Recommendations already covered the responsibilities of financial institutions to identify their clients, including beneficial owners. A general discussion was held on the need for on Interpretative Note in this area and a draft of such a Note was presented to the joint meeting of Working Groups I and II on 12 May. At this meeting it was agreed that further consideration should be given to this subject at a meeting of Working Group II in June and, as appropriate that Working Group I would have the opportunity to examine further the legal aspects of the issue.

Working Group I also considered the feasibility of other mechanisms to ensure that adequate records of the owners of shell corporations were maintained and available to law enforcement authorities in money laundering investigations.

V. Controlled Delivery

Working Group I had considered the issue of and adopted an Interpretative Note on deferred arrests and seizures in FATF III. In 1992-93 further work was carried out on the technique of controlled delivery. The Group agreed that this was an important law enforcement countermeasure against money laundering, particularly at the international level and adopted an Interpretative Note concerning removal of legal impediments to the use of this technique. The text of the Interpretative Note and supporting explanation is attached.

VI. Use of Non-Financial Businesses for Money Laundering

The Group held three discussions on the question of what countermeasures might be introduced to combat money laundering through non-financial businesses. It was recognised that this was a complex area which needed to be the subject of a long term study, extending into future FATF Rounds. It was noted that a wide variety of businesses could be used - whether willingly or without their knowledge - for money laundering purposes. Vulnerable businesses ranged from ones which carried out activities similar to those conducted by financial institutions to businesses which dealt with large amounts of cash.

It was agreed that in its work the Group should concentrate first on the quasi-financial businesses and: (i) examine how to identify such businesses; (ii) in what sectors or in what circumstances thesebusinesses should be subject to the FATF Recommendations; and (iii) what were the appropriate Recommendations for such businesses. In relation to the first item, the Group considered an approach based on the types of activity conducted rather than the sector or entity involved, including the implications of such an approach for the selection of the anti-money

laundering requirements to be applied. The Group considered that this approach merited further study along with other possible alternatives.

The work on use of non-financial businesses for money laundering will be pursued in Round V of FATF.

REPORT FATF IV - WG II

Report to the FATF from Working Group II (Financial Matters)

1992-1993

I. INTRODUCTION

On 9-11 September 1992, FATF-IV established the following mandate for Working Group II:

1. Continuation, updating and improvement of the balanced monitoring mechanism for, in consultation with Working Group I:

(a) self assessment:
(i) questionnaire;
(ii) compilation and analysis of answers;

(b) mutual evaluation:
(i) questionnaire;
(ii) participation in discussion of the draft reports.

Working Group II materially covers the topics of Recommendations 9-31. (Working Group I covers Recommendations 1-8 and 33-40); Recommendation 32 is covered by both Working Groups.)

2. Collection and dissemination among members of members' (updated) lists of non-bank financial institutions and other businesses that have been used, or are particularly vulnerable to being used, in money laundering.

3. Regulatory coverage of non-bank financial institutions.

4. Monitoring of new money laundering techniques ("typology") in co-operation with Working Groups I and III, and under the leadership of Working Group I, including general lessons to be learnt from specific cases.

5. Complements and/or interpretative notes to the 40 Recommendations as necessary.

6. Collection and dissemination among members of members' guidelines for assisting financial institutions in detecting suspicious patterns of behaviour by their customers, and consideration of the feasibility and utility of collecting suspicious or unusual transaction reports currently used in member countries in a standardised form and developing a standardised transaction reporting format.

7. Consider the feasibility and utility of measures dealing with money laundering cases that involve use of domestic and/or international electronic funds transfers.

8. Input, as necessary, into WGs I and III work (for example, shell corporations: standards of incorporation, recordkeeping by attorneys and other intermediaries, and due diligence by financial institutions).

During 1992/1993, the Working Group met six times (9-10 September 1992, 17 November 1992 (volunteer meeting), 20 January 1993, 31 March 1993, 12 May 1993, 28 June 1993. These meetings enabled Working Group II to address the issues contained in its mandate.

II. ACCOMPLISHMENTS

1. Monitoring Mechanism

(a) Self-assessment

During the 9-11 September 1992 FATF meetings, a revised self-assessment questionnaire was agreed upon. All countries have filed their answers to the questionnaire. The Secretariat has distributed a detailed compilation of answers to the questionnaire. During its 31 March 1993 meeting the Working Group discussed this compilation. As the answers filed are supposed to reflect the current state of implementation, several members subsequently updated the information contained in the compilation. An analysis, based upon the filed answers to the questionnaire as updated, was circulated.

(b) Mutual evaluation

During the 9-11 September 1992 FATF meetings, a revised mutual evaluation questionnaire was agreed upon. The Plenary adopted the programme for FATF-IV which included the mutual evaluation schedule. During a joint meeting on 30 March 1993, Working Groups I and II discussed the draft reports on Denmark and the United States. These groups jointly discussed draft reports on Belgium, Canada and Italy on 13 May 1993, and draft reports on Austria, Switzerland and Luxembourg on 28 June 1993. After having made some amendments, the working groups advised the Plenary to accept the reports.

2. Collection and dissemination among members of members' (updated) lists of non-bank financial institutions and other businesses that have been used, or are particularly vulnerable to being used, in money laundering.

A large majority of FATF members participated in an exercise to identify types of non-bank financial institutions[1]) and other businesses that have been used, or are particularly vulnerable to being used, in money laundering. A compilation of lists of such institutions was made by the Secretariat based on members' contributions. This compilation was discussed in a volunteer meeting of the Working Group on 17 November 1992 and subsequently during working group meetings on 20 January and 31 March 1993.

The Working Group identified categories which were often, sometimes, and occasionally mentioned. Within the main categories of non-bank financial institutions, bureaux de change), intermediaries in investment business, and life insurance companies were often mentioned by FATF members. Other categories of non-bank financial institutions, such as postal financial services, finance

[1] It is noted that FATF leaves the definition of "bank" or "credit institution" to individual members. Consequently, the definition of bank, and also of "non-bank financial institution" may vary between members. Members with a broad definition of "bank" may identify fewer non-bank financial institutions.

companies, collective investment schemes, and credit card companies were sometimes quoted. Leasing and factoring companies and money transmitters were occasionally quoted.

The issue of non-financial institutions and businesses was referred to Working Group I (legal issues). The first FATF-V Plenary could consider whether the compilation of lists of non-bank financial institutions would be the basis for further action. This action would concern some of the most often mentioned sectors on specific recommendations, particularly no. 15 (complex, unusual large transactions, and unusual patterns of transactions, which have no apparent economic or visible lawful purpose); no. 16 (suspicion that funds stem from a criminal activity); nos. 20/26 (programmes against money laundering); and no. 28 (guidelines which will assist (non-bank) financial institutions in detecting suspicious patterns of behaviour by their customers).

3. The application of the FATF Recommendations to non-bank financial institutions

During its volunteer meeting on 17 November 1992, and during its meeting on 31 March 1993, the Working Group discussed modalities for implementing the FATF Recommendations on financial matters (9-32, except recommendations 12 and 13 which are subject to a specific study on identification: see item 5 of this report) in three specific sectors of non-bank financial institutions: the securities (intermediaries in investment business) and insurance industries, and the bureaux de change. The discussions were structured on the basis of papers presented by the United Kingdom (securities), the Netherlands (insurance), and the United States (bureaux de change). A report has been prepared on the basis of the discussions of the Working Group, identifying relevant particulars of these sectors and containing proposals for clarifications and interpretative notes to Recommendations 9 and 15. The two interpretative notes are related to the insurance sector and they read as follows:

Recommendation 9: **"The FATF Recommendations should be applied in particular to life insurance and other investment products offered by insurance companies, whereas Recommendation 29 applies to the whole of the insurance sector."**

Recommendation 15: **"The word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits."**

4. New money laundering techniques

On 19 January 1993, a joint meeting of Working Groups I and II discussed and adopted the draft report that had been prepared by the 16 November 1992 typologies Sub-Group meeting. The report of Working Group I (legal issues) covers this issue in more depth.

5. Complements and/or interpretative notes to the 40 Recommendations as necessary

The Working Group saw no need for additional recommendations. As noted under 3 above, two interpretative notes are suggested for the implementation of the recommendations in the insurance sector.

In parallel, the Working Group noted that many transactions or entries into business relations between financial institutions and their customers involve no face to face contact between the two parties. In such cases, the provision of identifying documents poses real difficulties or is impractical and runs counter to the way in which transactions/business relations are conducted in these cases. A non paper on customer identification requirements for certain transactions with financial institutions set out an analytical view of the general identification requirements in cases where there is no face to face contact between the

institution and its customer. Although the Working Group recognised the importance of this subject, it was decided not to adopt interpretative notes. It was agreed to further work on the issue of identification requirements (Recommendations 12 and 13) during FATF-V, bearing in mind two specific elements: the need to establish a level playing field between categories of financial institutions and a balance between flexibility and security.

6. Suspicious and unusual transactions guidelines and reporting formats

The Working Group noted that point 6 of its mandate contains two aspects:

(a) collection and dissemination among members of members' guidelines for assisting financial institutions in detecting suspicious patterns of behaviour by their customers; and

(b) consideration of the feasibility and utility of collecting suspicious or unusual transaction reports currently used in member countries in a standardised form and developing a standardised transaction report format.

With regard to point (a), members were asked to provide the Secretariat with updates and new elements that could be useful to other members who are also in the process of developing guidelines for assisting financial institutions in detecting unusual or suspicious patterns of behaviour by their customers (the implementation of recommendations 15, 16, 20/26 and 28). The Secretariat has made a compilation of members' updates.

With regard to point (b), the Italian delegation and the Secretariat have drafted a brief questionnaire on the issue of standardisation. It contains two main questions:

- what are the view of the members on which information should as a minimum be contained in a suspicious or unusual transaction report?

- what actual measures have been taken by the authorities to ensure that financial institutions provide this information?

This questionnaire will be used to address the feasibility and utility of this standardised transactions reporting format during FATF-V.

7. Electronic funds transfers

Following on from analysis presented to the FATF by various law enforcement authorities showing that many major money laundering cases in recent times have involved the use of electronic payment arrangements, the FATF mandated an ad hoc group to study the use made of the world's electronic funds transfer systems in the money laundering process. The ad hoc group concluded that it had become relatively easy to transfer funds through the international banking system in such a way that the identity of the original ordering customer or the ultimate beneficiary is concealed.

The ad hoc group was mandated to hold discussions about this issue with the Society for Worldwide Interbank Financial Telecommunication SC (SWIFT) - the principal carrier of cross-border electronic payment messages. These resulted in the Chairman of SWIFT sending a broadcast to all users of the SWIFT system on 30 July 1992 asking them to ensure that they key fields for the ordering and

beneficiary customers in the important MT100 message type are completed with names and addresses.[2] A subsequent follow-up letter was sent to all user organisations on 30 October 1992 by the Chief Executive Officer of SWIFT. FATF member governments have also taken steps to encourage the users of the SWIFT system within their own respective jurisdictions to follow the advice contained in the SWIFT broadcast.

Further discussion with SWIFT has resulted in their agreeing to redraft the instructions for completion of the ordering institution field in the MT100 message type and to issue a Usage Guideline on identifying the ordering parties in the MT100. The purpose of this is to ensure that, regardless of however many messages are sent to achieve a particular payment, details of the financial institution which initiated the payment for the ordering customer are identified throughout the payment chain.

These two initiatives are aimed at ensuring that using the SWIFT system to give payment instructions does not provide money launderers with a means of breaking the audit trail. FATF member governments would determine if it is appropriate and technically feasible that payment messages in their respective national electronic payment systems contain information on the ordering and beneficiary customers and the institution that originated the payment instruction.

8. Input into the work of other working groups

On 19 January 1993, a joint meeting of Working Groups I and II had a presentation by the United States on the subject of shell corporations, followed by a preliminary discussion of the issues. On 30 March 1993, Working Groups I and II had a further presentation on this subject. The issue of shell corporations was discussed again during the FATF May and June meetings.

[2] In the case of the ordering customer, if it is not possible to include the name and address, the account number may be included instead.

REPORT TO THE FATF FROM WORKING GROUP III (EXTERNAL RELATIONS) 1992-93

I. Introduction

The mandate for Working Group III was adopted at the FATF meeting on 10 - 11 September 1992. The work of the Group during 1992-93 has concentrated on implementing of the action programme for external relations set out in the report of FATF III. The Group mounted a large number of activities to promote the widest possible global mobilisation against money laundering, and encourage non-Member governments both to commit themselves to implement the FATF Recommendations and agree to assess their progress in doing so. In response to requests from particular third countries, Working Group III has also provided training and technical assistance through the services of FATF Members and others. The Group has also developed its co-operation with the international and regional organisations with an interest in money laundering. Finally, the Group has continued to monitor the contacts between relevant Member governments and their dependent, associate or otherwise connected territories regarding their implementation of Task Force Recommendations.

II. Outreach Programme

In carrying out its programme of contacts with third countries the Group decided to create various sub-groups of particular FATF members to advise on the best approach for developing contacts with selected regional areas. Under the general direction of the Group, these sub-groups have organised and carried out various seminars and training programmes.

a) Central and Eastern Europe

Central and Eastern Europe has been a particular focus for the FATF's external relations work during 1992-93. Although this area is not at present a major money laundering centre, the countries are becoming an increasingly attractive target for money launderers as they develop their financial systems, open their economies and move towards convertibility of their currencies. With the spread of organised crime gangs in this part of Europe, the area could also see the development of domestic money laundering operations, making use of the financial systems in other countries as well as their own. Hence it is very important that they take the opportunity of the reform and restructuring of their laws and systems to put in place measures to protect themselves against money laundering.

The Council of Europe held a major money laundering conference in Strasbourg in September 1992, attended by representatives from most Central and Eastern European countries, including Russia and certain Newly Independent States. In the framework of this conference members of Working Group III met delegates from Hungary, Poland, the (then) Czech and Slovak republics, Bulgaria, Romania, Russia, Latvia, Croatia and Slovenia. The purpose of these meetings was to find out more about the money laundering situations within these countries and discuss how the FATF might assist them.

These contacts led to requests for both policy seminars and more detailed training programmes from Hungary and Poland. The first seminar took place in Budapest on 4-5 and 8-10 February. In addition to representatives from financial, legal, prosecutorial and law enforcement interests from Hungary (including commercial banks), delegations from Albania, Bulgaria, the Czech Republic, Poland, Romania and Slovakia attended the policy seminar as observers, thanks to financial support from the Council of Europe. The seminar and training programme were carried out by delegations from 9 FATF members, together with officials from the Council of Europe, INTERPOL and the UNDCP and

included representatives from banks and other financial institutions. Prior to the policy seminar, the FATF presenters met with relevant Hungarian Ministries and agencies for detailed discussions on the money laundering situation in Hungary and progress in developing counter-measures. The seminar and training programme provided a thorough exposition of anti-money laundering measures, with individual sessions for financial, regulatory, legal and law enforcement groups. The outcome was the preparation of a set of recommendations to the Hungarian authorities on their next steps in this area.

The symposium in Warsaw, held on 2-4 March, followed a similar pattern, although in this case participation was limited to officials from Polish government agencies and financial institutions. The experience gained from the seminar in Budapest enabled the refinement and compression of the programme. Again, the FATF presenters had the opportunity for discussions with the relevant Polish agencies before the start of the seminar and there was also a meeting with the Governor of the National Bank of Poland and other high-level officials, and recommendations were made to the Polish authorities resulting from the symposium.

In addition to these two events, during the year individual FATF members also took part in missions to particular Central and Eastern European countries organised by the Council of Europe or on a bilateral basis. The European Community has incorporated in its Association agreements with Eastern European countries specific clauses committing them to apply the FATF recommendations. A PHARE pilot programme of assistance to six countries in the region is being set up in the field of drugs. This programme covers money laundering. The FATF and UNDCP have also begun preparations for a money laundering seminar in Moscow in September for Russia and other members of the CIS.

b) Asia and the Pacific

Contacts with Asian and Pacific countries had been made in earlier FATF Rounds through a conference organised by Japan, together with the Economic and Social Commission of the United Nations for Asia and the Pacific, in February 1991 and FATF representation at a meeting of South East Asian Central Banks Board of Governors in Jakarta in October 1991. Given the importance of this region both in terms of the numbers of developed or emerging financial centres and the drug producing countries, it was decided to hold two meetings in the area during 1992-93.

The meeting of the FATF in Sydney in September provided the opportunity to organise a programme in parallel for selected Asian and Pacific states. Representatives from Fiji, Indonesia, Malaysia, Nauru, Papua New Guinea, the Philippines, the Solomon Islands, Tonga and Taiwan attended the sessions at which there were presentations and discussions on the money laundering situation in the region.

This was followed in April 1993 by the Asia Money Laundering Symposium organised jointly by the FATF and the Commonwealth Secretariat, with the support of the UNDCP and hosted by the Government of Singapore. This was a major conference involving participants from 14 non-FATF countries/regions and SEACEN, 9 FATF members (including the 7 FATF sponsors), UNDCP and INTERPOL. The Symposium concentrated on raising awareness of the money laundering problem and explaining countermeasures. Separate detailed sessions were held for financial and regulatory; legal and judicial; and law enforcement groups. A written statement of the conclusions of the Symposium was produced and the non-FATF members were asked to give serious consideration to implementing the 40 FATF Recommendations. The value was recognised of holding a further Symposium in about a year's time.

c) The Caribbean

FATF members have worked closely with the Caribbean Islands and Central American States since 1990 and a Caribbean Financial Action Task Force (CFATF) has been established. The CFATF process has gathered pace in 1992-93 and major progress has been made in promulgating the FATF message in the Caribbean region. With the support of FATF members, a Ministerial Conference of the CFATF was held in Kingston, Jamaica in November 1992. At this meeting the CFATF members formally endorsed and agreed to implement the 40 FATF Recommendations and the 19 Recommendations drawn up at the Aruba Conference in 1990. It was also agreed that there needed to be a mechanism to monitor and encourage progress in this work, including a self-assessment and mutual evaluation process. To further this and to facilitate the provision of training and technical assistance in the region, the meeting proposed the creation of a small CFATF Secretariat to be based in Trinidad and Tobago, which is taking over the Presidency of this body. Another meeting of the CFATF will be held in 1994 to evaluate progress. The FATF sponsoring countries (Canada, France, Netherlands, UK and US) are now discussing arrangements for the ongoing operations of the CFATF.

d) Africa

Working Group III has given continued attention to the mechanisms for pursuing anti-money laundering initiatives in Africa, given the absence of any clearly suitable continental body with whom the FATF can work. In November 1992 members of Group met representatives of the Central African Republic, the Ivory Coast, Kenya, Morocco, Nigeria and Zimbabwe for discussions on the best way forward. The FATF Secretariat is also in contact with selected regional organisations. Proposals for FATF activities in Africa during Round V of the Task Force are being drawn up, taking account of these consultations.

e) Other Areas

In the Middle East the Gulf Co-operation Council has continued to encourage compliance with FATF Recommendations by its six Gulf State members. A conference on money laundering, organised jointly by the FATF, GCC and the Saudi Arabian Monetary Authority, is planned for October 1993.

In South America, as in previous Rounds, the FATF has not pursued any direct contacts, given the well-established initiative of the OAS in this area.

III. Co-ordination and Oversight of Liaison between Relevant Members and their Dependent, Associate or Otherwise Connected Territories.

At its meeting in April 1993 the Group received reports from "sponsor" members on the action taken by these territories in implementing anti-money laundering measures. The conclusion was that progress is being made in a number of areas but the FATF "sponsors" need to continue their efforts to encourage early action.

The Working Group has also begun consideration of how to evaluate progress by these territories. Certain have completed self-assessment questionnaires (and some are also involved in the CFATF process) but there is currently no comprehensive and systematic mechanism.

IV. Co-operation with Regional and International Organisations in Furthering the Objectives of the FATF

During Round IV the FATF has further developed the good relations established with other organisations most closely involved in combating money laundering. Representatives from the Council of Europe, INTERPOL, the UNDCP and CCC have regularly attended meeting of Working Group III and participated in the planning and execution of the various external relations initiatives carried out in 1992-93. FATF members have also taken part in money laundering events organised by these bodies and the Chairman of Working Group III was invited to make a presentation at the November 1992 meeting of the United Nations General Assembly's Third Committee devoted to action against drugs trafficking and money laundering.

The Round has also seen FATF extend the range of organisations with whom it has worked. There was close co-operation with the Commercial Crime Unit of the Commonwealth Secretariat in respect of the Asia Money Laundering Symposium. The FATF has also developed links with the European Bank for Reconstruction and Development regarding anti-money laundering initiatives in Eastern Europe. A representative from the Bank attended the Symposium in Budapest and the Chairman of Working Group III visited the Bank in May for discussions on further co-operative efforts in this area.

With the number of international organisations engaged in anti-money laundering work, particularly in some areas of the world, particularly Eastern Europe, it is clearly important to make best use of the available resources and avoid overlap and duplication of efforts. In conjunction with the other major organisations, FATF through Working Group III is taking steps to institute a co-ordination mechanism, starting with the production of a calendar of all the money laundering initiatives planned by the various bodies.

V. Conclusions

The Group has made substantial progress in its external relations agenda during Round IV. Building on the contacts established in previous Rounds, the Group has continued its mission of promulgating the FATF message. Promoting money laundering awareness remains an important feature of its work but emphasis is placed not only seeking a firm commitment from third countries to implementation of the 40 Recommendations but also an agreement to be evaluated on progress. Clearly results cannot be expected immediately and the FATF is at different stages in its contacts with various regions. However, the CFATF process has shown that, over time, substantive commitments can be achieved. The challenge for future Rounds will be to ensure that there is proper follow-up to the actions already taken whilst finding a way to reach those parts of the world where even awareness of the money laundering problem remains at a very low level.

INTERPRETATIVE NOTE

CONTROLLED DELIVERY OF FUNDS SUSPECTED OR KNOWN TO BE THE PROCEEDS OF CRIME

1. In its third report the FATF called on member governments to consider taking the necessary measures to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of money for the purpose of identifying persons involved in such activities or for evidence gathering. This was with the specific intention of enabling the use of procedures such as controlled delivery and undercover operations. In its fourth round the FATF has carried out further studies on the issue of controlled delivery.

2. Controlled delivery is a technique whereby, when law enforcement agencies become aware of a shipment of, or a transaction involving, items of an illegal or suspected illegal origin, those items are not seized immediately. Instead, law enforcement interests are better served by allowing the shipment/transaction to proceed under the close, covert surveillance of the authorities in order to gather evidence and identify those involved. Arrests and seizures are then made at a later stage as appropriate. Application of controlled delivery techniques to international transportation of illegal drugs has been accepted in law enforcement circles for many years. Provisions for their international use are included in the 1988 Vienna Convention.

3. The FATF considers that controlled delivery is an equally valid technique in money laundering cases involving shipments of or transactions involving funds[3] suspected to be the proceeds of crime, whether at the domestic or international levels. Indeed, it is arguably of greater utility from an evidential standpoint in such cases than in those involving drugs trafficking. In the latter, it is easy to establish if the substances are illegal. However, it may not be readily apparent whether or not particular funds are the proceeds of crime. Further investigations are generally necessary to determine this and controlled delivery is a very effective method in this context. Even where it is clear that funds are of criminal origin, a controlled delivery operation, subject as necessary to the requisite legal authorisation, can be of great value in helping to identify and gather evidence against as many as possible of the criminals involved. In particular, it offers a route to the higher level criminals and the beneficial owners of the funds.

4. Controlled delivery is an important counter-measure against money laundering at the international level. The FATF's work on money laundering methods has indicated that there is an increasing return to cross-border movement of the proceeds of crime, especially those from drugs trafficking. This trend can be expected to continue as the various FATF members (and other countries) implement the FATF Recommendations as regards preventing and detecting the use of their financial systems for the purpose of money laundering. The major money laundering organisations have shown that they are sensitive to national law enforcement initiatives. The enforcement of anti-money laundering measures by countries provides a disincentive for criminals to use their financial systems and instead to move funds generated from crimes in those countries to countries which do not yet have adequate anti-laundering measures and whose financial systems can consequently be penetrated with less risk.

---

[3] The term funds covers not only currency but all types of monetary and financial instruments.

5. Application of controlled delivery techniques to international movements of funds can obviously be of value in obtaining information and evidence concerning particular money laundering operations. At a more strategic level, it can also provide useful intelligence on the international flows of illegal funds, identifying countries whose financial systems are perceived by money launders as particularly vulnerable. In this context, the application of the techniques to suspicious international inter and intra bank bulk cash transactions as well as particular cross-border consignments of cash by money launderers is important. Use of controlled delivery techniques is of particular value in countries or territories which have yet to implement the full range of anti-money laundering measures as, for this reason, they are the most likely targets for illegal currency flows.

6. Clearly there needs to be effective co-operation between law enforcement agencies in the various countries concerned if international controlled deliveries are to be successful. An essential precondition is that countries should permit controlled delivery whether under their general law or specific legal provisions. This is already the case in the majority of FATF members, subject to the law enforcement agencies having any necessary permission from legal/judicial authorities to conduct the operation.

7. The Customs Co-operation Council has endorsed a recommendation that its members be encouraged to use controlled delivery techniques and both it and INTERPOL consider it would be helpful if the FATF were to encourage action by these organisations in this area.

8. In the light of the above considerations and in furtherance of FATF Recommendations 32, 33, 36 and 38 (including the Interpretative Note to this Recommendation), the Interpretative Note on deferred arrests and seizures as well as Article 9 of the Vienna Convention, the FATF has therefore adopted the following Interpretative Note.

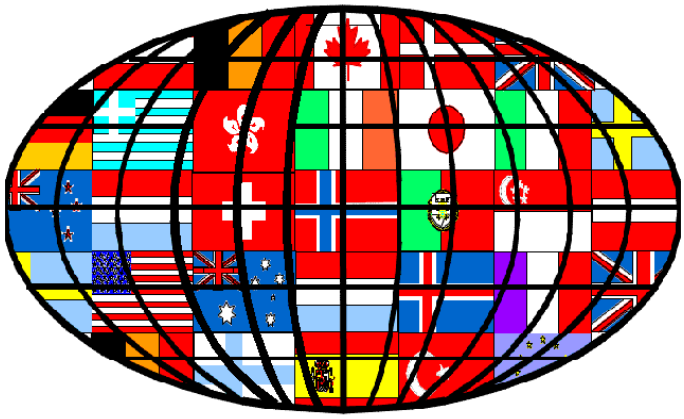
" The controlled delivery of funds known or suspected to be the proceeds of crime is a valid and effective law enforcement technique for obtaining information and evidence in particular on international money laundering operations. It can be of great value in pursuing particular criminal investigations and can also help in obtaining more general intelligence on money laundering activities. The use of these techniques should be strongly encouraged. The appropriate steps should therefore be taken so that no obstacles exist in legal systems preventing the use of controlled delivery techniques, subject to any legal requisites, including judicial authorisation for the conduct of such operations. The FATF welcomes and supports the undertakings by the Customs Co-operation Council and INTERPOL to encourage their members to take all appropriate steps to further the use of these techniques."

Appendix K:

FATF, *Financial Action Task Force on Money Laundering: Annual Report 1997-1998* (Paris: FATF, 1998)

FATF-IX

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING



ANNUAL REPORT 1997-1998

June 1998

TABLE OF CONTENTS

CONCLUSION

ANNEX A - Address by Michel Camdessus, Managing Director of the International Monetary Fund to the Plenary Meeting of the FATF, on 10 February 1998

ANNEX B - Sources of support for the forty Recommendations outside the FATF membership

ANNEX C - 1997-1998 Report on Money Laundering Typologies

ANNEX D - Summary of compliance with the forty Recommendations

ANNEX E - Providing Feedback to Reporting Financial Institutions and Other Persons: Best Practices Guidelines

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

ANNUAL REPORT 1997-1998

SUMMARY

1. Belgium chaired the ninth round of the Financial Action Task Force on Money Laundering (FATF). A major task conducted during the 1997-1998 round by the FATF was the review of its future mission and programme of work from 1999 to 2004. The FATF also continued its work relating to the implementation and refinement of anti-money laundering measures. In addition, the Task Force further developed co-operation with a number of international organisations concerned with the combat of money laundering.

2. On 28 April 1998, FATF Ministers and the European Commissioner for Financial Services endorsed the report prepared by the FATF which defines a five year plan -- 1999-2004 -- to spread the anti-money laundering message to all continents and regions of the globe. To this end, Ministers urged FATF to foster the establishment of a world-wide anti-money laundering network based on adequate expansion of the FATF membership, the development of FATF-style regional bodies such as the Caribbean FATF and the Asia/Pacific Group on Money Laundering, and close co-operation with all the relevant international organisations, in particular the United Nations Office for Drug Control and Crime Prevention (UNODCCP) and the International Financial Institutions. They also agreed that other important tasks of the FATF for the next five years should include improving the implementation of the forty Recommendations within its own membership and strengthening the review of money laundering trends and countermeasures.

3. As in previous rounds, the Task Force devoted a considerable part of its work to the monitoring of members' implementation of the forty Recommendations on the basis of the self-assessment and mutual evaluation procedures. Through an enhanced process, which now includes a question and answer session at a Plenary meeting, the 1997-1998 self-assessment exercise showed that members had continued to make progress in implementing the forty Recommendations. Furthermore, the mutual evaluation procedure, which provides for a thorough examination of the counter-measures in place and their effectiveness, continues to be an irreplaceable monitoring mechanism. Sixteen FATF members have now been examined in the second round of mutual evaluations. Summaries of the eight mutual evaluation examinations (Canada, Switzerland, Germany, the Netherlands, Italy, Japan, Norway and Greece) which were conducted during FATF-IX are contained in Part II of the report.

4. The assessment of current and future money laundering threats, an essential part of the FATF's work, confirmed the trends observed in previous exercises. The annual survey of money laundering typologies [1] clearly noted the emergence of new areas which are not yet fully mapped: electronic money, new payment technologies, remittance businesses, non-financial professions, the insurance sector and stock exchange dealers. The FATF also continued the dialogue which has been opened with the private sector through a second Forum with representatives from the international financial services industry. The event provided an opportunity for representatives from the industry to meet with FATF government delegates and discuss issues of importance such as the need to provide feedback to reporting financial institutions. During the round, experts from FATF members and several international organisations continued the work commenced in 1997 on estimating the magnitude of money laundering.

[1] See Annex C.

5. The FATF's strategy for relations with non-members is directed towards supporting the various activities of other regional and international bodies involved in the fight against money laundering. In this regard, it should be noted that a Select Committee of the Council of Europe and the Offshore Group of Banking Supervisors commenced mutual evaluation programmes of the anti-money laundering measures taken by their members. While the Caribbean FATF pursued its anti-money laundering activities, notably its mutual evaluation programme and typologies exercise, a major event during 1997-1998 was the first meeting of the Asia/Pacific Group on Money Laundering, which was held in March 1998 and which was attended by 23 countries and territories throughout the region. Finally, in September 1997, the FATF carried out a mission to Cyprus and in October 1997, it organised, with the Bank of Russia, an international money laundering Conference in St. Petersburg.

6. The necessary development of in-depth international co-operation in combating money laundering was clearly demonstrated at the highest level when Mr. Michel Camdessus, Managing Director of the International Monetary Fund[2], and Mr. Pino Arlacchi, Executive Director of the United Nations Office for Drug Control and Crime Prevention, addressed the February 1998 FATF Plenary meeting. To meet the request for technical assistance from its member States, particularly in fulfilling their obligations to counter money laundering deriving from the 1988 Vienna Convention, the United Nations launched, in 1997, their Global Programme against Money Laundering. Furthermore, the 1998 June Special Session of the United Nations General Assembly provided an opportunity for governments to renew their commitment to combat the drug problem, including the countering of money laundering. In 1997-1998, the UNODCCP and the FATF co-operated in several anti-money laundering meetings. The Task Force also initiated contacts with the regional development banks, particularly the Inter-American Development Bank.

7. According to the objectives decided in the review of the FATF's future, the issue of enlarging FATF membership will need to be addressed in 1998-1999. This critical task will be carried out under the Presidency of Japan, which will commence on 1 July 1998.

[2] See Annex A.

INTRODUCTION

8. The Financial Action Task Force was established by the G-7 Summit in Paris in 1989 to examine measures to combat money laundering. In 1990, the FATF issued forty Recommendations for action against this phenomenon. These were revised in 1996 to reflect changes in money laundering trends. Membership of the FATF comprises twenty six governments[3] and two regional organisations[4], representing major financial centres of North America, Europe and Asia. The delegations of the Task Force's members are drawn from a wide range of disciplines, including experts from the ministries of finance, justice, interior and external affairs, financial regulatory authorities and law enforcement agencies.

9. In July 1997, Belgium succeeded Italy in holding the Presidency of the Task Force for its ninth round of work. Three Plenary meetings were held in 1997-1998, two at the headquarters of the OECD in Paris and one in Brussels. Two special experts' meetings were held; the first in November 1997 in Paris to consider trends and developments in money laundering methods and counter-measures and the second in May 1998 to work on the issue of estimating the size of money laundering. In addition, a meeting of the FATF Ministers was held in the margins of the OECD Council meeting at Ministerial level on 28 April 1998.

10. The FATF co-operates closely with international and regional organisations concerned with combating money laundering. Representatives from the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Council of Europe, the Commonwealth Secretariat, the European Bank for Reconstruction and Development, the International Monetary Fund (IMF), the Inter-American Development Bank (IDB), the Inter-American Drug Abuse Control Commission (CICAD), Interpol, the International Organisation of Securities Commissions (IOSCO), the Offshore Group of Banking Supervisors (OGBS), the United Nations Office for Drug Control and Crime Prevention (UNODCCP), the World Bank and the World Customs Organisation (WCO) attended various FATF meetings during the year.

11. A major element of the deliberations of the Task Force during 1997-1998 was the review of its future mission. Part I of the report sets out the conclusions of this review, which were endorsed by all FATF member governments. Parts II, III and IV of the report outline the progress made over the past twelve months in the following three areas:

- monitoring the implementation of anti-money laundering measures by its members;
- reviewing money laundering methods and countermeasures; and
- promoting the widest possible international action against money laundering.

---

[3] Australia; Austria; Belgium; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong, China; Iceland; Ireland; Italy; Japan; Luxembourg; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the United Kingdom and the United States.

[4] European Commission and Gulf Cooperation Council.

I. THE FUTURE MISSION OF THE FINANCIAL ACTION TASK FORCE

12. In 1994, five years after the FATF was established by the 1989 G-7 Summit, its members decided that the Task Force -- which is not a permanent international organisation -- should continue its work for a further five years, i.e. until 1999. It was also agreed that no final decision on the future of FATF should be taken until 1997-1998, at which time it would be necessary to consider how the fight against money laundering could best be carried forward. Therefore, an in-depth review of the FATF's needs, mission and work programme, which is summarised in the paragraphs below, was carried out during FATF-IX.

A. PROGRESS ACHIEVED

13. The FATF issued in 1990 and revised in 1996, forty Recommendations which cover legal, financial regulatory, law enforcement and international action which governments should take to combat money laundering. The FATF's forty Recommendations have become an internationally accepted benchmark in this area.[5] Since 1991, the FATF has concentrated on the following three main tasks: establishing standards and reviewing money laundering methods; monitoring the implementation of anti-money laundering measures by member governments; and promoting the adoption of counter measures by non-member countries.

14. Considerable progress has been made in the implementation of anti-money laundering measures by FATF members. By mid-1999, every member will have undergone two evaluations of their anti-money laundering systems. The first round of evaluations dealt with the question of whether all members had adequately implemented the forty Recommendations, while the second round deals with the effectiveness of the anti-money laundering system in each member. The FATF has also conducted an ambitious programme of missions and seminars in non-member countries to promote awareness of the money laundering problem and to encourage them to take action. While the FATF's forty Recommendations have gained some international prominence, a large number of countries around the world still need to implement anti-money laundering systems.

15. There is no doubt that the FATF has played a key role over the last eight years in building an international consensus on the measures that need to be taken to combat money laundering. It has also helped to persuade many countries to implement these measures. In this process, it has helped to create a "network" of money laundering experts in each of the FATF members, improving co-operation and the flow of information, both at the domestic level and internationally. Moreover, the FATF has achieved this with very limited permanent resources.

B. FUTURE MISSION AND PROGRAMME OF WORK

(i) The need for continued action against money laundering and the major tasks to be accomplished

16. Although considerable progress has been made in the fight against money laundering since 1989, much remains to be done and there is an obvious need for continued mobilisation at the international level to deepen and widen anti-money laundering action. The major tasks are described hereafter.

(a) To establish a world-wide anti-money laundering network and to spread the FATF's message to all continents and regions of the globe

---

[5] See Annex B.

17. The FATF has decided to foster the establishment of a world-wide anti-money laundering network based on :

- an adequate expansion of the FATF membership to strategically important countries which already have certain key anti-money laundering measures in place (criminalisation of money laundering; mandatory customer identification and suspicious/unusual transactions reporting by financial institutions), and which are politically determined to make a full commitment towards the implementation of the forty Recommendations, and which could play a major role in their regions in the process of combating money laundering;

- the development of FATF-style regional bodies, especially in areas where FATF is not sufficiently represented and strengthening of work of bodies which already exist (the CFATF, the Asia/Pacific Group on Money Laundering, the Council of Europe, the OAS/CICAD and the OGBS); and

- close co-operation with relevant international organisations, in particular the United Nations bodies and the International Financial Institutions.

(b) Improve the implementation of the forty Recommendations in FATF members

18. Improving the implementation of the forty Recommendations in FATF members is an important and challenging policy objective to be pursued. There is a need to ensure that all members have implemented the revised forty Recommendations in their entirety and in an effective manner. It was therefore agreed to review the existing monitoring mechanisms so as to establish a renewed assessment process, focusing on compliance with the 1996 Recommendations, and involving the following elements:

- en enhanced self-assessment process; and

- a third round of simplified mutual evaluations for all FATF members starting in 2001, focusing exclusively on compliance with the revised parts of the Recommendations, the areas of significant deficiencies identified in the second round and generally the effectiveness of the counter-measures.

(c) Strengthen the review of money laundering trends and countermeasures

19. Money laundering is an evolving activity, the trends of which should continue to be monitored. It is therefore crucial for FATF members to acquire the best possible experience and knowledge of money laundering trends and techniques and to assess the effectiveness of the FATF Recommendations. There is also a need to extend the geographical scope of the future typologies exercises. The latter may raise the issue of the need for new countermeasures. If this occurs, the FATF must be at the forefront of the elaboration of these new countermeasures. In order to achieve a set of Recommendations to counter actual money laundering threats, the FATF could embark, if necessary, on a further updating exercise in 2003/2004, covering new countermeasures as well as perhaps reviewing those Recommendations which currently ask members simply to consider and decide whether action should be mandatory or not, incorporating the input from FATF-style regional bodies. In any case, FATF must ensure that the forty Recommendations remain the most effective and widely-respected international standard in the anti-money laundering area.

(ii) Future Direction, Duration and Objectives of the FATF

20. Action to combat money laundering must rely on effective co-operation between experts from a wide range of disciplines: legal and judicial, financial and regulatory, and law enforcement. The success of the FATF's work so far demonstrates that there is no alternative international organisation, body or

group, which has the necessary expertise, i.e. of a multidisciplinary nature with the experience and ability to assume responsibility of the FATF in a flexible and efficient way.

21. The medium to long term objectives of the FATF are: the development of credible and effective FATF-style regional bodies and an adequate expansion of its membership to include strategically important new members. At the beginning of 2005, the FATF should ideally have achieved its objective of promoting the establishment of a world-wide anti-money laundering network. In any case, an assessment of the FATF's achievements and strategy between 1999 and 2004, and future should be carried out in 2003-2004.

C. POLITICAL SUPPORTS TO THE FATF'S FUTURE MISSION

22. A Ministerial meeting of the FATF, held on 28 April 1998 in the margins of the OECD Council meeting at Ministerial level, fully endorsed the conclusions of the review of the future of the Task Force and the continuation of its work until 2004. The Ministers stressed that the major focus of FATF's future work should be to promote the establishment of a world-wide anti-money laundering network encompassing all continents and regions of the globe. They particularly supported the intention to bring into the FATF some additional strategically important countries which are committed to the combat of money laundering and to foster the development of further regional anti-money laundering bodies, in addition to the Caribbean FATF and the Asia Pacific Group on money laundering.

23. Further expressions of support towards the FATF's future mission were made at political level. In their April 1998 Communiqué, the Ministers of the OECD "welcomed the decision of the FATF Ministerial meeting to extend its work for a further five years and the new strategy it has adopted" and also noted the "FATF decision to promote the establishment of a world-wide anti-money laundering network based on adequate expansion of membership".

24. On 8 May 1998, the G-7 Finance Ministers "commended the work that FATF has carried out since its creation to develop and promote action against money laundering" and endorsed the decision of the FATF to continue its mandate for a further five years and the new strategy it has adopted". The G-7 Finance Ministers also called on the FATF to make recommendations on what can be done to rectify the abuses raised by a "number of countries and territories, including some financial offshore centres, which continue to offer excessive banking secrecy and allow screen companies to be used for illegal purposes".

25. Finally, on 17 May 1998, the G-8 Heads of State and Government "welcomed the FATF decision to continue and enlarge its work to combat money laundering in partnership with regional groupings" and "placed special emphasis on the issues of money laundering and financial crime, including issues raised by offshore financial centres".

II. MONITORING THE IMPLEMENTATION OF ANTI-MONEY LAUNDERING MEASURES

26. A considerable part of FATF's work focuses on monitoring the implementation by its members of the forty Recommendations. FATF members are clearly committed to the discipline of multilateral surveillance and peer review. All members have their implementation of the Recommendations monitored through a two-pronged approach:

- an annual self-assessment exercise; and,

- the more detailed mutual evaluation process under which each member is subject to an on-site examination.

A. 1997/1998 SELF-ASSESSMENT EXERCISE

(i) Process

27. In this exercise, each member is asked to provide information concerning the status of their implementation of the forty Recommendations. This information is then compiled and analysed, and provides the basis for assessing to what extent the forty Recommendations have been implemented by both individual countries and the group as a whole.

(ii) State of implementation[6]

(a) Legal issues

28. The overall state of implementation is very similar to the situation recorded in the previous round, which reflects that almost all members are in compliance with a large majority of the Recommendations, though there are still a few areas of weakness. It is satisfying to note that the Vienna Convention has now been ratified and implemented by twenty-three members, and that the remaining three members will soon be in a position of full compliance.

29. In regard to most Recommendations the position is quite satisfactory. All members have enacted laws to make drug money laundering a criminal offence, and all but three members have enacted an offence which covers the laundering of the proceeds of range of crimes in addition to drug trafficking. The overall level of compliance will improve considerably when Japan, Luxembourg and Singapore have extended their drug money laundering offences to serious crimes. In Luxembourg, a Bill extending money laundering offences beyond drug trafficking is about to be enacted. In Japan, a Bill of a similar type has been submitted to the Diet. Singapore expects to put in place laws to criminalise serious crimes money laundering before the end of 1998.

30. A number of members also still need to take measures in relation to confiscation and provisional measures, both domestically and pursuant to mutual legal assistance. In relation to domestic confiscation, nineteen members are in full compliance, with six in partial compliance, whilst for mutual legal assistance in this area, there are seventeen members in full compliance, five partially comply, and three are out of compliance (Canada, Greece and the United States). These figures reflect only a marginal increase in compliance over the past few years, and despite the attention paid by FATF to this issue, there needs to be urgent action by some members to bring themselves into compliance with the relevant Recommendations.

(b) Financial issues

31. The 1997-1998 self-assessment exercise generally showed a slight improvement in the overall implementation of the FATF Recommendations on financial issues. Significant improvements were recorded in relation to two new recommendations that were introduced in 1996, namely Recommendation 13 dealing with the need to pay attention to new technologies, and Recommendation 25 dealing with shell corporations. However, differences still remain in the relative state of implementation between the banking sector and the non-bank financial institution sector. On an individual country basis, Finland and Switzerland made significant progress following the enactment of new legislation.

---

[6] A copy of the summary of compliance with the legal and financial recommendations is at Annex D.

32. Almost all members comply fully with customer identification and record-keeping requirements for banks, but there are some persistent gaps in coverage with respect to certain categories of non-bank financial institutions. However, as mentioned in the mutual evaluation section of this report, the serious concerns regarding the anonymous passbooks for residents in Austria have not been resolved, and are being pursued through the FATF non-compliance procedures.

33. In relation to the requirement for financial institutions to report suspicious transactions and related measures, the position is generally very satisfactory in relation to banks and almost as good for non-bank financial institutions. However there is still room for improvement with respect to non-bank financial institutions and the need to pay attention to large, unusual transactions and the obligation to develop internal controls. For banks, almost all members have now established anti-money laundering guidelines and taken steps to guard banks against control or acquisition by criminals, and though there were improvements, a number of countries still have to take similar measures for all categories of non-bank financial institutions. Canada and Iceland need to take urgent measures to bring themselves into full compliance with respect to various categories of non-bank financial institutions, and additional measures also need to be taken in the banking sector. In the United States, there is also a pressing need to finalise and implement the proposed regulations to significantly enhance anti-money laundering controls over many categories of non-bank financial institutions, particularly bureaux de change, money remitters, check cashers, issuers and sellers of money orders and travellers cheques, casinos and securities brokers and dealers. The United States is also urged to place additional money laundering controls on insurance companies.

(iii) Summary of performance

34. The overall conclusion from the 1997-1998 self-assessment exercise is that a large majority of members have reached an acceptable level of compliance with the 1996 forty Recommendations, and notable progress was made during the year by some members. However, as mentioned above, a number of members still need to take steps to widen their money laundering offence, or to implement a fuller range of anti-money laundering measures in the financial sector. It is important that these changes be brought in as soon as possible.

(iv) Gulf Cooperation Council

35. In May 1997, the GCC agreed to carry out, in conjunction with the FATF, an evaluation of the anti-money laundering measures that had been taken by its six member States - Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (U.A.E), and as a first step self-assessment questionnaires were sent in August 1997. However, due to partial and incomplete replies from some GCC members, the FATF is currently unable to determine the level of compliance with the forty Recommendations. It was therefore agreed that a high level mission will meet with the relevant officials in the Secretariat General of the GCC and the U.A.E. in order to obtain more information on the implementation of the forty Recommendations in the GCC member States and to discuss how to improve the implementation of effective anti-money laundering systems in the Gulf region.

B. MUTUAL EVALUATIONS

(i) Objective and process of the second round of mutual evaluations

36. The second and major element for monitoring the implementation of the FATF Recommendations is the mutual evaluation process. Each member is examined in turn by the FATF on the basis of a report drawn up by a team of three or four selected experts drawn from the legal, financial and law enforcement fields of other members. The purpose of this exercise is to provide a comprehensive and objective assessment of the extent to which the country in question has moved forward in implementing effective measures to counter money laundering and to highlight areas in which further progress may still be required.

(ii) Summaries of reports

Canada

37. The largest source of criminal proceeds laundered in Canada comes from narcotics trafficking (approximately 70%), however numerous other types of profitable criminal activities exist such as tobacco and alcohol smuggling, illegal gambling, smuggling and white collar crimes such as fraud, counterfeiting and computer/ telecommunications crimes. Money laundering mechanisms in Canada involve the use of a wide range of techniques and methods in many different parts of the financial and non-financial sectors. Money laundering has occurred through deposit taking institutions, currency exchanges, the securities industry, real estate, incorporation and operation of shell companies, dealings in gold and precious metals, the insurance industry, gambling facilities (lotteries and casinos), automobile and boat dealerships, professionals (lawyers and accountants), and cross border movement of illicit proceeds. The pattern of money laundering has changed in recent years, with a movement from bank to near-banks/currency exchanges by money launderers, whilst an important external factor is the location of Canada next to the United States.

38. Canada's money laundering control scheme is based on a strong penal response through the prosecution of money launderers and the confiscation of the proceeds of crime. There have been a limited number of significant direct changes made to the anti-money laundering regime since the first evaluation, though some amendments have indirectly strengthened the regime. The most significant legislative changes were measures contained in organised crime legislation enacted in May 1997 which widen the money laundering offences, and introduce a power to freeze and confiscate the instrumentalities of organised crime offences. Other amendments improved several aspects of the forfeiture legislation, and give the police extra powers with respect to "sting" and controlled delivery operations. Another significant measure was the creation of 13 new Integrated Proceeds of Crime (IPOC) units to combat money laundering and organised crime. In the financial sector, the Office of the Superintendent of Financial Institutions published new anti-money laundering guidelines in 1996.

39. The penal legislation appears to be working well, though the extension of the more serious money laundering offence to all serious crimes, together with some minor changes to the forfeiture legislation, would make the system even more effective. Canada must be strongly commended for the willingness to apply significant resources into tackling the problem of proceeds of crime - a measure which will undoubtedly result in many more prosecutions and forfeited proceeds. Considerable efforts have also been made in relation to international co-operation and the only major weakness is the inability to effectively and efficiently respond to requests for assistance in relation to restraint and forfeiture. The use of domestic money laundering proceedings to seize, restrain and forfeit the proceeds of offences committed in other countries is recognised as sometimes ineffective, and legislation to allow Canada to enforce foreign forfeiture requests directly should be introduced.

40. In the law enforcement area the suspicious transaction reporting regime does not appear to be working effectively, and there needs to be an urgent resolution of the internal review process which has been continuing since 1993. The examiners consider that the most essential improvements are to create a new regime, consistent with the Charter of Rights and Freedoms, which makes reporting mandatory, and to create a new financial intelligence unit which would deal with the collection, management, analysis and dissemination of suspicious transaction reports and other relevant intelligence data. Other measures which would assist are detailed guidance on what transactions may be suspicious, a penal or administrative sanction for failing to report, and improved general and specific feedback. In addition, detailed proposals need to be created and taken forward for a system of cross border reporting and ancillary powers for Customs officers. The adoption of these measures, when combined with the new IPOC units, should lead to a much more effective system.

41. Changes are also required in the financial sector, where the mixture of federal, provincial and self regulation, the lack of uniformity and the combination of requirements laid down by law and also by guidelines, makes the system complex. The limited customer identification obligations in relation to corporations and beneficial owners of accounts is not in conformity with Recommendation 11, and additional measures should be enacted to remove this discrepancy. The legislation should also be extended to cover other types of non-bank financial institution such as money remitters and check cashers, as well as non-financial businesses such as casinos. The threat posed by professional facilitators of money laundering should also be examined. The regulations and systems for compliance review, internal controls, education and training for the different parts of the non-bank financial sector need to be more comprehensive and uniform, and there needs to be greater co-ordination and support by government agencies.

42. The Canadian anti-money laundering system as a whole is substantially in compliance with the almost all of the 1990 FATF forty Recommendations. In those areas where it has been proactive such as prosecutions, forfeiture, and general international assistance it has achieved considerable success. It now needs to expeditiously extend this proactive response, and resolve the deficiencies identified above. By doing so it will create a law enforcement and regulatory system which should combat money laundering most effectively.

Switzerland

43. Switzerland's central geographical location, its relative political, social and monetary stability, the current context of liberalisation and the professional secrecy that characterises the country's financial system are attractive to all investors, whether the origin of their funds is legal or illegal. In addition, advanced technology and a great diversity of institutions in the financial centre expose Switzerland to being used in international money laundering schemes. In this context, Switzerland is used primarily, but not exclusively, at the "layering" stage of the money laundering process.

44. There are three main facets to Swiss anti-laundering policy: a very broad definition of laundering offences involving assets derived from any crime; a system of self-regulation in the financial sector (banking and non-banking) accompanied by State monitoring; a "reporting right", which since 1994 has authorised financial intermediaries to convey their suspicions and which was replaced on 1 April 1998 with a "reporting obligation".

45. For some years, the Swiss authorities have been endeavouring to toughen the penal law in order to step up the fight against new forms of crime, particularly economic offences and organised crime. As a result, on 1 August 1990, Articles 305 *bis* and 305 *ter* of the Penal Code), on the offences of money laundering and lack of due vigilance in financial transactions respectively, entered into force. This arsenal of criminal law was supplemented on 1 August 1994 by a second round of measures against organised crime which strengthened powers of confiscation and authorised financial intermediaries to report suspicious transactions (CP: Article 305 *ter*, paragraph 2). In addition, the Federal Act of 7 October 1994

on the Central Offices of the Federal Criminal Police set up an organisation vital to improved prosecution of persons involved in organised crime.

46. In the financial sector, the Federal Banking Commission (CFB) issued a circular of 18 December 1991 to all licensed banks and auditing firms containing guidelines for preventing and combating money laundering. Concerning the obligation to identify, CFB circular 91/3 mirrors the Agreement on the Banks' Obligation of Diligence (CDB).

47. A Law on counter-laundering in the financial sector ("the Money Laundering Act", or LBA) was adopted by the Parliament on 10 October 1997. Under this legislation, all physical and legal persons active in the financial sector would be subject to special obligations of diligence (to ascertain the identity of customers and beneficial owners, to clarify certain transactions and to establish and keep certain documents). These persons must also take organisational measures to prevent money laundering. The LBA calls for the creation of a Money Laundering Control Authority responsible for monitoring the compliance of financial intermediaries with anti-laundering obligations. Intermediaries will also be required to file reports with the Money Laundering Reporting Office and to freeze suspicious assets if they have reason to suspect that money is being laundered. The Act entered into force on 1 April 1998.

48. Although the penal aspect of the Swiss system has been significantly improved, prevention for the non-banking sector should be in accord with FATF Recommendations with the entry into force of the LBA. In order to comply with the new Recommendation 15, the LBA introduces a reporting obligation. However, as this obligation only exists when business relations are established, compliance with this Recommendation would not be fully met if a restrictive interpretation should be made of it. Before the entry into force of the LBA, Switzerland did not comply with Recommendation 17. The LBA introduces a prohibition to inform the customer during the period of freezing established by Article 10, this prohibition will be generally relayed by a decision of the penal cantonal authorities which are competent to decide during the entire investigation. In general, the current proposals to remedy shortcomings pointed out in the first evaluation are significant, but their application is too slow.

49. Switzerland is nevertheless to be congratulated on the LBA definition of professionals subject to its anti-money laundering obligations, which spans the entire financial sector, including financial activities carried on professionally by lawyers. However, assessment of compliance with the new obligations of vigilance by non-banking professions will have to await implementation of the LBA, even though Article 305 ter already imposed an obligation of vigilance in financial transactions.

50. At this stage, it is impossible to assess the effectiveness of the system for reporting suspicions, given the lack of appropriate statistics. The LBA will contribute to an appreciable improvement in this system with the introduction of an obligation to declare suspicions of which the incomplete nature of the obligation, due to the fact that the latter arises only at the establishment of business relations, should be noted as well as the restrictive interpretation of it by financial institutions. The Swiss financial sector rather tends to protect itself against money launderers by being scrupulous in entering into business relations and hence gives preference to refusal to enter business relations with suspect customers. Although the LBA is intended to change this state of affairs, the role of the supervisory authorities, including the CFB, the Money Laundering Control Authority as well as the Reporting Office in particular, will be vital in convincing the entire financial sector of the need actively to participate in preventing money laundering. As regards the non-banking sector the Money Laundering Control Authority, as empowered by the LBA, has to act effectively, particularly in sectors at present not covered such as money changers.

51. In legal terms, the provisions on seizure and confiscation and on offences under the Criminal Code which largely reflect Recommendation 4, are to be welcomed. The absence of real prosecution powers at federal level is an obstacle to effective prosecution. Giving power to the public prosecutor of the Confederation as is at present being considered, is a first step, but does not seem to go far enough.

Real progress would be made by giving the Confederation -- as proposed in the draft overall revision of the Constitution -- power to legislate on criminal procedure.

Netherlands

52. The major sources of illegal proceeds in the Netherlands are believed to be fraud and drug trafficking. The patterns of money-laundering have changed as a result of the enactment of the anti-money laundering legislation and the growing awareness by financial and non-financial institutions of the phenomenon of money-laundering. The carriage of cash across borders with neighbouring countries has increased, as has the use of money transfer businesses. Whilst the number of bureaux de change has decreased significantly, other areas of money laundering concern remain. One issue is the inflow of money from some countries of the former Soviet Union and Eastern Europe, the origin of which cannot be checked, whilst another is the operation by representative offices of certain foreign banks of "collection accounts" to send money on behalf of their nationals back to the country of origin.

53. The principal aims of the Dutch anti-money laundering system are to protect and maintain the integrity of the financial system, and to detect and prosecute activities concerning money laundering. The heart of the system is the mandatory reporting of unusual transactions on the basis of objective and subjective indicators. The investigation and prosecution of financial crime is a priority for the government, as is the exchange of information and co-operation, both nationally and internationally. Since the first evaluation, some of the more significant changes have been the enactment of the Identification (Financial Services) Act (the Identification Act) and the Disclosure of Unusual Transactions Act (the Disclosure Act); the licensing and supervision of bureaux de change; and the expansion of the reporting obligation to credit card companies, bureaux de change and casinos.

54. The anti-money laundering system in the Netherlands is comprehensive and progressive, and is subject to a continuous process of review and improvement. The government has responded positively to many of the suggestions for improvement in the first mutual evaluation report, and the result is a system which meets, and in many areas goes beyond, the forty Recommendations. The solid legislative basis has been complemented by an active system of supervision, co-operation, education and training in the financial sector. All relevant parts of government, supervisors and the private sector are involved in the fight against money laundering, and the general approach is one of professionalism and commitment by all agencies concerned. Despite this, there are some areas for improvement.

55. The penal offence has a broad scope as it covers all predicate offences, and the mens rea extends to reasonable suspicion. The legislation will be strengthened though if money laundering is made an offence separate from receiving, and the position regarding the elements that need to be proved in relation to foreign predicate offences is clarified. The confiscation system also appears to have a solid legal foundation, though it is unclear from the statistics how well the system is working. However, it is most important that a solution be quickly found to the problems caused in the "Bucro" case, which prevents the seizure and confiscation of assets held in the name of a third party legal entities, even if they are derived from criminal activity. These issues are currently being examined.

56. Measures taken in the financial sector regarding such matters as customer identification and the supervision of institutions such as bureaux de change provide a model that could be followed in other countries. Through the government committees and working groups, the major financial institutions and their associations have shown a high level of commitment, and these result in strong interaction between the government and the private sector, and a constant examination and review of potential sources of weakness. The system of reporting unusual transactions to the financial intelligence unit (MOT), which then reports the suspicious transactions to law enforcement appears to be working effectively in most respects. However there are some potential risks which need to be addressed - in particular there needs to be an increased emphasis on non-cash money laundering and continued attention needs to be paid to the lack of reports from the securities and insurance sectors. The extension of the reporting system to

professionals such as lawyers, notaries and accountants should be seriously examined, and minor refinements could be made in relation to feedback and the exemptions available to reporting institutions.

57. The Netherlands is party to a wide range of international instruments which allow it to provide and make requests for all types of assistance. This would be further strengthened if the requirement of a treaty or agreement was removed. Administrative co-operation between MOT and other similar bodies needs to be further improved through entering more agreements (memoranda of understanding) for the exchange of information at an international level.

58. Overall, the legal and administrative structure for the anti-money laundering system appears to be an effective one, with strong efforts made to promote and co-ordinate anti-money laundering activities in many parts of government and the financial sector. The results in several areas are not apparent because of the lack of statistics, and this makes it difficult to judge the true effectiveness of the system. However the basic structure is a strong one, and combined with the firm commitment at all levels and the resolution of the deficiencies identified above, this will result in a very strong anti-money laundering system.

Germany

59. The major sources of illegal proceeds in Germany are believed to be from drug trafficking, property offences, and the smuggling of alcohol and cigarettes. Other crimes which generate significant profits for organised crime include subsidy fraud against the European Union, counterfeiting, illegal arms sales, extortion, prostitution and investment fraud. The amount of international criminal activity and the profits generated from crime have increased considerably since the last evaluation. It appears that criminals have increasingly resorted to areas where no safeguards have been taken or where regulatory bodies do or did not exist, such as bureaux de change, money remittance and cross border transportation of cash etc. A large amount of money is transferred to Germany from Eastern Europe and the C.I.S states, often through cash importation, but the source of that money is unknown in most cases. Other money laundering techniques and trends which have been observed include the purchase of luxury goods, and the increasing use of so-called collective accounts of foreign credit institutions or the representative offices of such.

60. A twofold approach has been adopted to counter money laundering. Measures within the financial sector are intended to have a preventive effect, while criminal provisions such as the money laundering offence and confiscation laws will punish the offender for the criminal activity as well as depriving him of any illegal benefits. Since the first evaluation, the most significant changes have been the extension of the list of predicate offences for money laundering to include less serious offences committed on a commercial and gang basis, and an amendment to the Banking Act which made bureaux de change, money transmitter agencies, brokers, and other companies offering financial services subject to banking supervision. Legislation is also pending which will, inter alia, extend the list of predicate offences for money laundering and criminalise money laundering activity by the predicate offender; facilitate the provisional seizure of suspicious amounts of money; raise the threshold for customer identification in occasional transactions over DM 30,000 (US$ 16,700); and increase the involvement of the tax authorities in combating money laundering.

61. In most respects the legal framework for the German anti-money laundering system is comprehensive and strong, and in compliance with the forty Recommendations. Certain deficiencies were identified by the German authorities and this has led to amendments which have either been brought into force or are proposed, and all these measures will substantially strengthen the system. The penal legislation in relation to money laundering and the seizure and forfeiture of criminal proceeds is basically sound and comprehensive, and though the number of convictions obtained for money laundering is disappointing, there is a significant commitment to pursuing this offence. The offence will be strengthened by making the predicate offender liable for laundering his own proceeds. The confiscation legislation provides for a wide

range of measures, but the available statistics indicate that the amount of money confiscated is quite small, and this suggests that there is a significant problem of implementation. The amendments to deal with the claims of victims and the issue of "urgent suspicion" will help to make the system more effective, but consideration should also be given as to how the concept of extended forfeiture can be used more effectively within the limits of court decisions. There would also be benefit if the concept of units dedicated to the proceeds of crime and money laundering issues were introduced.

62. Law enforcement powers and resources in relation to money laundering are sufficient, and bilateral co-ordination and co-operation appears to work reasonably well. However, as stated in the first mutual evaluation report, there is an urgent need to implement a more efficient and effective structure to centralise the STR reporting procedure. The establishment of a central reception point or financial intelligence unit would be the most effective option, and an extension of the joint financial investigation group concept which is currently operating may be a solution. If this is not realistic within the political context, then a minimum requirement must be the creation of a central data-base accessible to all law enforcement agencies. Given that steps have already been taken by the ZKA to develop a system, this project should be completed and implemented as soon as possible, and should be supplemented by ensuring that all relevant law enforcement agencies have access to the databases maintained by the Länder.

63. The results of the suspicious transaction reporting system show that the number of cases generated from STRs has remained fairly static and that the vast majority of reports come from banks, with insurance companies also contributing a significant number. The system could be improved through efforts to resolve weaknesses such as the comparatively modest number of reports, the over-emphasis on cash transactions, and the lack of reports from outside the banking and insurance sectors. The quality of STR reporting would also improve if there was increased feedback to financial institutions.

64. Measures in the financial sector are characterised by extensive obligations and a comprehensive framework in certain parts of the financial system, but with distinct areas of weakness and inconsistency in other parts. The extensive and thorough guidelines, the innovative training and education process, active supervision of banks and insurance companies' anti-money laundering compliance, and the commitment of such institutions are most commendable and provide an example for other jurisdictions. However, the extensive obligations in the Money Laundering Act (the Act) impose some unnecessary burdens. The increase of the threshold for customer identification in relation to large cash transactions to DM 30,000 is helpful, but should be accompanied by measures to eliminate the requirements to identify customers making cash withdrawals. The use of s.154 of the Fiscal Code for customer identification when opening an account creates several weaknesses, and the legislation would be strengthened if this obligation was set out in the Act. One matter of concern is the lack of specific sanctions for: (a) failing to comply with the obligation under s.154, (b) breach of the FBSO and FISO guidelines, and (c) non-compliance with the requirements laid down in ss.6, 11 & 14 of the Act (suspicious transaction identification, STRs and safeguards). All these requirements should be made subject to sanctions such as administrative proceedings and a possible fine. Stricter supervision of NBFI, and particularly casinos, which are supervised by Land authorities is needed, though the situation should improve with the transfer of supervisory responsibilities to the FBSO.

65. The framework for mutual legal assistance is fundamentally very sound, and with a few minor modifications would be an exemplary system. Co-operation at an administrative level is made more complex by the federal system, fragmented nature of the law enforcement response to money laundering, and the lack of any centralised database for all STR. Co-operation with police and Customs authorities in other countries appears to be working well, but the inability to directly exchange information with so-called administrative FIUs is a weakness. Consideration should be given to entering into agreements or understandings which would give law enforcement agencies which have access to all STR the ability to co-operate directly with such bodies, provided they observe similar obligations of secrecy as exist in Germany.

Italy

66. The main sources of illegal proceeds in Italy are derived from fraud, corruption, international drug trafficking, extortion as well as organised crime. The structure of the organised crime, based on associations (clans, families) which control drug trafficking, smuggling, etc., means that a large part of the illicit proceeds is channelled into domestic financial and/or commercial circuits. This implies that these organisations ("cosa nostra", "ndrangheta", "camorra", "sacra corona unita"), exercise a firm control on the territory where they are located as well as on local business activities. In some recent cases, it has been noticed that organised crime (especially "cosa nostra") has been engaging in increasingly sophisticated money laundering activities, with the help of highly skilled external consultants or independent organisations. The internationalisation of the Italian criminal organisations means that funds are transferred to less regulated countries, thus reducing the chances of being detected. However, this does not rule out an interest by organised crime in local investments including financial ones.

67. Law no. 197 of July 1991 instituted measures to curtail the use of cash and bearer instruments in financial transactions and to prevent the criminal use of the financial system for money laundering purposes. Its key provision is the prohibition of transfers of cash and bearer instruments in amounts greater than L 20 million (about US$ 12,000), except when such transfers are carried out by means of authorised intermediaries which are required to identify customers and register transactions. Other main provisions deal with the reporting of suspicious transactions and the monitoring of financial intermediaries' compliance with the law.

68. The provisions establishing money laundering as an offence were amended in 1993, to widen the original scope of predicate offences to "all intentional criminal offences". Recently, a Legislative Decree (no. 153/97 of 26 May 1997) amended the laws in force by three important measures: firstly, so as to enhance compliance with the obligation to report suspicious transactions, ensuring that the identity of any person reporting such information be kept absolutely confidential; secondly, the centralisation of the reporting of suspicious transactions to the Ufficio Italiano dei Cambi (UIC) a public institution chaired by the Governor of the Bank of Italy and thirdly, operational links were established for money laundering between financial, investigative and judicial authorities as far as organised crime is concerned. In the near future, the Government is planning to extend the scope of specific categories of non-financial businesses to anti-money laundering measures. Moreover, a review of the anti-money laundering legislation has already started in order to strengthen it by introducing new provisions or eliminating redundancies.

69. The Italian Government has made significant progress in combating money laundering since its last mutual evaluation in 1993. The changes it has effected are for the most part quite recent and derive from the latest anti-money laundering legislation, Legislative Decree no. 153/97. The most significant change provided for in the Decree is the designation of a single recipient for suspicious transaction reports, namely, the Ufficio Italiano dei Cambi, thus in effect becoming Italy's Financial Intelligence Unit (FIU). Previously, reports from financial institutions were reported to the local police.

70. Law enforcement efforts also focused on the financial aspects of organised crime have aided Italy in achieving a degree of sophistication which the new reporting system should further strengthen. This observation also applies for the legal measures because Italian anti-money laundering legislation has been developed taking also into account the need for combating organised crime. The scope of the Italian legislation is now very wide and the legislative base both for confiscation and money laundering offence is sound domestically and also, following new legislation in 1993, internationally. However, extending the anti-money laundering provisions to cover corporate liability would improve the system. In addition, the decision of the Italian Government to consolidate all the various laws into a more accessible form would also assist in training and in general use.

71. Measures in the financial sector are characterised by extensive obligations and a comprehensive framework. However, the implementation of these measures by non-bank financial institutions not subject to

prudential supervision presents some weaknesses in comparison with the very innovative internal procedures and training programmes carried out by the banks and other financial institutions regulated in a similar manner. Further supervision, guidance and training is therefore needed for non-bank financial institutions not subject to prudential supervision in order to improve their participation in the reporting of suspicious transactions. It is also quite clear that the envisaged extension of the anti-money laundering provisions to individuals or companies carrying out activities which are particularly liable to being used for money laundering purposes will considerably strengthen the Italian anti-money laundering system. For all these reasons, it is hoped that the new legislation will be enacted soon.

72. Overall, the legal and administrative framework of the Italian anti-money laundering system appears to be fundamentally sound, characterised by commendable efforts to improve the major deficiencies identified in the first mutual evaluation. In addition, the strong and firm commitment at political and high civil servant level to combat money laundering is evident. The establishment of an Interagency Policy Commission, comprising all the ministries and agencies concerned, if properly implemented, should be able to exercise strong and effective overshight. The lack of available statistics in certain areas and the weaknesses related to the previous system for reporting suspicious transactions, make it difficult to judge the true effectiveness of the system. However, it is expected that the full implementation of Decree Law no. 153/97 will result in an effective anti-money laundering system.

Norway

73. Drug trafficking together with smuggling and illegal trade in goods subject to high rates of taxation - such as alcohol and tobacco - remain the most significant sources of illegal income. Various types of economic crime, such as national and international investment fraud, invoicing frauds, tax and VAT fraud, and bankruptcy fraud against creditors also appear to be generating a large amount of illegal proceeds and the problem is increasing. As regards money laundering trends, there are indications of increasing cash movements across the borders, and criminals residing in Norway are depositing cash into banks in foreign countries, before transferring the money back to Norway as loans. Like many other countries, Norway has a problem with funds related to persons or companies from the former Eastern Bloc Countries, due to the difficulty of clarifying whether the funds are legal or not. Non-financial businesses or professions are also regularly used in the various stages of the money laundering process.

74. Norwegian control policy on money laundering is based on international initiatives, and an old preventive principle of Norwegian law that crime shall not pay. Measures that are considered important in meeting Norway's anti-money laundering objectives are: (a) increasing the risk of detection and prosecution; (b) improving the tracing and confiscating of illegal proceeds; and (c) facilitating international co-operation. The most significant changes since 1993 have been amendments which entered into force on 1 January 1997, and which extended the predicate offences for suspicious transactions reporting to offences with a sentence greater than six months; extended the preventive measures to the Central Bank, Postbank and more non bank financial institutions; and made available to ØKOKRIM information gathered pursuant to the system of reporting of foreign exchange transactions and the notifications of import and export of cash. The 1988 Vienna Convention and the 1990 Council of Europe Convention on Money Laundering were both ratified in 1994.

75. The money laundering offence, which covers both money laundering and general receiving offences, is very broadly worded and provides a firm basis for prosecution. However, consideration could be given to a specific money laundering offence, which is not part of the general receiving offence. The present confiscation legislation provides a basic structure, and if the recommendations of the Commission on Confiscation are fully implemented, the system should be a strong and effective one. The proposals to reverse of the burden of proof, extend provisions so as to allow illegal assets to be recovered from third parties and extra measures relating to provisional measures and enforcement are all to be commended. Further administrative resourcing measures are required, as are training initiatives, and staff dedicated to the issue of proceeds of crime in the police districts. In relation to international co-operation, Norway is party to

a wide range of international instruments which allow it to provide assistance. This would be further strengthened if operational co-operation between ØKOKRIM and similar foreign bodies were improved through an easing of the secrecy requirements and the entering of more memoranda of understanding to exchange information.

76. The efforts of ØKOKRIM have enhanced the suspicious transaction reporting system, but further changes are required to make the operational and investigative aspects of law enforcement more effective. An increase in resources allocated to ØKOKRIM will allow it to effectively fill the central role that has been allocated to it. The Norwegian police appear to have a more limited knowledge of anti-money laundering procedures and need comprehensive training on the issue of money laundering, so that they can successfully investigate and prosecute such cases. Customs should be taking an increased co-operative role in relation to investigations through an enhanced input in relation to cross-border transactions and more effective measures to combat smuggling and related money laundering. Implementation of the recommendations of the Commission on Investigative Methods should lead to an improved legal framework in relation to new investigative techniques and these measures should be used more frequently in practice.

77. The basic structure of the anti-money laundering measures for the financial sector as set out in the Financial Services Act and Regulations is sound. All the basic elements are there, and the amendments of 1 January 1997 helped to considerably strengthen the legislation. The larger banks are fully supportive of the anti-money laundering initiatives, and are co-ordinate with government authorities, though they would like to increase the degree of contact and exchange of information. However, some further measures would enhance the system.

78. Insurance companies need to be expressly referred to in the Act. A careful and comprehensive study should be made of the categories of non-financial businesses or professions which should be brought under the Act and Regulations. The STR provisions are strong ones, and the system of feedback is excellent, but there is a need to encourage greater and more widespread reporting through increased training and education. The more active involvement of Kredittilsynet in a number of these issues will also improve the implementation of anti-money laundering measures throughout the financial sector.

79. In general, the anti-money laundering system in Norway is solidly based and meets almost all the requirements of the FATF forty Recommendations, and in certain areas the anti-money laundering legislation and system has the potential to be very effective. The positive response to many suggestions of the 1993 FATF report has led to an enhancement of the system, and this has been complemented by the strong role provided by ØKOKRIM in seeking to make the anti-money laundering system effective. Increased expertise and support from other parts of government, together with implementation of the further changes referred to above, will make the system a fully effective and efficient one.

Japan

80. It may be assumed that substantial volumes of criminal gains are laundered in Japan although these acts are not all criminalised. The principal sources of these laundered gains are probably drug crime and fund-raising offences (illicit gaming, extortion, illicit betting, as well as violent crime and property-related offences of all kinds) committed by criminal organisations, e.g. the Boryokudans (Japanese mafia). The latter commit a variety of crimes in pursuit of a vast amount of funds, sometimes abusing legitimate corporate activities. The laundering in Japan, whether each act is criminalised as a money laundering offence or not, of an appreciable volume of gains from foreign crime cannot be ruled out either.

81. Until recently, the Japanese Government had focused its attention on combating drug money laundering. The most important piece of legislation in this respect is the Anti-Drug Special Law (ADSL) which was adopted by the Diet on 2 October 1991, and became effective on 1 July 1992. The ADSL penalises money laundering by prescribing the offences of concealment and receipt of illicit proceeds derived from drug offences. It also enlarges the system of confiscation (including value-based confiscation) and introduces freezing of illicit proceeds, as well as the suspicious transactions reporting system of which the only target is illicit proceeds from drug offences. In accordance with the FATF forty Recommendations and ADSL, financial supervisory authorities have put financial institutions under an obligation to identify their customers on the occasion of certain transactions, and to make suspicious transaction reports (STRs)to their respective supervisory authorities if they suspect that properties taken might be proceeds deriving from drug crimes.

82. However, the Japanese government intends to step up action against money laundering and to reinforce the legal measures at its disposal, as follows:

- the catalogue of predicate offences for money laundering is to be substantially enlarged so as to include all criminal offences of fundamental significance, which will make it easier for financial institutions to report suspicious transactions and the provisions for freezing and confiscating assets are to be extended; and
- a financial intelligence unit (FIU) is to be established in the Financial Supervisory Agency, in conjunction with a new STR system, in which this FIU evaluates the suspicious transaction reports and pass them on through official channels to the law enforcement agencies.

83. To this end the Japanese Government has submitted to the Diet a new Anti-Organised Crime Law (hereafter referred to as "AOCL"), which would provide for the above-mentioned anti-money laundering measures. Upon the enactment of AOCL, strict enforcement of the latter and ADSL would be an effective way to further enhance the combat against money laundering.

84. The Japanese government did not begin until 1996 to remedy some of the defects identified in the first mutual evaluation (the limitation of predicate offences for money laundering to drug crimes, the lack of guidelines for STRs by financial institutions, the lack of a central agency for the receipt of STRs and the limited access of investigatory authorities to these reports). Thus guidelines on STRs were issued in July 1996 and the police are now notified of STRs without an express request. To date, however, this has not brought any decisive improvement in combating money laundering. The low number of STRs shows that investigators are still deprived of the information from financial institutions that is very useful for initiating and assisting investigations. Effective improvements in action to counter money laundering may be expected should the draft of the AOCL come into effect. This applies in particular to the extension of the catalogue of predicate offences and the installation of an FIU at the Financial Supervisory Agency.

85. Pending the adoption of the AOCL, the current legal anti-money laundering provisions of Japan can be assessed as virtually ineffective because of the limited scope of the money laundering predicates

and the direct tracing requirements placed on law enforcement. In addition, these provisions have seldom been used in the fight against money laundering. Compared with other leading international financial centres, the low level of STRs in Japan demonstrates obvious weaknesses in the anti-money laundering system. While the uniqueness of the Japanese economy may contribute to a lower level of STR than western economies, it is difficult to comprehend why an economy of Japan's size and its drug problem should not have led to a more reasonable level of disclosures.

86. While the police appeared to be highly motivated towards money laundering investigations, they do lack valuable tools to assist them in their efforts. In addition, law enforcement and prosecutors must become more proactive in their approaches to detecting and prosecution money laundering. Additional measures, such as setting up independent anti-money laundering units in the investigatory authorities, close co-operation among law enforcement authorities, the Financial Supervisory Agency and its FIU, and use of special investigation methods including electronic surveillance which is incorporated in the AOCL, would greatly assist in the fight against money laundering.

87. The Japanese financial institutions have shown some appreciation of the money laundering problem in Japan and the vulnerability of the financial system. Nevertheless, in practice, there are doubts as to how well their appreciation of the money laundering problem is translated into anti-money laundering action, and whether front-line staff are properly and adequately trained and encouraged to identify and report suspicious transactions. In addition, more industry-specific and detailed guidelines to money changers, securities dealers, insurers and other financial institutions, including those drawn from international typology experience should help to improve the system.

88. As a whole, the current Japanese anti-money laundering system is not effective in practice. In this context, Japan's intention to step up action against money laundering is more than welcome. However, it will not be possible to assess the effectiveness of the future system until it has been in place for several years.

Greece

89. Drug trafficking remains the major concern for Greek authorities, and it is estimated that it accounts for a large part, probably in excess of 50%, of the proceeds of all Greek criminality. Other serious crimes of concern include smuggling, particularly in the antiquities trade, usury, major fraud and other crimes connected with organised crime, as well as other economic crimes such as tax evasion. There is a lack of strong evidence clearly identifying money-laundering trends, however cash placement still seems to be the main problem. The influx of refugees and so-called "economic migrants" from neighbouring Balkan countries has led to increased crime, whilst the activities of some émigrés from the former Soviet Union have been the subject of suspicious transaction reports. There has also been an increase in the physical cross-border transportation of cash, especially foreign banknotes, with such money being deposited temporarily in Greece and then transferred abroad.

90. Greece has attached a high priority to the development of its anti-money laundering framework and policies, and since the first mutual evaluation has worked to build up a satisfactory legislative framework, an effective organisational structure, and an adequate mechanism to ensure compliance and enforcement. The most significant changes were the enactment of : (a) Law 2331 of 24 August 1995 which established the money laundering offence, dealt with confiscation and provisional measures, and introduced provisions to enhance co-operation between law enforcement authorities and financial institutions and suspicious transaction reporting (STR). It also laid the groundwork for the establishment of a central authority (the "Competent Committee"), the functioning of which was completed by Presidential Decree 401/10 December 1996; and (b) the creation of the Financial and Economic Crimes Office with powers to investigate economic crimes, including money laundering.

91. The money laundering offence extends to 20 predicate offences, and makes it an offence if the defendant knew that the property was derived from criminal activity. This could be strengthened if the offence was extended to at least all serious offences, and the mental element of the offence widened to at least gross negligence, though perhaps with less severe penalties than provided for the intentional offence. The provisions relating to confiscation and provisional measures are generally adequate, though some provisions such as article 3(1) Law 2331, which reverses the burden of proof, have the potential to be very effective. However the provisions to confiscate and seize property from non bona-fide third party owners could be enhanced, and it is a matter of concern that no confiscations and few seizures have taken place. This problem should be considered and rectifying measures taken where needed. As regards international co-operation, the most important step is for Greece to ratify and fully implement the 1990 Council of Europe Convention as soon as possible.

92. The creation of the Competent Committee as the financial intelligence unit for Greece has set up a unique structure for the receipt, investigation and analysis of STR. The Committee has a wide range of experience available in its membership, and possesses extensive powers, but because it is a part-time body it will need to carefully monitor its workload and the administrative arrangements with other Greek authorities as they develop. The suspicious transaction reporting system has only been in full operation for 18 months and it is too early to fully assess how effective the system is, and though the results so far are modest, they appear to be progressing the right direction. Some further measures or issues which should be considered include extending the obligation to report to all criminal offences, supplementing the guidance and education which is provided in relation to reporting, whether the time period in which the Committee must consider reports is adequate, and enhancing general and specific feedback.

93. The basic structure of the anti-money laundering measures for the financial sector as set out in Law 2331 and ancillary provisions is sound, though the system of laws, guidelines, education and training appears to have been much more effective in the banking sector than in the non-bank financial sector. The Hellenic Banking Association and the Bank of Greece, and more recently the Competent Committee, have taken a strong and active role in promoting anti-money laundering measures and must be commended for this. Although there also appears to be a preparedness to adopt anti-money laundering measures by non-bank financial institutions, the progress has been considerably slower. The supervisory authorities, and particularly the supervisor for the insurance sector, need to take a more active role in checking the implementation of effective anti-money laundering measures in the non-bank financial sector, through a program of increased supervision, guidance and training.

94. Since the first mutual evaluation in 1994 Greece has made considerable advances and the platform that has been built will provide a sound springboard for the future. The Greek anti-money laundering system now meets most of the 40 Recommendations, and though lack of statistics and data, as well as the fact that major legislative and regulatory measures are quite recent, made it difficult to accurately assess the effectiveness of the system, it appears to be working reasonably well in several areas. Despite this, the results achieved so far, though moving in the right direction, are modest, and Greece will need to continue to monitor the system and implement the necessary changes to make the system more effective.

C. APPLICATION OF THE FATF POLICY FOR NON-COMPLYING MEMBERS

(i) Principles

95. Being aware that it could not expect others to do what certain of its members fail to do, FATF defined in 1996, a policy for dealing with its members which are not in compliance with the initial forty Recommendations. The measures contained in this policy represent a graduated approach aimed at enhancing peer pressure.

(ii) Steps applied in 1997-1998

Austria

96. In accordance with the request made at the June 1997 FATF meeting, Austria reported back to the FATF in February 1998 on the anti-money laundering measures it had taken between June 1997 and February 1998, and the plan of action that it proposed to remove the problems identified in the report. Austria advised that it had:

- amended the common note of interpretation so as to require identification of trustors by lawyers, notaries and certified public accountants;
- acted to clarify other identification requirements;
- created guidelines concerning the protection of employees of credit and financial institutions which act as witnesses;
- set up procedures to obtain extra statistics; and
- published a draft Bill regarding the removal of the monetary threshold of ATS 100,000 in Art 165 Penal Code.

97. However, Austria also advised that the Austrian government had not altered its position in relation to anonymous passbook for Austrian residents. In consequence of this failure, the President wrote a letter to the Austrian government indicating the concern of the FATF regarding the lack of progress in removing the anonymous passbooks. Due to the failure of the Austria to indicate that it would be taking positive steps to remove the passbooks, it was decided to pursue the measures in the FATF policy for non-complying members, i.e. to send a high level mission to Vienna in order to reinforce this expression of concern.

Canada

98. It was suggested during the discussion of the second Canadian mutual evaluation report in September 1997 that Canada provide a progress report, in view of serious concerns over its failure to comply, or to comply fully, with a number of the forty Recommendations. Canada provided a progress report at the June 1998 Plenary meeting and advised that:

- The Department of the Solicitor General had issued a public consultation paper which sets out proposals for :

  a) a mandatory suspicious transaction reporting (STR) system, which would be based on sets of indicators;
  b) offences for failing to file a report and filing a false report, as well as a "tipping-off" offence;
  c) protection from criminal and civil liability for any person or body which makes a report;
  d) the establishment of a federal authority as a new financial intelligence unit (FIU) which would be at arms-length from law enforcement, and which would receive all STR, as well as reports on cross-border transactions, and information from foreign FIU;

e) a cross border reporting system for currency and monetary instruments greater than C$ 10,000, as well as powers to seize as forfeited if no declaration is made. An administrative process for remission of penalty might also be included.

- the Solicitor General has indicated that following the consultation period, Canada intends to table legislation as soon as possible, and probably during autumn 1998;
- Canada was considering signing the 1990 Council of Europe Convention, and will consider in the future the question of amending its legislation to allow enforcement of foreign confiscation orders. However no timeframe has been set for these measures;
- in relation to customer identification, including beneficial ownership, Canada is reviewing the existing regulations and practices with a view to issuing fuller and more comprehensive draft regulations for public comment in autumn 1998, which could come into force in spring 1999;
- it will review the existing coverage of its anti-money laundering regulations with a view to expanding coverage to further categories of non-bank financial institutions such as check cashers, money remitters and postal money order business;
- it will review existing guidelines on matters such as customer identification, record keeping, internal controls and Recommendation 21, with a view to closing any gaps. The federal guidelines will be reviewed initially and revised as appropriate for all federally regulated financial institutions. Furthermore, the federal government will be working with provincial governments and regulators regarding their role in furthering compliance with the FATF Recommendations through the provision of appropriate guidance to provincially regulated financial institutions. Additional measures will be taken with respect to sectors which are not subject to supervision. It was indicated that Canada hopes to achieve some results by spring 1999, although noting that any initiatives are likely to be developed and implemented over the longer term.

Canada offered to provide a further report to the Plenary at the FATF meeting in February 1999.

III. REVIEWING MONEY LAUNDERING METHODS AND COUNTER-MEASURES

99. The FATF conducted a further survey of money laundering methods and countermeasures which provides a global overview of trends and techniques. In this context, the issues of money laundering through new payments technologies (smart cards, banking through Internet), and the non-financial businesses and remittance companies were addressed. Two other areas of work were the issues of how to improve the appropriate level of feedback which should be provided to reporting financial institutions, and the continuation of work on estimating the magnitude of money laundering. Finally, the FATF convened a second Forum with representatives of the world's financial sector institutions.

A. 1997-1998 SURVEY OF MONEY LAUNDERING TRENDS AND TECHNIQUES

100. The FATF typologies exercises provide a forum for the exchange of information and intelligence on prevailing trends in money laundering and effective countermeasures, through an annual meeting of experts from member law enforcement agencies and regulatory authorities. The following paragraphs summarise briefly the conclusions of this year's survey.[7]

101. In addition to money laundering via non-financial professions and businesses, which was the main subject for the FATF-IX typology exercise, the experts also discussed issues relating to companies which specialise in international money transfers, and new technology payments. With regard to new

[7] The Report of FATF-IX on Typologies is at Annex C.

technology, much work has still to be done before all the related money laundering dangers have been clearly identified and before any possible specific counter-measures can be considered. However, even at present, the speed at which transactions are performed in this sector, admittedly an advance in itself, seems to pose grave threats to the adequacy of the traditional anti-money laundering methods as they relate to the systems of new payment technologies. With regard to companies specialising in international money transfers, consideration and action were both further advanced, judging from the scale of counter-measures already in place in many FATF member countries.

102. Among other typologies of interest, particular emphasis was placed on money laundering through the gold market. Although FATF has already devoted considerable attention to sectors such as insurance or money changing, the involvement of both in money laundering is still clearly on the increase. With regard to the bureaux de change sector, it is clear that further consideration must be given to the consequences of the conversion of European currencies into the Euro. Finally, the survey of money laundering trends in non-member countries again proved most instructive. Although progress is being made in implementing anti-money laundering measures outside the FATF membership, much still remains to be done to mobilise many countries which remain somewhat passive and complacent about the financial, economic, political and social dangers posed by money laundering.

103. The 1997-1998 typologies exercise was marked by a more targeted form of discussion than in previous exercises. Since the classic mechanisms for laundering are now well identified, the main challenge in the future will be to survey the emergence of new areas which are not yet fully mapped, such as electronic money and new-technology forms of payment, non-financial professions, the insurance sector and stock exchange dealers.

B. OTHER AREAS OF WORK

(i) Providing feedback to financial institutions

104. Following consideration of the range of general and specific feedback that was being provided in FATF members, and having regard to the importance of providing appropriate and timely feedback, it was decided that a set of guidelines indicating current best practice would be prepared. The guidelines recognise that ongoing law enforcement investigations should not be put at risk, that secrecy laws in some countries may prevent their financial intelligence unit from disclosing significant feedback, and that general privacy laws can also limit feedback. Therefore, the guidelines are not mandatory requirements, but are meant to provide assistance and guidance to financial intelligence units, law enforcement and other government bodies which are involved in the receipt, analysis and investigation of suspicious transaction reports, and in the provision of feedback to reporting institutions on those reports. The Guidelines[8] were discussed with representatives of the financial services sector at the Second FATF Financial Services Forum in June 1998.

105. Amongst the recommendations relating to general feedback are the following : (a) statistics be kept on the reports received and on the results obtained, together with appropriate breakdowns of that information; (b) the statistics on the reports received are cross referenced with results so as to identify areas where money laundering and other criminal activity are being successfully detected; (c) new money laundering methods or techniques, as well as trends in existing techniques are described and identified, and that institutions are advised of these trends and techniques; (d) that sanitised cases be made available to reporting institutions, and that each case could include a description of the fact, a summary of the result, a description of the inquiries made by the FIU if appropriate; and a description of the lessons to be learnt from the reporting and investigative procedures that were adopted in the case.

[8] See Annex E.

Consideration should also be given to providing other general information, such as an explanation on money laundering process, the legal obligations regarding reporting, the procedures and processes etc.

106. The guidelines also consider the methods by which such feedback can be provided, and these include annual reports, regular newsletters, videos, electronic information systems such as websites, electronic databases or message systems, meetings with institutions, conferences and workshops, and working or liaison groups. When deciding on the methods of general feedback to use, each country should take into account the views of the reporting institutions as to degree to which reporting of suspicious or unusual transactions should be made public knowledge.

107. Specific feedback is more difficult to provide than general feedback, for both legal and practical reasons. Practical concerns include not putting ongoing law enforcement investigations at risk and the issue of resource implications, while legal issues can involve secrecy laws relating to the financial intelligence unit or general privacy laws. Finally, there is a need to ensure the safety of the staff of institutions, and to protect them from being called as witnesses in court. Having regard to all these matters, it is recommended that whenever possible, the following specific feedback is provided:

- receipt of the report should be acknowledged by the FIU;
- if a report will be subject to a fuller investigation, the institution could be advised of the agency that will investigate the report, if this would not adversely affect the investigation; and
- if a case is closed or completed, whether because of a concluded prosecution, because the report was found to relate to a legitimate transaction or for other reasons, then the institution should receive information on that decision or result.

(ii) Estimating the magnitude of money laundering

108. During 1997-98 work continued on the study to estimate the magnitude of money laundering. An Ad Hoc group, chaired by the head of the United States delegation, has considered a number of studies that had been completed previously as well as some current ongoing studies that consider issues relating to estimating the volume of criminal proceeds. One important strand of the work is being principally carried out by the IMF, which is updating a previous study it made in 1996 on the "Adjusted Demand for Money Model". This model estimates the impact of money laundering associated with crime on the demand for currency and money balances in the banking system, and concludes that it can have a significant impact.

109. The major part of the work of the group has focussed on obtaining agreement for a sound but practical methodology for using microeconomic data and techniques to estimate the amount of criminal proceeds available in relation to a range of serious profit generating crimes, and the amount of such proceeds available for money laundering. A meeting of experts from members and international organisations sponsored by the Chair of the Ad Hoc Group on 28-29 May 1998, considered the alternative methods and data sources that are available for making the necessary calculations. The meeting also considered a United Kingdom study that was being prepared in the context of efforts by the European Union to develop estimates of the proceeds of certain illegal activities for national accounts purposes.

110. It was recognised that the complex questions arise concerning the availability, reliability and comparability of national and international data, and in relation to the methodology which should be adopted; however it was agreed that the FATF should continue to develop this study and that all FATF member jurisdictions should participate. The study will therefore continue during FATF-X, and will focus on researching the available national and international data, and on finalising details as to how that data can be gathered and analysed.

C. SECOND FORUM WITH THE FINANCIAL SERVICES INDUSTRY

111. One of the FATF's goals is to encourage cooperation with the private financial sector in the development of policies and programmes to combat money laundering. To further this aim, two years after the first international meeting between the FATF and representatives of the financial services industry, a second Forum was convened during FATF-IX. The purpose of this event was to discuss with the private sector, areas of common interest and ways to best develop measures to prevent and detect money laundering through the financial community.

112. Representatives from FATF members, national banking and insurance associations as well as members of the non-bank financial sector and delegates from international financial services industry organisations (Banking Federation of the European Union, International Banking Security Association, European Insurance Committee, European Grouping of Savings Banks, Federation of Latin American Bankers Association, International Federation of Accountants, the Central Bank of the Russian Federation) attended a Forum organised by the FATF in Brussels. Five general topics were addressed in the Forum: money laundering typologies exercises and the development of FATF policy; the nature of the money laundering threat and the countermeasures in the non-bank financial institutions; the implications of the new technologies (including direct banking) for money laundering and the use of these media to detect suspicious/unusual transactions; providing necessary feedback to financial institutions reporting suspicious transactions; and the role of the accounting profession in anti-money laundering action.

IV. FATF'S EXTERNAL RELATIONS AND OTHER INTERNATIONAL ANTI-MONEY LAUNDERING INITIATIVES

113. As the third component of its mission, the FATF undertakes external relations actions designed to raise awareness in non-member nations or regions to the need to combat money laundering, and offers the forty Recommendations as a basis for doing so. In promoting the adoption of anti-money laundering measures, it is important to bear in mind that the FATF does not act in a vacuum. A number of international organisations or bodies play a significant role in this respect. The following paragraphs describe the most important developments which occurred in 1997-1998 in the international fight against money laundering.

114. In general, the FATF continued to collaborate with the relevant international organisations/bodies rather than launch new initiatives. The FATF participates in anti-money laundering events organised by other bodies so that it can observe the developments taking place in non-members and in particular the adoption of money laundering counter measures. The United Nations Global Programme on Money Laundering will contribute significantly to the implementation of these measures through the provision of training and technical assistance.

115. To increase the effectiveness of international anti-money laundering efforts, the FATF and the other organisations and bodies endeavour to co-ordinate their activities. Regular co-ordination meetings of the regional and international bodies concerned with combating money laundering take place in the margins of the FATF Plenaries.

A. FATF'S EXTERNAL RELATIONS INITIATIVES

Cyprus

116. A FATF mission to Cyprus took place at the beginning of September 1997, with the participation of an OGBS's representative, to discuss money laundering issues with the competent Government departments and the Central Bank of the Republic of Cyprus. It was quite clear that a number of important steps had been taken to fight money laundering, particularly the enactment of the Law on the Prevention and Suppression of Money Laundering Activities in April 1996. Among other measures, the Law contains a definition of a serious crimes money laundering offence and a requirement to report suspicious transactions to the Unit for Combating Money Laundering. The Republic of Cyprus has also ratified the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. However, the FATF mission recommended that the Cypriot authorities continue their efforts, specifically with respect to the coverage of the non-bank financial sector. The mission also strongly encouraged Cyprus to undergo a joint Council of Europe/OGBS mutual evaluation of its money laundering system so that further progress can be made. This evaluation was carried out in the spring of 1998.

Russian Federation

117. A joint FATF/Bank of Russia Money Laundering Conference took place on 9-10 October in St. Petersburg, as a follow-up to the FATF high-level mission to Moscow of 1996. The Conference was attended by participants from nine FATF countries. The Russian Federation was represented by numerous delegates from the Bank of Russia, the Ministry of Finance, the Ministry of Justice, the Customs Committee, the Federal Service on Foreign Exchange and Export Control, the Ministry of the Interior, the Federal Security Service, the State Tax Service, the Tax Police, the General Prosecutor, and the Association of Russian Banks.

118. The Conference discussed the role of the financial and credit institutions in the combat of money laundering with particular emphasis on the regulatory bodies. It was pointed out that the Bank of Russia has taken a major anti-money laundering step by creating a national system of preventive measures aimed at safeguarding the banking community against dirty money. In July 1997, the Bank of Russia issued recommendations to prevent illegal funds passing through banks and credit institutions; a Directive on organising internal banking controls and a Guideline on how to organise internal controls in credit institutions which participate in financial markets. Due to a lack of legislation, these texts will assist banks and credit institutions to undertake anti-money laundering work. For the elaboration of the above-mentioned texts, the Bank of Russia used as a basis the forty FATF Recommendations.

119. Participants from the FATF countries expressed their support for the joint efforts undertaken by the Federal Government bodies and the Bank of Russia in creating a national system to prevent dirty money from entering into the economy. They also expressed the wish that the Bill on "Countering Legalisation (Laundering) of Illegally Gained Incomes" which has been pending in the Duma for more than a year, will be expedited.

B. ANTI-MONEY LAUNDERING ACTION BY "FATF-STYLE" REGIONAL BODIES

Caribbean FATF

120. Since its inception, participation in the CFATF has grown to twenty-four states of the Caribbean basin.[9] The CFATF has instituted measures to ensure the effective implementation of, and compliance with, the Recommendations. The CFATF Secretariat monitors members' implementation of the Kingston Ministerial Declaration through the following activities:

- self-assessment of the implementation of the Recommendations;
- on-going programme of mutual evaluation of members;
- co-ordination of, and participation in, training and technical assistance programmes;
- bi-annual plenary meetings for technical representatives; and
- annual Ministerial meetings.

121. To further its mandate to identify and act as a clearing house for facilitating training and technical assistance needs of members, the Secretariat works closely with regional Mini-Dublin Groups, the diplomatic representatives of countries with interest in the region. Prominent here are Canada, France, the Netherlands, the United Kingdom and the United States. There is also close liaison with CARICOM, the Caribbean Customs Law Enforcement Council (CCLEC), the Centre Interministériel de Formation Anti Drogue (CIFAD) in Martinique, the Association of Caribbean Chiefs of Police (ACCP), the Commonwealth Secretariat and the International United Nations Drug Control Programme (UNDCP).

122. Supported by, and in collaboration with UNDCP, the CFATF Secretariat has developed a regional strategy for technical assistance and training to aid effective investigation and prosecution of money laundering and related asset forfeiture cases. The development of this regional strategy parallels and closely co-ordinates with similar initiatives by the European Commission and with efforts arising from the Summit of the Americas Ministerial in Buenos Aires.

123. The FATF strongly supports the significant progress which has been made by the CFATF under both the chairmanships of Costa Rica and Barbados. Three mutual evaluation reports were discussed (Costa Rica, Panama, Barbados), and six on-site visits took place (Antigua and Barbuda, Bahamas, Bermuda, the Dominican Republic, St. Vincent and the Grenadines, Turks and Caicos) in 1997-1998 together with the adoption of a firm timetable for the remainder. The CFATF also pursued its active typologies programme and the development of important internal processes, which are all significant advances.

Asia/Pacific

124. The Working Party meeting of the Asia/Pacific Group on Money Laundering (APG) which was held in Beijing in July 1997 made valuable progress. Countries in the region have started to exchange information and examine the strengths and weaknesses of their systems through the mechanism of jurisdiction reports. Measures are also proposed for improving technical assistance and training, enhancing mutual legal assistance and improving cooperation with the financial sector. The Working Party also recognised that, although regional differences need to be taken into account, the FATF forty Recommendations provide guiding principles for action in establishing an effective anti-money laundering system. The FATF stands ready to assist the APG in its consideration of how international standards such as the forty Recommendations can best be implemented in the region.

[9] See the list of CFATF members at Annex B.

125. The Asia/Pacific Group currently consists of 16 members[10] in the Asia/Pacific region comprising members from South Asia, Southeast and East Asia and the South Pacific. In March 1998, the first annual meeting of the APG was held in Tokyo and attended by 25 jurisdictions from the region. A revised Terms of Reference was agreed, as well as an action plan for the future. The Tokyo meeting represented the full establishment of the APG as a cohesive regional group following on from the earlier awareness-raising efforts. The Asia/Pacific Group provides an essential foundation for countering the global threat of money laundering. It will lead to more effective anti-money laundering legislation in each country, and to enhanced international cooperation.

126. In addition to a statement issued on 6 April 1997 by the Finance Ministers of the Asia Pacific Economic Cooperation (APEC) welcoming the establishment of the APG, the leaders of the 1998 Asia-Europe Meeting (ASEM) asked their Finance Ministers to encourage enhanced co-operation between Europe and Asia in the fight against money laundering.

C. MUTUAL EVALUATION PROCEDURES CARRIED OUT BY OTHER BODIES

General

127. The FATF has adopted a policy for assessing the implementation of anti-money laundering measures in non-member governments. The rationale for this policy is that the implementation of a mutual evaluation procedure will encourage countries and territories not only to get on with implementing anti-money laundering laws but also to improve the counter-measures already in place. The Task Force has already validated and supported the mutual evaluation processes of other bodies which have agreed to carry out mutual evaluations of their members. In this respect, the FATF assessed the CFATF, the Council of Europe and the OGBS's mutual evaluation procedures as being in conformity with its own principles. As the latter is comprised of representatives of banking supervisory authorities, the FATF has sought formal political endorsement of the procedures and the forty Recommendations from those governments of the members of the OGBS which are not represented in either the CFATF or the FATF.

128. The FATF believes that the mutual evaluation procedures of the CFATF, the Council of Europe and the OGBS will contribute to secure the adoption of adequate anti-money laundering measures in many non-member countries and territories. The FATF has therefore furthered its co-operation with these bodies. First, it stands ready to provide assistance in the training of mutual evaluators of non-FATF bodies. Second, FATF member countries will supply observer examiners, if requested, by one of the three bodies/organisations mentioned above.

CFATF

129. CFATF member governments have made a firm commitment to submit to mutual evaluations of their compliance both with the Vienna Convention and with the CFATF and FATF Recommendations. Signalling this firm commitment is the fact that the October 1997 CFATF Council of Ministers in Barbados adopted a mandatory schedule of mutual evaluations. According to the latter, the CFATF's first round of mutual evaluations will be completed by the year 2000. In the past eighteen months of the schedule, eight members have undergone mutual evaluations: Costa Rica, Panama, the Dominican Republic, Barbados, St. Vincent and the Grenadines, the Bahamas, Antigua and Barbuda, and Turks and Caicos Islands. Even before this, in 1995, the Cayman Islands and Trinidad and Tobago were evaluated. By the end of 1998, Bermuda, St. Lucia, St. Kitts and Nevis, and Nicaragua will increase the number of members to have been mutually evaluated.

Council of Europe

[10] See the list of APG members at Annex B.

130. In September 1997, the Committee of Ministers of the Council of Europe established a Select Committee (PC-R-EV) to conduct self- and mutual assessment exercises for member states of the Council, which would be modelled on FATF processes. Over a two year period ending in December 1999, mutual evaluations are to be conducted for the members of the Council which are not also members of the FATF. Experts from member countries of the FATF will assist with and participate in those evaluations. The process commenced with evaluations of Slovenia and Cyprus (conducted in conjunction with the Offshore Group of Banking Supervisors), and the mutual evaluation reports for those two countries were considered and adopted at a meeting of the PC-R-EV in June 1998. Further evaluations (e.g. Czech Republic, Slovakia, Malta, Hungary, Lithuania and Andorra) will be conducted during the second half of 1998.

131. In March 1998, the Council of Europe, in conjunction with the Belgian Presidency of the FATF and the European Commission, organised in Brussels a training seminar for persons from non-FATF countries who would be participating as evaluators in the mutual evaluation process. This event, which was well attended by participants from those countries, discussed the applicable international conventions and instruments, the practical aspects of the process, and the legal, financial and law enforcement components of anti-money laundering systems.

OGBS

132. FATF has received ministerial letters indicating political endorsement of the forty Recommendations and the mutual evaluation procedure from all but one member of the Offshore Group of Banking Supervisors (Lebanon). The Task Force has therefore endorsed the commencement of the OGBS mutual evaluation process, except for the aforementioned country which, as a result, has been changed from full membership of OGBS to observer status. The OGBS is taking steps to carry out its first mutual evaluations before the end of 1998; these will concern Jersey, Guernsey, the Isle of Man and possibly Vanuatu. Two other members of the OGBS -- Cyprus and Malta -- have been or will be covered by a joint Council of Europe/OGBS mutual evaluation.

D. OTHER INTERNATIONAL ANTI-MONEY LAUNDERING ACTION

United Nations

133. The Global Programme against Money Laundering (GPML), a research and technical co-operation programme implemented by the UN Office for Drug Control and Crime Prevention (ODCCP), is now in operation. Its aim is to increase the effectiveness of international action against money laundering through comprehensive technical co-operation services offered to Governments. The Programme is carried out in cooperation with other international and regional organisations. In the context of the GPML, the UNODCCP organised several important international anti-money laundering events in 1997-1998, including two awareness-raising seminars for West Africa in Ivory Coast on 1-3 December 1997 and for South Asian countries plus Myanmar and Thailand in New Delhi on 2-4 March 1998.

134. Finally, the United Nations General Assembly was convened on 8-10 June 1998 in New York for a Special Session devoted to the fight against the illicit production, sale, demand, traffic and distribution of narcotic drugs and psychotropic substances and related activities, including money laundering. The General Assembly adopted a Political Declaration in which the Member States of the United Nations undertake to make special efforts against the laundering of money linked to drug trafficking and recommend that States which have not yet done so, adopt by the year 2003 national anti-money laundering legislation and programmes in accordance with relevant provisions of the Vienna Convention and a package of measures for countering money laundering, adopted at the same session.

Commonwealth

135. Commonwealth Heads of Government at recent summits have repeatedly called for concerted action to combat money laundering which has been and continues to be a high-priority activity for the Commonwealth Secretariat. Following their last meeting in Edinburgh, in October 1997, a joint meeting of finance and law officials was convened so that a co-ordinated approach could be developed to consider further measures to combat money laundering. The joint meeting was held in London on 1-2 June 1998 and considered the four following main items:

- improving domestic co-ordination through national interdisciplinary co-ordinating structure;
- the special problems of dealing with money laundering in countries with large parallel economies;
- strengthening regional initiatives for more effective implementation of anti-money laundering measures; and
- self-evaluation of progress made in implementing anti-money laundering measures in the financial sector.

Inter-American Development Bank

136. The IDB, in conjunction with the Banking Superintendent of Colombia and the Andean Development Corporation, sponsored a seminar on the subject of asset laundering during the 1998 annual meeting of the Board of Governors in Cartagena de Indias (Colombia). The session addressed the multifaceted aspects of asset laundering activities as well as international approaches to combat money laundering on the basis of presentations made by the United Nations, the OAS/CICAD, the IDB, the IMF, the Federation of Latin American Bankers Association and the FATF. The seminar ended with certain common goals, focusing on a multilateral approach to combating asset laundering in Latin America and the Caribbean, as well as current and future activities in the region. The IDB was encouraged to: (a) use its own funds and to seek additional funding for programmes, including the training needs of supervisors, regulators and financial institutions, particularly on the detection and prevention of new laundering techniques on a regional and/or national basis; (b) serve as a clearing house for such proposed programmes, sources of funding, and potential executing entities; (c) strengthen the dialogue between private banking sectors and government regulators; and (d) use its good offices to encourage implementation of effective laws and regulatory frameworks to address the issue of asset laundering.

OAS/CICAD

137. The CICAD Group of experts to Control Money Laundering has continued to put into effect the Buenos Aires Plan of Action.[11] The CICAD Group of Experts, which meets twice a year, at its last meeting in May 1998 approved a training programme for judges, prosecutors, FIU personnel and law enforcement. It also undertook to amend the Model Regulations to expand the predicate offence for money laundering and to provide for the creation of national forfeiture funds. In addition, the Group finalised a directory of contact points for the purpose of effecting information exchange and mutual legal assistance which would be accessible through the OAS's web-page.

---

[11] In December 1995, the Ministers responsible for addressing money laundering in the States of the Western hemisphere met in Buenos Aires where they endorsed a Statement of Principles to combat money laundering and agreed to recommend to their Governments a Plan of Action reflecting this Statement of Principles for adoption and implementation. The Plan of Action specifically provided that the Governments intended to institute on-going assessments of the implementation of the Plan of Action within the framework of the OAS. This and other activities identified in this Plan were remitted to the CICAD for action.

CONCLUSION

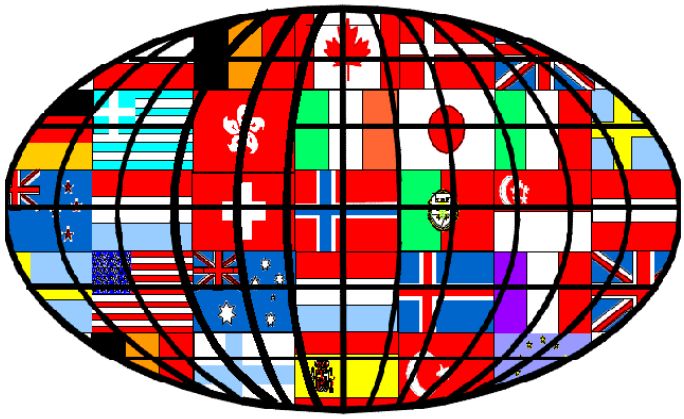
138. During 1997-1998, further progress was again made in combating money laundering, both within and outside the FATF membership. However, the need for continuing action against money laundering is obvious. It is for this reason that it was decided that the Task Force should continue its work for a further five years and focus its efforts to spread the anti-money laundering message to all continents and regions of the globe.

139. The globalisation of financial markets -- and financial crime -- implies that the counter-measures necessary to combat money laundering must be universally applied. To this end, the FATF will work to foster the establishment of a world-wide anti-money laundering network based on an adequate expansion of the FATF membership, the development of the FATF-style regional bodies such as the Caribbean FATF and the Asia/Pacific Group on Money Laundering, and close co-operation with all the relevant international organisations. As money laundering is an evolving phenomenon, it will also be essential to strengthen the review of money laundering trends and countermeasures. In addition, improving the effective implementation of the forty Recommendations within the FATF membership will be a critical challenge.

140. As the world-wide mobilisation against money laundering has now become the priority goal of the FATF, external action will be given a high priority in the forthcoming years. This vital task will be carried forward in 1998-1999 under the Presidency of Japan.

FATF-IX

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING



ANNEXES

1997-1998 ANNUAL REPORT

June 1998

TABLE OF CONTENTS

ANNEX A

Money Laundering: the Importance of International Countermeasures

Address by Michel Camdessus
Managing Director of the International Monetary Fund
at the Plenary Meeting of the Financial Action Task Force
on Money Laundering
Paris, February 10, 1998

The statement at the October 1996 Annual Meetings in Washington D.C. of the IMF's Interim Committee—its highest decision-making authority—featured money laundering as one of the most serious issues facing the international financial community. This is a confirmation, if at all needed, of our wish to develop our relationship with you as the main body for dealing with money laundering, and this is also why I wished to come here today to honor your remarkable work, which has been most impressive in its scope and the speed with which it has been geared up. Let me do so by putting this question before you: why is money laundering viewed as such a serious threat to the global monetary system? And if it is a threat, what is the role that the IMF can play in assisting the work of the FATF? How can we limit this threat, which can take on such proportions that it undermines the effectiveness of macroeconomic policy?

* * * * *

Macroeconomic impact of money laundering

I hardly need say that the IMF regards the anti-money laundering actions advocated by the FATF as crucial for the smooth functioning of the financial markets. While we cannot guarantee the accuracy of our figures—and you have certainly a better evaluation than us—the estimates of the present scale of money laundering transactions are almost beyond imagination—2 to 5 percent of global GDP would probably be a consensus range. This scale poses two sorts of risks: one prudential, the other macroeconomic. Markets and even smaller economies can be corrupted and destabilized. We have seen evidence of this in countries and regions which have harbored large-scale criminal organizations. In the beginning, good and bad monies intermingle, and the country or region appears to prosper, but in the end Gresham's law operates, and there is a tremendous risk that only the corrupt financiers remain. Lasting damage can clearly be done, when the infrastructure that has been built up to guarantee the integrity of the markets is lost. Even in countries that have not reached this point, the available evidence suggests that the impact of money laundering is large enough that it must be taken into account by macroeconomic policy makers. Money subject to laundering behaves in accordance with particular management principles. There is evidence that it is less productive, and therefore that it contributes minimally, to say the least, to optimization of economic growth. Potential macroeconomic consequences of money laundering include,

but are not limited to: inexplicable changes in money demand, greater prudential risks to bank soundness, contamination effects on legal financial transactions, and greater volatility of international capital flows and exchange rates due to unanticipated cross-border asset transfers.

Moreover, I should add that while, from the viewpoint of the Fund as a financial institution, I emphasize the economic costs, we must also remember the social and political dimensions of crime and related money laundering—the suffering of the victims and the overall weakening of the social fabric and collective ethical standards. All of this lends urgency to anti-laundering efforts, which attack criminal activity at the most vulnerable point—where its proceeds enter the financial system.

But does this mean that we should abandon the liberalization of the financial markets? This high-minded argument is often raised by those of our critics who believe that the IMF should halt its efforts to move its members away from control-based, towards market-based, financial systems because such systems open up possibilities for money launderers. Some have argued that keeping in place centralized credit allocation and foreign exchange control systems is necessary to identify money launderers—even if we now know that such systems are inimical to economic growth. However, I am reassured that Recommendation 22 of the FATF's 40 Recommendations is very clear on this point: "Countries should ... monitor the physical cross-border transportation of cash and bearer instruments—without impeding in any way the freedom of capital movements." Information, rather than control of the transactions, is the key to the basic "know your customer" approach of the FATF. More generally, the value of adequate information to guide the supervision of financial markets has been made very clear by recent events in South-East Asia. It is not just free financial markets that the IMF advocates, but also modern financial markets—in which there is a good measure of transparency and prudential regulation to ensure the fairness, soundness, and legality of the systems. Adoption of the FATF's recommendations is an important part of that aspect of market development. On the other hand, controls of all kinds and state interventions do not have an impressive record in avoiding money laundering, while they frequently create opportunities for corruption. Does this still hold true in a context of globalization?

Globalization and money laundering

Globalization of financial markets is one of the most important contemporary developments. What are its implications for the fight against money laundering? Clearly, globalization implies that the prevention strategies must be universally applied. All countries must participate—and participate enthusiastically—or the money being laundered will flow quickly to the weakest point in the international system. It is in this respect that the FATF plays an especially important role. It has developed a comprehensive and authoritative set of international standards for anti-money laundering policies, and procedures for their application and enforcement. Through its so-called "typologies" exercises, the FATF has pooled the intelligence of its members regarding financial instruments and institutions used by the money launderers, and this is reflected in its standards. The FATF has also been energetic in spreading its message beyond its own membership, which is comprised largely of the industrial countries. Like the IMF, it has found the "mission" format, by which groups of FATF experts visit nonmember countries, to be valuable in disseminating and promoting its policies. But this process is even more effective when the countries concerned are members of the FATF group—and can enjoy the immediacy, "ownership," and self-evaluation that come with membership.

It is therefore a significant achievement that the FATF has established, within the few years since its own formation, two regional offshoots—the Caribbean FATF, and very recently, the Asia/Pacific Group on Money Laundering. These regional bodies will play an important role in promoting the "modern" financial markets that I referred to earlier—taking into account the special features and state of development of the regional systems.

Good governance

Much has been accomplished, but much remains to be done—on your part and our own. Our efforts and your efforts cannot be separated from the global strategy of improving governance. The IMF is increasingly incorporating governance issues within its overall mandate. The IMF's Interim Committee, at its meeting in Washington in September 1996, adopted a declaration which identified "promoting good governance in all its aspects, including ensuring the rule of law, improving the efficiency and accountability of the public sector, and tackling corruption" as an essential element of a framework within which economies can prosper. Particularly in countries where there is significant participation of government institutions or officials in illegal activities—which yields proceeds that must then be laundered—the adoption of anti-laundering policies can have far-reaching effects on governance. In such countries, the IMF is actively using its available leverage to persuade the authorities to take the necessary steps. The global nature of the IMF's surveillance and technical assistance activities offers opportunities for raising awareness of the need for a robust international anti-money laundering system—pointing to the need for governments to adopt effective anti-laundering legislation, and to contact the FATF for its expert assistance in developing detection and enforcement capabilities. An important step toward full international coverage of this system will be the creation of further regional FATFs—notably for the transitional economies of Europe, and in the African and Middle Eastern regions.

Role of banking supervision

Another area of the Fund's work that has a close association with the fight against money laundering is that of banking supervision. The Core Principles for Effective Banking Supervision, approved by the Basle Committee in September 1997, state that "Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict ?know-your-customer' rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements." The IMF provides extensive policy and technical assistance to central banks and other national institutions around the world in building up their supervisory capabilities. This assistance has been framed around, and in fact has contributed to, the core principles. Recent developments have shown an acute need for actions to strengthen the infrastructure for prudential supervision in some countries that otherwise have relatively advanced financial markets, but where inadequate supervision remains an "Achilles heel." Top priority must be given to developing supervision of financial sectors. Such supervisory frameworks will also constitute an important means of generating close adherence to the FATF's principles. They are in the best interest not only of the international system, but also, and first and foremost, of the individual countries concerned.

In the context of banking supervision, I would like to say a special word about offshore banking centers. With the widespread elimination of exchange controls and the emergence of domestic derivative finance, the traditional role of the offshore centers has

diminished. However, the proliferation of smaller offshore centers offering "tax and regulatory services," including secrecy and confidentiality, is a cause for concern. Some of the offshore centers feature prominently in international discussions of serious money laundering problems. Even with the government's best will—and that is sometimes not present—very small countries or territories tend to lack the expert resources needed to supervise large numbers of offshore banks. Caution thus dictates that licenses to operate offshore facilities in such countries should be granted only to proven institutions that are adequately supervised in their respective countries of origin. I am not sure that this is always the case, and the question is whether the international community can continue to tolerate these weak links in its organization.

Other related work of the IMF

What other aspects of the IMF's activities bear on the money laundering problem?

- First, in many countries, the IMF provides technical and policy assistance to members in drafting new central bank and commercial banking laws. This provides a good opportunity to remind countries of the need for anti-laundering provisions, such as the obligation to verify the identity of customers and to report suspicious transactions to the police or similar enforcement groups. Model laws, which draw together expertise of other countries, can provide a very useful start to this process.

- Then there are the IMF's ***research and statistical functions***. It probably does not surprise you to know that IMF staff have been active in researching underground economies and the closely related money laundering problem for almost two decades now. Good analysis is necessary to determine the scope and form of the money laundering problem, and to help direct enforcement resources efficiently to the key aspects of the problem. Good data are also necessary—money laundering is by definition a hidden activity—and therefore indicators must be drawn from a wide range of economic and social data. Although not directly usable to identify money laundering, extensive international financial and cross-border data compiled by the IMF have been used in a number of economic studies of money laundering. In fact, money laundering is now an important consideration for compilers of international data because it creates global asymmetries in the data.

- Finally, there is the IMF's work on fiscal issues, and on ***tax evasion*** in particular. Although some members' anti-money laundering legislation does not apply to the proceeds of tax evasion, there are inevitably close linkages between the two. Money that has evaded taxes must be disguised, and laundered money must be kept hidden from the tax authorities. The IMF's policy and technical work to help its members improve their tax collections therefore assists the fight against money laundering—directly or indirectly, depending on the relevant legislation in the individual country.

* * * * *

I will conclude by emphasizing once again that there is no conflict between free, competitive markets and anti-money laundering regulations. On the contrary, there is considerable synergism between the two. The same oversight and supervision mechanisms that operate to ensure the smooth functioning of the market-oriented

financial system make a strong contribution to the information base and the general environment of integrity that supports the FATF policies. Conversely, money-laundering seriously undermines the functioning of markets, with a consequent negative impact on economic growth. It is true that the regulatory policies to achieve both sets of aims are by necessity those of sovereign nations and cannot simply be imposed on them. But unquestionably, they deserve the support of all—the international financial and enforcement communities, as well as the individual banks, nonbank intermediaries, and regulators in each of the countries. And we as international bodies must ensure that the policies are ***perceived*** as being in the self-interest of all. It need hardly be said that the quality of our cooperation will only add to the strength of our common message!

ANNEX B

Sources of support for the forty Recommendations outside FATF

CFATF

The Caribbean Financial Action Task Force (CFATF) endorsed the original forty FATF Recommendations in the Kingston Declaration of November 1992.[12]

The current CFATF members[13] are: Antigua and Barbuda, Anguilla, Aruba, the Bahamas, Barbados, Belize, Bermuda, the British Virgin Islands, the Cayman Islands, Costa Rica, Dominica, Dominican Republic, Grenada, Jamaica, Montserrat, the Netherlands Antilles, Nicaragua, Panama, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Turks and Caicos Islands, Trinidad and Tobago and Venezuela.

Commonwealth

In October 1997, the Commonwealth Heads of Government (CHOGM) welcomed the endorsement by Finance Ministers of the updated forty Recommendations of the FATF.

The Commonwealth members, which are not members of FATF,[14] are: Antigua and Barbuda, Bahamas, Bangladesh, Barbados, Belize, Botswana, Brunei Darussalam, Cameroon, Cyprus, Dominica, Gambia, Ghana, Grenada, Guyana, India, Jamaica, Kenya, Kiribati, Lesotho, Malawi, Malaysia, Maldives, Malta, Mauritius, Mozambique, Namibia, Nauru, Nigeria, Pakistan, Papua New Guinea, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Seychelles, Sierra Leone, Solomon Islands, South Africa, Sri Lanka, Swaziland, Tonga, Trinidad and Tobago, Tuvalu, Uganda, United Republic of Tanzania, Vanuatu, Western Samoa, Zambia and Zimbabwe.

Council of Europe

The Council of Europe Select Committee of Experts on the Evaluation of Anti-money Laundering Measures takes into account, as one of the relevant international standards, the forty Recommendations of the FATF (cf. Specific terms of reference adopted by the European Committee on Crime Problems for the Select Committee).

The membership of the Committee is comprised of the Council of Europe member States which are not members of the FATF: Albania, Andorra, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Liechtenstein, Lithuania, Moldova, Malta, Poland, Romania, Russian Federation, San Marino, Slovakia, Slovenia, "The Former Yugoslav Republic of Macedonia" and Ukraine.

---

[12] In the Kingston Declaration, the governments of the CFATF members also made a commitment to implement the 19 additional CFATF Recommendations. The CFATF has been conducting a typologies exercise evaluate and to determine whether any interpretative notes and/or amendments to the FATF revised Recommendations and the CFATF 19 recommendations are appropriate.

[13] Aruba and the Netherlands Antilles are part of the Kingdom of the Netherlands, which is a member of FATF.

[14] The Commonwealth members which are members of the FATF are: Australia, Canada, New Zealand, Singapore and the United Kingdom.

Offshore Group of Banking Supervisors

The conditions for membership of the Offshore Goup of Banking Supervisors (OGBS) include a clear commitment to be made to the FATF's forty Recommendations.

In addition, the following members of the OGBS, which are not members of the FATF or the CFATF, are formally committed to the forty Recommendations through individual Ministerial letters sent to the FATF President during 1997-1998: Bahrain, Cyprus, Gibraltar, Guernesey, Isle of Man, Jersey, Malta, Mauritius and Vanuatu.

Riga Declaration

In a Declaration signed at Riga in November 1996 by their Prime Ministers, Estonia, Latvia and Lithuania committed their Governments to the fight against money laundering. The preamble of the Declaration states, inter alia, that these governments are committed to implementing anti-money laundering measures based on the forty Recommendations of the FATF.

Asia/Pacific Group on Money Laundering (APG)

The revised Terms of Reference for the APG, adopted in Tokyo on 10-12 March 1998, recognised that the FATF's forty Recommendations are accepted international standards.

The members of the APG are: Australia, Bangladesh, Chinese Taipei, Fiji, Hong Kong,China, India, Japan, New Zealand, Peoples Republic of China, Republic of Korea, Republic of the Philippines, Singapore, Sri Lanka, Thailand, United States of America and Vanuatu.

ASEM

The Communiqué of the Asia-Europe meeting (ASEM2) held in London on 3-4 April 1998, stated that "The development of policies against money laundering has been helped by the FATF's forty Recommendations which are now the internationally accepted standard."

United Nations

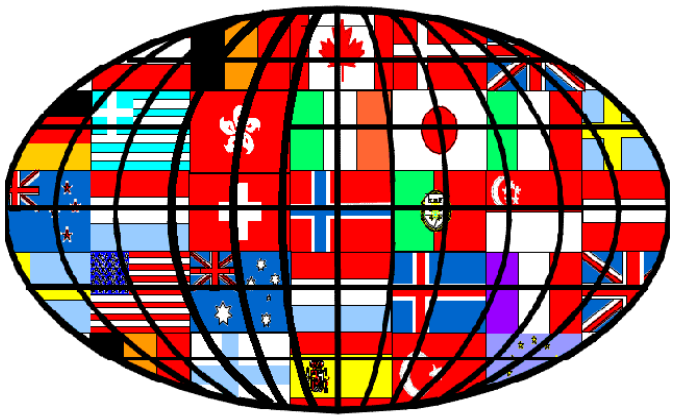
In a Declaration of 10 June 1998, the United Nations General Assembly in Special Session on the world drug problem recalled that the 1996 Resolution 5 of the United Nations Commission on Narcotic Drugs noted that "the forty Recommendations of the Financial Action Task Force .... remain the standard by which anti-money laundering measures adopted by concerned States should be judged;"

In December 1997, in Gand-Bassam (Ivory Coast), participants in the United Nations Workshop on Money Laundering recommended that States should adopt or take into account the Recommendations of the Financial Action Task Force on Money Laundering.

In March 1998, a United Nations Conference on Money Laundering awareness-raising for South and South West Asia recommended that "in drafting their legislation, States should have regard to the standards set out in the 40 Recommendations of the Financial Action Task Force on Money Laundering; ...".

ANNEX C

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING FATF



1997-1998 REPORT ON MONEY LAUNDERING TYPOLOGIES

12 February 1998

FATF-IX REPORT ON MONEY LAUNDERING TYPOLOGIES

I. Introduction

1. The group of experts met in Paris on 19-20 November 1997 under the chairmanship of Mr. Pierre Fond, deputy Secretary-General of TRACFIN (*Traitement du renseignement et action contre les circuits financiers clandestins* -- Treatment of information and action against illicit financial circuits). The meeting took place at the Conference Centre of the French Ministry of the Economy, Finance and Industry in Paris. The group comprised representatives of the following FATF members: Australia, Austria, Belgium, Canada, Denmark, European Commission, Finland, France, Germany, Greece, Ireland, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. Experts from non-member international organisations with observer status, namely Interpol, the International Organization of Securities Commissions (IOSCO), the World Customs Organisation (WCO) and the United Nations International Drug Control Programme (UNDCP), also attended the meeting.

2. The purpose of the 1997-1998 typologies exercise was to provide a forum for law enforcement and regulation experts to discuss recent trends in the laundering of criminal proceeds, emerging threats and effective countermeasures. While the discussions focused principally on money laundering developments in FATF member countries, the experts also sought to pool available information on prevailing money laundering patterns in non-member countries or regions.

3. In the context of work on the more targeted typologies, the present report focuses mainly on areas which still have to be mastered, such as new methods of payment, but also on the non-financial professional activities that constituted the central subject of the 1997-1998 exercise. The report also deals with the question of laundering through fund transfer companies and presents other interesting typologies noted by the experts. The final part of the report seeks to give a picture of the laundering situation in regions of the world where FATF has few or no members.

II. Analysis of specific trends in laundering in FATF countries

(i) Present trends in money laundering

4. A number of delegations stated that there had been no really new developments since the previous exercise. Drug trafficking and financial crime continue to be the chief sources of illicit proceeds. Several members cited increased cigarette and alcohol smuggling as the main origin of capital for laundering. Others cited usury, investment and VAT fraud, false invoicing and financial fraud. A shift of some laundering activities from the traditional financial sector to non-financial professions or enterprises was noted.

5. While it would not be strictly true to say that new segments of the financial sector are being used by launderers, new developments have been observed as regards *bureaux de change* and insurance companies. Manual currency exchange operations, which formerly were used essentially at the placement stage, are now being used also at the layering stage. Where insurance is concerned, relatively complex cases involving single premium contracts have recently been discovered which reveal less rapid procedures and less liquid transactions, allowing longer-term laundering that may offer a degree of safety to criminals. This complexity and diversification of laundering techniques, also to be found in the securities and futures trading sector, underscores the need for further investigative work in these areas. The other notable development in 1997 was the surge of new payment technologies in the banking and financial networks of FATF member countries.

(ii) New payment technologies

a. Present status of new technology systems and developments since the last typologies exercise

6. Although many members stressed that there had been little innovation relative to laundering, it was generally found that the new technology systems were in a phase of steady development or even rapid expansion. In Sweden, one of the country's largest banks now has 100 000 customers with an account on the Internet, with the same 24-hour services as those offered at the counter. An increasing number of banks have their own website and some have even introduced virtual counters permitting most of the conventional banking operations: consultation of accounts, transfers, etc. In some countries (Belgium, for example) these services are at present confined to domestic transactions.

b. How may the new technology systems facilitate money laundering?

7. Although no case of laundering has been detected in this sector, the experts endeavoured to show what might be the risks posed by the new technologies. The fact that no laundering operation has been identified to date may mean that the appropriate services lack the necessary means and capability of detection or else that the new payment technologies do not carry any particular laundering risks. However, this second possibility should probably be discounted in view of several features of these technologies such as the rapidity of transaction performance, the numerous opportunities for anonymity that are offered, and the risk of a break in the audit trail and withdrawal from the traditional banking system. The experts exchanged views on these questions in regard to the following systems: electronic purses, banking on the Internet and direct (distance) banking. Most members saw more inherent danger in Internet transactions than in smart cards, although other delegations stressed the dangers of the latter.

8. The vulnerability of electronic purses would be limited by the following conditions:

- limitation of the amount of any one transaction;
- distribution of cards by issuers connected to financial institutions, and linkage to a bank account;
- restriction of payment card operations to the national territory.

9. Electronic purse systems would present a laundering risk in future if their upper limits were to be raised substantially or even removed altogether. However, some of these limits are already quite high. In the United Kingdom, most smart cards have a payment capacity of between £ 100 and £ 200 (i.e. between roughly US$ 150 and US$ 320), but a few go as high as £ 500 (about US$ 820), in which case it could easily be imagined that criminals would not hesitate to practise "smurfing".

10. Electronic purse systems also present increased risks of laundering when they can be used for cross-border transactions. This risk is very real, given that the one corporation is preparing to introduce such a system, which will certainly pose problems of international co-operation as regards jurisdictional competence and the site of legal proceedings. Finally, the dangers of laundering are evident with the development of cyberpayment systems involving direct transfer from cardholder to cardholder so that there is no audit trail.

11. The Internet sites opened by duly authorised banks are not particularly disturbing in themselves. It seems natural that banks should use this new commercial technique like other business enterprises. What is clearly a problem, however, is the opening of bank sites on the Internet in breach of banking regulations. In this case, the difficulty is to bring proceedings against the perpetrator, given the international character of the Internet and the difficulty of locating a site, which may be different from the one where the illegal practices were identified, and identifying the national law that would apply. As

yet only one case of this kind has been encountered, namely that of the Antigua-based "European Union Bank" which explicitly proposed completely anonymous investments (see also paragraph 72).

12. The new payment technologies present features very similar to those of electronic funds transfers: rapidity of execution, dematerialisation and magnitude of transactions. These features pose difficulties as regards traceability of payments and law enforcement intervention only after the event. At the same time, the new technologies could theoretically provide effective means of record keeping. In practice, all that can be established at present is the fact that the necessary adaptation of controls to combat criminal activity has not kept pace with the industrialisation of transactions.

13. Apart from banking on the Internet and electronic purse systems, delegations noted that the development of banking by telephone and of casinos on the Internet could make laundering easier. The intensive use of 24-hour telephone banking services has created a significant obstacle to investigations of laundering. Direct banking implies the establishment of a distance between the banker and his client, and hence the lessening or even disappearance of the physical contact on which the traditional conception of client identification rested. While these services clearly have practical advantages for clients in terms of flexibility, they make it more difficult to detect laundering activities since the traditional methods of supervision cannot be applied. As regards information available on the Internet, casinos in several countries offer complete anonymity to potential gamblers, the latter placing their bets by way of credit card. The risk of laundering is even more patent if the casinos in question also manage the accounts of their Internet customers.

c. Implementation of countermeasures

14. Before introducing any countermeasures, law enforcement authorities should make certain that such measures will be of a nature compatible with the real risks and the constraints imposed on financial institutions and should engage in consultations with the private sector for this purpose. If one is to avoid the emergence of a two-speed system of anti-laundering action, with the traditional banking system on the one hand and the new technology systems on the other, controls will havc to be adapted to the latter.

15. A number of countries have set up task forces on this question: in Australia, following a 1996 report by AUSTRAC (Australian Transaction Reports and Analysis Centre) to the Commonwealth Law Enforcement Board, a research group on electronic trading has been established to provide advice to the Board and Government. In Belgium, a task force on the Internet has been set up by the Minister of Justice, notably to study prevention and indictment of all forms of criminal action committed on the network. In Sweden, a government commission is currently working on various problems connected with electronic money, including money laundering, and has produced a partial report. The final report is scheduled for the end of July 1998.

16. Of the different approaches envisaged, members decided to consider how the existing laws could be adapted as opposed to the introduction of new legislation. The need to apply different policies according to type of transaction was also mentioned. Finally, the importance of international co-operation in this area was stressed.

17. In more concrete terms, particular consideration might be given to the following measures:

- making not only issuers but also distributors of instruments linked with the new technologies subject to anti-laundering legislation, given the shift of laundering away from the financial sector and the fact that the agents of these systems are not all financial institutions;

- authorisation and surveillance of issuers of new technology products, since anti-launder ing measures are better complied with when they apply to a regulated and controlled sector;

- a possible adjustment of existing anti-laundering measures, notably as regards client identification and the audit trail, so as to enable issuers of new technology products to help the competent authorities to detect the circulation of anonymous instruments of payment for criminal purposes.

(iii) Funds transfer enterprises or activities (formal and informal)

a. Brief overview of the sector

18. In most FATF countries, international funds transfers are performed essentially by the banks. However, there are other possibilities of transferring funds abroad through money remitters, who normally provide a valid and legitimate financial service. Enterprises performing this activity receive from their clients cash sums which are transferred to designated beneficiaries against payment of a commission. Money remitters traditionally serve the non-banking segment of the population, notably new immigrants, permit-holding or clandestine foreigners or any other person not having a bank account. Funds are often transferred to the least advanced regions of the world where no proper banking services exist.

19. The different operations may be classsified as follows:

- funds transfer companies possessing separate networks (like Western Union and Money Gram);
- money transfer systems connected with clandestine banks (underground banking);
- money transfers by way of the collection accounts of foreign banks (accounts opened with subsidiaries or branches, or even representative offices of foreign banks which transfer the earnings of immigrant workers to their countries of origin);
- international money orders.

b. Use of international funds transfer for laundering purposes

20. The law enforcement services of different member countries have discovered an increasing number of suspicious transactions involving money remitters. The authorities of one member estimate that this is one of the principal laundering methods used in their territory. In a member country, the average sum transferred abroad is about US$ 4 900 and these transfers are often made under false identities. In an Asian member country, a money remitter operating without authorisation from the competent ministry transferred a total of about US$ 93 million to China over a period of three years. A member has established that Colombian cartels use certain money remitters operating in its territory to launder their proceeds from drug trafficking.

21. The risks of laundering are not confined to the funds transfer networks serving ethnic groups, they may also apply to official networks like those of the postal service. For example, the authorities of a Scandinavian country have noted a steep increase in international money orders to the countries of ex-Yugoslavia. In a member country, the mail services are being used to send packages containing large cash sums and also drugs anonymously.

22. Other laundering activities through funds transfer systems involve *bureaux de change*. The authorities of a member have identified several proprietors of exchange offices and remittance services who have links with drug traffickers and receive sums from them for transfer to other parts of the world. Another member noted that remittances on behalf of ethnic groups may also go through *bureaux de change*, although performance of these notional transfers by manual exchange operations is regarded as an illegal banking activity.

23. On the whole it is considered that systems based on trust rather than on a professional and legal foundation favour anonymity and make it difficult to identify the actual recipient of funds. Another problem, mentioned by Australia, is the insufficiency of hard evidence of laundering, although numerous investigations have been opened in this sector.

c. Countermeasures in place or planned

24. The dangers of laundering in the funds transfer sector have been taken seriously by all countries. Many have already introduced a set of measures or about to do so, even though the professions or activities in question are not specifically targeted by the present FATF Recommendations. A first approach has been to bring funds transfer companies within the scope of anti-laundering legislation (as in Australia, Belgium and Germany). In the Netherlands, money remitters will be made subject to the requirement to report unusual transactions and a system of surveillance will be introduced. In Spain, the competent authorities are preparing a decree regulating the activities of offices handling international funds transfers, which are already covered by the general rules regarding prevention of laundering in the financial system. The decree will serve to tighten supervision of the activities concerned. In February 1997, the Hong Kong police published specific directives for funds transfer corporations and *bureaux de change* advising them to adopt anti-laundering measures similar to those of the banks, as regards client identification, record keeping and reporting of suspicious transactions. In a number of countries, the international postal money order services, too, are subject to the anti-laundering law (as in France).

25. In Germany, the fact that suppliers of funds transfer services are subject to the anti-laundering law makes it possible also to cover the case of foreign banks' representative offices that perform transfers. The banking supervision authorities plan to introduce supplementary measures for money remitters, such as the lowering of client identification thresholds to DM 5 000 (about US$ 2 700), the requirement to supply monthly statistics on the number of transfers and their amounts, and additional measures as regards identification record keeping. In the Netherlands identification thresholds have also been lowered, from NLG 10 000 to 5 000 (approximately US$ 4 800 to US$ 2 400). While the lowering of these thresholds is an appropriate measure, there is still the question of the effects which this may produce, notably an increase in "smurfing" operations. Consequently, it is necessary to think about ways of detecting such activities. It is also important to ensure better identification of the recipients of funds, or at least to be able to detect any convergence of transactions on a sole operator located abroad.

26. As regards transfers made by agencies of international corporations like Western Union and Money Gram, these are covered by anti-laundering law in many member countries. In Switzerland, for example, transfers made through Western Union will be subject to the new law on money laundering as of 1 April 1998, and notably to the reporting requirement. In Sweden, a constructive dialogue appears to have begun between the NFIS (National Financial Intelligence Service) and Western Union representatives. However, in some countries, the sub-agents and agents of Western Union operating through "kiosks" are not covered by the anti-laundering regulations.

27. Several members pointed out that the introduction of measures should be reinforced by action to alert the professions concerned. In the United Kingdom, the National Criminal Intelligence Service (NCIS) is seeking to make fund transmitters aware of their obligations under anti-laundering law so that more information will be forthcoming from this sector. In Hong Kong, the police services have recently made on-the-spot visits to explain the content of the directives they have issued to money changers and fund transmitters.

28. Finally, there are more specifically targeted controls like the United States GTO (Geographic Targeting Order). These orders impose, relative to the Banking Secrecy Act, stricter requirements on financial services providers as to disclosure of suspicious transactions and the keeping of records for a limited period and in a specific geographic area. A GTO of 7 August 1996 was applied to 12 money transmitters and 1 600 agents in the metropolitan area of New York, requiring them to report all cash transfers of over US$ 750 to Colombia. The initial order, valid for 60 days, was renewed six times so as

to terminate in October 1997. Its coverage was also extended to 23 licensed transmitters and about 3 500 agents. The result of the New York GTO was an immediate and spectacular reduction in the flow of drug trafficking proceeds to Colombia (down 30 per cent in volume). About 900 money transmitters ceased their activity and some of them were even arrested.

(iv) Other observed trends in laundering

a. The insurance sector

29. The written submissions and presentations made at the meeting of the group of experts revealed some diversification of laundering activities in other segments of the financial sector, like insurance. A member noted the use of single premium insurance contracts to conceal illicit income. In two other member countries, reports of suspicious activities from the insurance sector reveal the practice of early redemption of capital invested, in spite of possible penalties.

b. Money changing

30. The *bureaux de change* sector continues to be a very important link in the laundering chain: cash proceeds from drug trafficking and other criminal activities often transit through this sector. For some years now the authorities of a member have noted a shift of certain very large-scale exchange transactions from the banks to small *bureaux de change*, and this development, which is the direct consequence of the rules of vigilance introduced by the banking sector, is becoming more pronounced. Thus a report of suspicious activity from a money changer implicated two individuals who had jointly made a US dollar/local currency exchange transaction amounting to US$ 5 million. The unusual feature of this transaction was that used dollar bills were changed into local notes which were then utilised, on the same day and in the same *bureau*, to purchase unused dollar bills. In another member country an investigation revealed a case of laundering in which an exchange office had changed more than US$ 50 million at a foreign bank over a period of 13 months (see Case No. 6).

31. In an European FATF member, during the first nine months of 1997 a total of 92 actions were initiated against 289 persons having used *bureaux de change* for transactions amounting in all to about US$ 45 million. In another member country, the law enforcement services have observed a strong and growing tendency for *bureaux de change* to be used by criminal organisations. Two main techniques are reported at present: the changing of large amounts of criminal proceeds in local currency into low bulk continental currencies for physical smuggling out of the country, and electronic funds transfers to offshore centres. Underground exchange mechanisms are obviously also being widely used for money laundering purposes (see Case No. 8).

32. With regard to exchange transactions, the member countries of the Economic and Monetary Union should consider whether existing anti-money laundering provisions are appropriate to the exceptional circumstances resulting from the period of conversion of national currencies to the Euro which will start in four years.

c. Cross-border transportation of cash and electronic funds transfers

33. Hard evidence of the growth and sophistication of cross-border transportation of cash was supplied by several members (see Case No. 3). In Spain, the government is considering expanding the current obligations to declare the import of cash at the customs.

34. Two other members pointed out that electronic funds transfers feature very often in layering operations. One of the most popular techniques is simply to transfer illicit funds through several different banks in order to blur the trail to the funds' source. Another method is to make transfers from a large number of bank accounts, into which deposits have been made by "smurfing", to a principal collecting account which is often located abroad in an offshore financial centre. In this regard, the

adequacy of present anti-laundering measures can be questioned: to obtain the relevant information concerning an international electronic transfer made in one day, the investigating services have to wait an average of about two years for the results of an investigation by jurisdictional delegation.

d. The gold market

35. The FATF experts considered for the first time the posibilities of laundering in the gold market. The scale of laundering in this sector, which is not a recent development, constitutes a real threat. Gold is a very popular recourse for launderers because of the following characteristics:

-- a universally accepted medium of exchange;
-- a hedge in times of uncertainty;
-- prices set daily, hence a reasonably foreseeable value;
-- a material traded on world markets;
-- anonymity;
-- easy changeability of its forms;
-- possibility for dealers of layering transactions in order to blur the audit trail;
-- possibilities of double invoicing, false shipments and other fraudulent practices.

36. Gold is the only raw material comparable to money. Although other precious metals and diamonds are used in cases of recycling, gold is preferred by launderers. Moreover, the drug routes, especially for heroin, coincide fairly clearly with the gold routes. The "hawala" alternative banking system, which is widespread in South Asia and the Middle East, is also connected with the gold circuits. The investigating services are having the greatest difficulty in piercing this system which facilitates both currency exchange and the purchase and sale of gold.

37. Two members instanced specific legislation to combat gold market laundering. In Australia, gold traders are subject to the requirements of client identification and disclosure of transactions in excess of A$ 10 000 (about US$ 6 700). In Italy, a procedure, similar to the US Geographic Targeting Order, requires all the financial institutions in a town where gold was refined to disclose all relevant ransactions.

38. The question of laundering in the gold market most certainly needs to be examined in greater depth. It would be extremely useful to continue to study it in future typologies exercises as a specific subject, after collecting written submissions on the different regulations in force in member countries.

III. Money laundering and non-financial professions

39. For the first time FATF has made an in-depth analysis of laundering in the non-financial sector, treating this question as a special subject in the 1997-1998 typologies exercise. The method used was to assemble all the facts indicating involvement in money laundering and the magnitude of the problem, together with the existence of specific or general countermeasures, on a strictly sectoral basis.

40. Given the development of anti-laundering legislation in many countries, criminals are having increasing recourse to intermediaries other than those of the banking and financial sectors. In view of this trend, governments have started to tackle the problem. In one member country, a recent study has identified a number of professions in which laundering activities are intensively pursued (dealers in motor vehicles, boats and real estate, lawyers and accountants, lotteries, horse races and casinos). In the framework of the European Union, a high-level task force on organised crime has called for measures to be developed to shield certain vulnerable professions from influences of organised crime in general and recommends that the obligation in the money laundering Directive to report suspicions should be extended to persons and professions outside the financial sector. Article 12 of the Directive already

provides a basis for such extension, although delicate questions such as the professional secrecy of certain professions, will have to be addressed.

41. Several countries are in the process of enacting legislation to bring non-financial professions under their anti-laundering regimes. In Belgium, an extension of the scope of the Act of 11 January 1993 to bailiffs, notaries, company auditors, external auditors, real estate agents, casinos and funds transport firms is the subject of a Bill for the implementation of the government's plan of action against organised crime. In Finland, a new law on prevention and detection of laundering will require casinos, betting offices and real estate agents to identify their clients and report suspicious transactions. In Italy, the provisions of the anti-laundering Act No. 197/91 will soon be extended to companies practising activities particularly liable to be used for laundering purposes (casinos, lawyers, accountants, jewellers). In Sweden, a Bill is under consideration for the introduction of reporting requirements, but not a complete incorporation of the non-financial professions into the anti-laundering regime.

42. Even in countries where the non-financial professions are already covered by anti-laundering legislation, attempts are being made to improve existing measures. For example, in the present state of law of one member, non-financial professions are required to report to judicial authorities the facts of laundering of which they have knowledge, as opposed to simply their suspicions. This provision, which has yielded few results (about ten cases in seven years), greatly diminishes the effectiveness of anti-laundering action, for in many files it is clear that the suspicious nature of the operation may have been discovered much earlier, in particular by the real estate agents or notaries concerned. The possibility of aligning the obligations of non-financial professions connected with real estate transactions (agencies, notaries) with those of financial institutions is therefore being studied.

(i) Lawyers, notaries and acountants acting as advisers or financial intermediaries

43. Several members cited cases involving lawyers. In one member country, one of the laundering techniques used is to deposit cash in solicitors' client accounts, in several amounts under about US$ 6 700, and then use the total credit balance for a real estate investment. In another member, a recent enquiry revealed how a lawyer could use a client account to launder the proceeds from a credit fraud offence. The funds were paid into the lawyer's client account, then coverted by him into cheques drawn on a bank of another country which were subsequently cashed by a correspondent designated by the lawyer concerned.

44. In one member country, thanks to information transmitted to the public prosecutor's office in real time by a local banking establishment, the criminal investigation department was able to arrest *in flagrante delicto* a lawyer from another country who had appeared at the counter of the bank concerned to withdraw the money in his correspondent's account by way of a power of attorney in due form. Investigations with foreign authorities confirmed that the acount holder was being held in their country on charges of large-scale drug trafficking. The account holder's credit balance amounted to about US$ 600 000.

45. In one member country, a solicitor transferred funds to a colleague, explaining that they were the proceeds from a sale of assets bequeathed by an individual in his will. The second solicitor was not satisfied with this explanation and reported his suspicions. The subsequent enquiry confirmed these suspicions about the legitimacy of the purported asset transactions.

46. In one member country, a prominent attorney performed services for a whole clientele of launderers. A client with US$ 80 million, proceeds from an insurance fraud, used the lawyer to transfer the money to financial institutions in countries where there are few or no anti-laundering regulations. The attorney opened accounts in various banks under false names of individuals or corporations. The illegal funds were placed in the form of cash or cheques in banks in the member in question, then wired to the different accounts controlled by the attorney. It should be noted that because of his professional

repute the domestic banks never considered it necessary to look more closely at the nature of the transactions in question (see Case No. 4).

47. Accountants may also be involved in various cases of laundering. In one member, an accountant was recently sentenced to three years' imprisonment for laundering drug money. He had received 10 per cent commission on a total sum of about US$ 700 000 in profits of criminal origin. At the same time it has to be acknowledged that accountants can also be useful sources of information in anti-laundering action. Technically, they are among the professionals best fitted to detect the fraudulent mechanism that may underlie an unusual transaction. Accountants and auditors are very present in the business sector, and less directly in charge of their clients' interests than lawyers. In France, for example, the association of accountants, concerned about its reputation and aware of its responsibilities in combating the scourge that criminal money has become, has contacted the authorities to see what contribution it might make. Needless to say, the inclusion of accountants in the scope of anti-laundering legislation can be effective only if they become familiar with the typologies of criminal money recycling.

48. The need for relevant training of this profession, but also of lawyers and notaries, was stressed by several delegations, even in the case of countries where an anti-laundering system is already in place. In the United Kingdom, solicitors and accountants respectively have to comply with professional codes of conduct and guidelines, but to date they have made very few declarations of suspicion. In the Netherlands, notaries are required to check the identity of their clients and that their services are being used for legal purposes. A list of relevant indicators has been issued by the association of notaries. If the checks do not confirm legality, the notary must refuse to provide his services.

49. Because of their central position in the legal system applying to real estate transfers and other important transactions, and in some countries the setting up of corporations, notaries are liable to experience instances of laundering. Their involvement may range from simple acquiescence to facilitation or even active participation in the laundering operation with full knowledge of the facts. In one member country, nationals of a Central European country were reported for having, on numerous occasions, paid cash sums into the account of a notary up to a total of about US$ 700 000. Another case revealed a swindle perpetrated by a European company for the benefit of another company located in a tax haven, the deal being founded on a contract signed in due form in the presence of a notary. The sum in question amounted to about US$ 840 000.

50. The problem confronting legislators in many countries is to establish a clear distinction between the financial intermediary and advisory activities not only of notaries but also of lawyers. In Switzerland professionals offering financial services will be subject to the money laundering legislation as of 1 April 1998. They will then have two years in which to register with a self-regulatory body.

51. The examples cited in this section of the report, both as to cases and as regards countermeasures, are applicable only to the individual countries concerned, since the definitions of the legal professions vary greatly from one country to another. It would therefore be useful to have a complete picture of the anti-laundering legislations applicable in the different member countres, bearing in mind that the responses to the new annual self-assessment questionnaires should also yield some interesting information in this regard.

(ii) Shell corporations and company formation enterprises

52. Shell corporations, in countries where these exist, continue to be a widely used tool for recycling illegal money (see Case No. 2). In this connection two delegations provided a good example of a case that also involved a company supplying secretarial services (see Case No. 5).

53. The role that company formation enterprises might play was mentioned by the United Kingdom. NCIS has therefore recently published a set of guidelines for such enterprises, some of which are covered by the anti-laundering regulations.

(iii) Casinos and gambling

54. In this other part of the non-financial sector, cases of laundering abound. In one member country, methods reported during the past year include the purchase and repayment of gambling tokens in multiple amounts of less than about US$ 6 700, the receipt by casino clients of winner's cheques made out in the name of third persons, and the use of tokens for purchases of goods and services and for drug purchases. Other delegations cited different cases involving casinos, gaming businesses and various lotteries, including horse-racing. These entities provide ample opportunities for laundering, given the amount of cash that changes hands there.

55. Casinos are the site of the first stage in the laundering process, i.e. converting the funds to be laundered from banknotes (circulating currency) to cheques (bank money). In practice the method is to buy chips with cash and then request repayment by cheque drawn on the casino's account. The system can be made more opaque by using a chain of casinos with establishments in different countries. Rather than request repayment by cheque in the casino where the chips were purchased with cash, the gambler says that he will be travelling to another country in which the casino chain has an establishment, asks for his credit to be made available there and withdraws it in the form of a cheque in due course.

56. Gaming businesses and lotteries, too, are being used increasingly by launderers. One member has evidence of multiple financial transactions made by the same person by way of cheques drawn on gambling agencies: loto, horse-racing and also casinos. This suggests that circuits have been set up to organise systematic buy-back of winning tickets from their legitimate holders. Another laundering technique connected with horse-racing and gaming has emerged. In this case the person will actually gamble the money to be laundered, but in such a way as to be reasonably sure of ultimately more or less recovering his stake in the form of cheques issued by the gambling or betting agency and corresponding to perfectly verifiable winnings from gaming. This method is much more reliable than the previous one, since the police investigation service, once it has verified the reality of the gaming operation and the person's winnings, will in principle have a great deal of trouble in going further and identifying the source of the money staked.

57. Countermeasures specific to the gambling sector, mainly for casinos, have been enacted by some FATF members. The closing of casinos in Turkey, which took effect on 10 February 1998, is anticipated by that country to contribute to anti-money laundering efforts as well. In the Netherlands, casinos belong to a public establishment named Casinos of Holland. Casinos are covered by the anti-laundering legislation, and only winnings from gambling are accepted for electronic transfer to a bank account. This arrangement might prove effective in countries where casinos offer a wide range of financial services, as in the United States. Other examples of countermeasures are to be found in the United Kingdom where emphasis is being placed on the importance of client identification, the concept of gamblers' "profiles" and the need to involve all the authorities concerned. Since the gambling sector is not covered by anti-laundering regulations, a code of conduct for the gaming profession has been adopted.

58. In the United States, comments have been requested on a new declaration form for casinos entitled SARC (Suspicious Activity Report by Casinos), which is already in use in the State of Nevada. In Belgium the introduction of a requirement for casinos to report to the CTIF (*Cellule de Traitement des Informations Financières* -- financial information processing cell) is envisaged. Casinos and the gambling sector in general should therefore constitute a genuine subject of concern for FATF, given that it is an expanding industry which is central to the development of tourism in many countries. Gambling is also becoming increasingly international in scale. Finally, the consequences of the growth of non-casino types of gambling and their development on the Internet (e.g. Bingonet) should be examined very carefully.

(iv) Other non-financial professions, including real estate agents and sellers of high-value objects

59. The real estate sector is now fully within the sphere of money laundering activities. Investment of illicit capital in real estate is a classic and proven method of laundering dirty money, particularly in FATF countries enjoying political, economic and monetary stability. Laundering may be effected either by way of chain transactions in real estate to cloak the illicit source of funds, or by investment in tourist or recreational real estate complexes which lend an appearance of legality.

60. Numerous cases of laundering were cited by the experts. One of the methods used is to buy and sell properties under false names. In a recent case presented by one member, two criminals were arrested for laundering about US$ 270 000 through a real estate agency. One member was apprised of an interesting case involving a real estate agent located in an offshore centre and a notary (see Case No. 1). In another member, many suspicious real estate transactions take place in the south and involve amounts of the order of several million francs. In the Netherlands, thanks to the vigilance of banks, unusual transactions involving real estate agents have been reported to the MOT (Office for reports of unusual transactions). The government of that country is currently consulting the profession on its possible contribution to anti-laundering action.

61. In a Scandinavian country, a recent case was based on information concerning a previously convicted drug trafficker who had made several investments in real estate and was planning to buy a hotel. An assessment of his financial situation did not reveal the source of his income. Following his arrest and further investigations, he was sentenced for drug trafficking and money laundering to seven and a half years' imprisonment and about US$ 4,4 million was confiscated (see Case No. 7). In another Scandinavian country, despite a strict system of recording all real estate transactions, the authorities have identified a few cases involving low-interest loans of suspect origin obtained abroad for purposes of investment in that country.

62. Finally, sellers of high-value objects like artworks are unquestionably a significant presence in laundering activities. Within the European Union, systems of national heritage protection have been adopted, particularly in France where exports of cultural goods require prior authorisation by the Ministry of Culture. In the previously mentioned case concerning real estate, another part of the drug profits had been laundered by the director of a art museum from another country, who received about US$ 15 000 for producing false certificates of sale of art objects.

63. Another case, reported by a member, concerns the use of a rather special technique whereby a financial swindler on a international scale made one of his companies available to a major trafficker and launderer seeking to establish a source of funds. The latter would make periodic cash remittances to the money manager/swindler, who paid them into his company's accounts. Transfers were immediately made to Monaco and to other banking establishments in this member, in company accounts of which the launderer was the economic beneficiary. The purpose put forward to justify these transfers was the purchase of paintings by a master artist (Goya), either as payments on account or as settlements. The paintings were in fact fakes and, moreover, were never shipped. The payments in question were for amounts on the order of about US$ 1 million. With this technique it is obviously possible to launder extremely large amounts of illicit money.

64. As regards these latter categories of professions in the non-financial sector, existing legislation appears even more disparate than for the legal professions or gambling activities. Where reporting requirements exist, very few disclosures are forthcoming from these professionals, as pointed out by several delegations. This is another area where intensive efforts will have to be made to alert professionals to suspicious or unusual transactions through appropriate education.

IV. Assessment of world trends in money laundering

65. Money laundering is obviously not a problem restricted to FATF countries. Thanks to the implementation of countermeasures in those countries, the experts have been able to make the relatively detailed analyses that figure in the preceding sections of this report. The information available on money laundering in non-member countries is much less comprehensive; consequently, the following assessment by FATF of world trends in laundering does not claim to be exhaustive.

(i) Asia/Pacific

66. Sources of information on laundering activities in this vast region of the world are fairly scarce. The situation will be considerably improved when Interpol, in co-operation with the US agency FinCEN (Financial Crimes Enforcement Network), produces its reports on individual Asian countries. It should be noted that the Interpol group FOPAC (*Fonds provenant des activités criminelles* -- proceeds from criminal activities) has already produced similar reports on the Central and Eastern European Countries, and that the second series on Asian countries has been given high priority.

67. Two delegations considered that there were no really new laundering developments in this part of the world. The main factors observed in previous typologies exercises are still present. Thus in South Asia and India money laundering is still linked with drug trafficking and is undoubtedly facilitated by the parallel remittance systems known as "hawala" and "hundi".

68. In South-East Asia the countries that seem to warrant particular attention are Indonesia and Malaysia. Given the absence of appropriate legislation and the regime of strict bank secrecy in Indonesia, money laundering is only part of the financial crime that prevails there essentially in the shape of large-scale fraud and corruption. Several other countries in the region, notably Malaysia, offer numerous features attractive to launderers: provision of a wide range of financial services, facilities for setting up trust companies and offshore structures. Bank fraud is still a very important source of money for laundering.

69. In the Pacific region, Vanuatu is featuring increasingly in the laundering circuits. The offshore legislation in place there has created a favourable climate for laundering and the country's financial institutions have been cited in several cases.

70. Generally speaking, it would clearly be desirable to have more information on the Asia/Pacific region. FATF members therefore greatly welcomed the fact that the region's new anti-laundering group, set up at a symposium on money laundering in Asia and the Pacific at Bangkok in March 1997, would shortly be conducting its own typologies exercise. This initiative is a follow-up to the earlier workshops on Disposal of Proceeds of Crime, Money Laundering Methods organised by the FATF Asia Secretariat and Interpol in Hong Kong in 1995 and 1996.

(ii) Central America, South America and the Caribbean Basin

71. All these parts of the world continue to attract money laundering activities. As regards the Caribbean, FATF members welcomed the activities conducted by the Caribbean Financial Action Task Force (CFATF) in respect of typologies. The approach used by the latter is somewhat different from that of FATF, but it should nevertheless give rise to some very useful and interesting work, as regards both analysis of regional trends and assessment of the countermeasures to be adopted. The CFATF typologies exercise is phased over a number of years. Since February 1997 the CFATF experts have studied the forms of money laundering in domestic financial institutions and in the gambling sector. Future meetings will address the following themes: offshore financial establishments and international business corporations, financial institutions and cybermoney.

72. Laundering in the Caribbean region continues to be a serious problem and appears to concern the following countries in particular: Antigua, the Dominican Republic and St Vincent and the Grenadines. Suspect operations have also been detected in the French overseas departments, particularly in the areas of exchange and gaming. Russian organised crime operating out of Miami and Puerto Rico continues to be active in forming front companies all over the region in order to launder illicit profits. A case in point here is the European Union Bank set up in Antigua and famed as the first offshore bank operating via the Internet. The two Russian founders absconded with the deposits and subsequently the bank failed and was closed down in August 1997. Free trade zones, including those in Aruba and Panama, continue to be a target for money launderers using the black market peso exchange system to purchase and smuggle goods into Colombia (see Case No. 8). The Aruban and Panamanian governments are to be commended for taking aggressive steps to address this difficult problem.

73. The Dominican Republic and Jamaica were likewise mentioned in connection with money laundering circuits. In the United States, Dominican launderers use fund transfer companies to send sums not exceeding US$ 10 000 to the Dominican Republic under false names. Consequently the US Department of the Treasury this year issued a Geographic Targeting Order which requires the reporting of all transfers of over US$ 750 from Puerto Rico and the New York Metropolitain area to the Dominican Republic. In Jamaica, a recent case of money laundering concerned an offshore bookmaking operation by telephone for a total amount of several million dollars. Where no specific measures regarding cross-border currency movements exist, cash transportation seems to be a common method of laundering.

74. The nations of Latin America also continue to be affected by laundering of illegal funds, essentially the proceeds from drug trafficking. In Mexico numerous anti-laundering measures have been enacted in the past year. Banks are now required to report suspicious transactions to a central agency for financial information. In spite of these efforts, money laundering is still a problem to be taken very seriously, especially now that the Mexican drug cartels have parted company with their Colombian counterparts and have acquired some predominance in the region. One of the most favoured techniques continues to be outbound currency smuggling, along with electronic transfers, Mexican bank drafts and the "parallel" peso exchange market. Corruption remains the chief impediment to Mexico's anti-laundering efforts.

75. Another Central American country experiencing a growth of laundering activities is Costa Rica, notably by way of large-scale currency smuggling and investment by Colombian cartels in the tourist real estate sector. In Guatemala and Honduras laundering potential continues to increase in the absence of appropriate legislation. In Panama the target of launderers remains the Colon Free Zone. It should be pointed out, however, that anti-laundering measures applicable to the banking sector have been extended to the Zone. In Colombia, billions of dollars in drug money are being laundered through the "parallel" peso exchange market, which in fact is run by drug traffickers (see Case No. 8).

76. Within the framework of OAS (Organization of American States) the Inter-American Drug Abuse Control Commission (CICAD) has decided to launch its own typologies exercise through its group of experts on money laundering. FATF members welcomed this initiative, which will cover nearly all the countries of South America. Many countries in that region have recently introduced anti-laundering legislation following the Summit of Americas Ministerial Conference of December 1995. Despite these efforts, drug trafficking and money laundering are still major problems in this part of the world. It is therefore encouraging to see that the next Summit of Americas, to take place in Santiago, Chile in April 1998, will again address the subject of money laundering as a priority.

(iii) Middle East and Africa

77. In the absence of proper regional anti-money laundering groups, information on laundering in these areas is extremely limited. But numerous factors which assist laundering are present in the Gulf States with the international finance centres in Bahrain and the United Arab Emirates (in particular Abu Dhabi and Dubai), the hawala "banking" system and free trade zones. It should be noted, however, that

the Gulf Co-operation Council (GCC) has recently launched an evaluation of the anti-laundering measures adopted by its members (United Arab Emirates, Oman, Saudi Arabia, Qatar, Bahrain and Kuwait) which will provide a picture of the status of legislation in the region.

78. In the Near East the lack of anti-laundering legislation in Lebanon remains a matter of significant concern to FATF. It is hoped that a bill will soon be passed into law in Israel, where the authorities are facing general problems with organised crime and need to tackle the dangers of laundering in the diamond industry. In Cyprus the authorities have vigorously built up a comprehensive anti-laundering scheme since relevant legislation was passed in April 1996, and a unit has been established to receive suspicious transaction reports from banks. FATF experts visited Nicosia in September 1997 and noted the resolute and praiseworthy efforts being made by the Cypriot authorities to counter money laundering even if the name of Cyprus still appears in cases of laundering transactions at the layering stage.

79. Crime groups are increasingly turning to sub-Saharan Africa to conduct their activities, including money laundering. A few countries have begun to respond by introducing legislation, but significant obstacles have still to be overcome, notably the lack of resources available to operational services in Africa. One trend observed in West Africa concerns the use by organised crime of bank accounts of commercial businesses. Illicit funds can be moved via undercover banking systems and evade exchange control regulations. All FATF members acknowledge that the chief problem in West Africa continues to be fraud by Nigerian organised crime. It was accepted that this problem, which has been going on for too long, would merit appropriate international collective action. Nigerian organised crime is also active in South Africa, which is progressively becoming an entry point to the rest of the continent for crime groups.

(iv) Central and Eastern Europe

80. The East European countries continue to be a significant and indeed growing concern for the European members of FATF. The greatest difficulty concerning funds connected with individuals or companies in Central and Eastern European countries is in clarifying their source, which is very often impossible. The frequent use by some CEEC nationals of expertly forged identity papers, designed to get round strict application of the principle of customer identification by financial institutions, was noted. In addition, transcription from Cyrillic to Roman is often used to change identities, or provide multiple identities. Cases of dual nationality (Russian/Greek or Russian/Israeli, for example) are frequent, and hold similar potential for disguising true identity. Armenian or Georgian nationals claim Greek origins. The most significant problem in transactions with Russia is that the true beneficiary is not known.

81. As in previous years, the experts noted numerous cases involving Russian organised crime and from other members of the Commonwealth of Independent States. Most of the shell companies operating in one member are carrying on quite legitimate business, but their finance comes from fraud and criminal activities in Eastern Europe. A competent unit of this country, which has detected growing sophistication at the layering stage, with substantial use of offshore companies, is going to follow developments in this area very closely from 1998. The refinement of the methods used by organised Russian crime groups was also noted by the police of one member in a case involving letters of credit issued by a Russian bank for a total of US$ 100 million. Very substantial sums are involved in cases relating to nationals of Central and Eastern European countries or to CEEC-related financial transactions. One case detected in another member concerned US$ 13 million overall.

82. But there are other problem countries as well, notably the countries of the former Yugoslavia, as was noted by one member, which considers this to be the most serious problem that it comes across, in particular in relation to drug trafficking. In one member, a case covering a wide range of currencies (the equivalent of around US$ 300 000 involved Serbian immigrant workers. In Croatia, the authorities face a significant problem with the establishment of organised groups specialising in particular types of crime. These structures provide links with crime groups in Italy or Germany, and those operating in Russia, Serbia and Bosnia.

83. In the Black Sea region, only two countries (Greece and Turkey) belong to FATF. Their closeness to fifteen countries of the former Soviet Union raises a particular problem with regard to laundering. Another problem encountered by the banks of a member country has been massive inflows of funds from Albania, linked to the pyramid savings scandal. Investigations following the suspicious transaction reports have shown that considerable amounts in cash, around US$ 20 million, were deposited at banks in a neighbouring country during the summer of 1997. This is a problem which affects several FATF members. In addition, after the deliberate failures of many banks in Bulgaria, triggered by their owners' corruption, they were bought up by groups of white-collar criminals who could then help themselves to the bank assets.

84. Some progress has nonetheless been made in adopting and implementing counter-measures over the past year. The Czech Republic, Slovakia, Hungary and Slovenia have developed anti-laundering programmes, and now have financial intelligence units in operation. But the anti-money laundering Bill tabled in the Russian Parliament in late 1996 has still not been passed.

85. In the summer of 1997 the Central Bank of the Russian Federation issued guidelines to banks on customer identification and the prevention of money laundering. Together with FATF it organised an international seminar on money laundering in St. Petersburg in October 1997. But these efforts will only yield really practical results when the anti-laundering obligations of the financial sector are spelt out in law.

86. Reference should finally be made to a vital recent initiative by the Council of Europe, which launched its programme to evaluate anti-laundering measures in those of its members which do not belong to FATF. The countries in question are not all in Central and Eastern Europe, but the programme should give a considerable boost to enhancing or introducing anti-laundering legislation in that part of the world over the coming years.

V. Conclusions

87. The November 1997 meeting of the group of experts on typologies was marked by a new form of discussion, with in-depth treatment of more targeted topics than in previous exercises. Since the classic mechanisms for laundering are now well identified, the purpose will in future be to survey the new ground being broken by imaginative launderers, and to demonstrate how and why given new laundering practices are being developed. In short, the FATF's strategy needs to be tailored to the emergence of new areas which are not yet fully mapped: electronic money and new-technology forms of payment, non-financial professions, the insurance sector and stock exchange dealers.

88. In addition to laundering via non-financial professions and companies, which is the main subject for the FATF-IX typology exercise, the experts also examined issues relating to companies specialising in international money transfers, and new-technology means of payment. These are both essential areas that FATF needs to understand more fully in order to develop effective counter-measures. With regard to new technology, much work still has to be done before all the related laundering dangers are clearly identified and before any possible specific counter-measures can be considered. Even at present, the speed at which transactions are performed in this sector, admittedly an advance in itself, poses grave threats to the adequacy of the traditional anti-laundering methods to the systems of new payment technologies. As a result, this topic is likely to recur systematically at forthcoming typology meetings. With regard to companies specialising in international money transfers, consideration and action are both much further advanced, to judge from the scale of counter-measures already in place in many FATF member countries. This is in fact an area where exchanges of information on current regulations, and of practical experience, can no doubt be of benefit to those countries which have not yet really tackled the problem.

89. Among other typologies of interest, particular reference should be made to the gold market. While this is not a new topic, discussions showed that it was an area where FATF should also expend

energy in order to identify the problems more clearly. It is accordingly planned to make this a priority item for one of the forthcoming typology exercises. In any case, although FATF has already devoted considerable attention to sectors such as insurance or manual currency exchange, the involvement of both in money laundering is still clearly on the increase. With regard to the exchange bureaux sector, it is clear that further consideration must be given to the consequences of the conversion of European currencies into Euro.

90. Last, the survey of laundering trends in non-Member countries again proved most instructive. Although progress is being made in implementing anti-laundering measures outside the FATF members, much still remains to be done to mobilise a fair number of countries which remain somewhat passive and complacent about the financial, economic, political and social dangers posed by laundering.

12 February 1998

ANNEXES TO THE 1997-1998 FATF REPORT ON MONEY LAUNDERING TYPOLOGIES

Selected cases of money laundering

Case no. 1

Real Estate agents and Notaries

Facts

A real estate agent in a tax haven jurisdiction opened an account at a bank in a European country. The account was used to encash a cheque drawn by a foreign notary. Once the cheque had cleared, part of the funds were withdrawn as cash, part were re-transferred back to the original jurisdiction, and the balance was credited to the account of a notary in that country and used to purchase real property there.

The information that was acquired from the police authorities showed that the different persons involved in the transactions had been involved in fraud. Although the system put in place by the perpetrators appeared to be legal, inquiries showed that the account opened at the bank was only used as a temporary transfer account for the laundering of the proceeds of financial crime.

Results

The financial intelligence unit transferred the case to the judicial authorities, on the basis of the serious indications of money laundering.

Lessons

1. This case shows the need to be vigilant when considering possible money laundering cases, as even transactions which initially do not appear to be particularly suspicious can involve money laundering.

2. It also shows the importance of the “know your customer principle”, since the criminal past of the persons involved in this case was the only indicator which led to the discovery that the transactions in this case involved money laundering.

Case no. 2

Shell Corporations

Facts

A drug trafficker used drug trafficking proceeds to purchase a property of which part was paid in cash and the remainder was obtained through a mortgage. He then sold the property to a shell corporation, which he controlled, for a nominal sum. The corporation then sold the property to an innocent third party for the original purchase price. By this means the drug trafficker concealed his proceeds of crime in a shell corporation, and thereby attempted to disguise the origin of the original purchase funds.

Results

The accused pled guilty and an order of forfeiture was granted. The property which was part of the money laundering scheme is being disposed of by the authorities.

Lessons

1. The need to carefully trace the ownership history of a property, in order to identify possible links between owners and any suspicious transfers that may indicate attempts to commingle assets.

2. The need for enforcement agencies to be familiar with the general rules and practice regarding the purchase of property in relevant jurisdictions, and the need to be aware that transfers involving nominal amounts can be easily structured in some jurisdictions.

Case no. 3

Cross border cash

Facts

Three suspicious transaction reports were received relating to a number of transactions which were carried out at Danish banks whereby large amounts of money were deposited into accounts and then withdrawn shortly afterwards as cash. The first report was received in August 1994, and concerned an account held by Mr. X. Upon initial investigation, the subjects of the reports (X, Y and Z) were not known in police databases as being connected to drugs or any other criminal activity. However further investigation showed that X had imported more than 3 tonnes of hashish into Denmark over a 9 year period. Y had assisted him on one occasion, whilst Z had assisted in laundering the money.

Most of the money was transported by Z as cash from Denmark to Luxembourg where X and Z held 16 accounts at different banks, or to Spain and subsequently Gibraltar, where they held 25 accounts. The receipts from the Danish banks for the withdrawn money were used as documentation to prove the legal origin of the money, when the money was deposited into banks in Gibraltar and Luxembourg. It turned out that sometimes the same receipt was used at several banks so that more cash could be deposited as ”legal” than had actually been through the Danish bank accounts.

Results

X and Y were arrested, prosecuted and convicted for drug trafficking offences and received sentences of six and two years imprisonment respectively. A confiscation order for the equivalent of US$ 6 million was made against X. Z was convicted of drug money laundering involving US$ 1.3 million, and was sentenced to one year nine months imprisonment.

Lessons

1. Financial institutions should not accept proof of deposit to a bank account as being equivalent to proof of a legitimate origin.

2. Carrying illegal proceeds as cash across national borders remains an important method of money laundering.

Case no. 4

Lawyers

Facts

A prominent attorney operated a money laundering network which used sixteen domestic and international financial institutions, many of which were in offshore jurisdictions. The majority of his clients were law abiding citizens, however a number of clients were engaged in various types of fraud and tax evasion, and one client had committed an US$ 80 million insurance fraud. He charged his clients a flat fee to launder their money and to set up annuity packages to hide the laundering activity. In the event there were to be any inquiries by regulators or law enforcement officials, the attorney was prepared to give the appearance of legitimacy to any withdrawals from the "annuities".

One of the methods of laundering was for him to transfer funds from a client into one of his general accounts in the Caribbean. This account was linked to the attorney in name only, and he used it to commingle various client funds, before moving portions of the funds accumulated in the general account via wire transfers to accounts in other countries in the Caribbean. When a client needed funds, they could be transferred from these accounts to a U.S. account in the attorney's name or the client's name. The attorney indicated to his clients that they could "hide" behind the attorney-client privilege if they were ever investigated.

Another method of laundering funds was through the use of credit cards. He arranged for credit cards in false names to be issued to his clients, and the credit card issuer was not aware of the true identity of the individuals issued the cards. When funds were needed the client could use the credit card to make cash withdrawals at any automated teller machine in the United States. Once a month the Caribbean bank would debit the attorney's account in order to satisfy the charges incurred by his clients. The attorney knew the recipients of the credit cards.

Results

The attorney pleaded guilty to money laundering.

Lessons

1. Banks and their employees should be alert to "layered" wire transfers which utilise instructions such as "for further credit to". This may occur more frequently with correspondent accounts of "offshore banks". Suspicious transactions can then be identified and reported.

2. Banks should utilise "know your customer" requirements when issuing credit cards. In this case, the banks were issuing the credit cards to the attorney for further issuance to his clients.

3. Investigators should be aware that in a number of countries lawyer/attorney-client privilege is not applicable if the lawyer/attorney and his client were directly involved in criminal activity, and they should consult prosecutors if such an issue arises.

Case no. 5

Shell corporations and secretarial companies

Facts

During 1995/1996 financial institutions in a European country made suspicious transaction reports to the financial intelligence unit which receives such reports. The reports identified large cash deposits made to the banks which were exchanged for bank drafts made payable to a shell corporation based and operated from an Asian jurisdiction. The reports identified approximately US$ 1.6 million being transferred in this way to an account held by the shell corporation at a financial institution in the Asian jurisdiction.

At the same time police had been investigating a group in that country which were involved in importing drugs. In 1997 police managed to arrest several persons in the group, including the principal, who controlled the company in the Asian jurisdiction. They were charged with conspiring to import a large amount of cannabis. A financial investigation showed that the principal had made sizeable profits, and a large percentage of this has been traced and restrained. A total of approximately US$ 2 million was sent from the European country to the Asian jurisdiction, and subsequently transferred back to bank accounts in Europe, where it is now restrained.

Two methods were used to launder the money. The principal purchased a shell company in the Asian jurisdiction which was operated there by a secretarial company on his instructions. The shell company opened a bank account, which was used to receive cashiers orders and bank drafts which had been purchased for cash in the country of origin. The principal was also assisted by another person who controlled (through the same secretarial company) several companies, which were operated for both legitimate reasons and otherwise. This person laundered part of the proceeds by sending the funds on to several other jurisdictions, and used non-face to face banking (computer instructions from the original country) to do so.

Results

Seven persons including the principal are awaiting trial in the European country on charges of drug trafficking, and the principal and three other persons face money laundering charges.

Lessons

1. It shows how desirable and easy it is for criminals (even if not part of international organised crime) to use corporate entities in other jurisdictions, and to transfer illegal proceeds through several other jurisdictions in the hope of disguising the origin of the money.

2. It demonstrates the ease with which company incorporation services can be obtained, and shows that many of the companies which sell shelf/shell companies, as well as the secretarial companies which operate them, are not likely to be concerned about the purpose for which the shell company is used.

3. Highlights the need for financial institutions to have a system which identifies suspicious transactions not just at the front counter, but also for non-face to face transactions such as occurred in this case.

4. The length of time it can take to conduct international financial investigations and to trace the proceeds of crime transferred through several jurisdictions, and the consequent risk that the funds will be dissipated.

Case no. 6

Bureaux de change

Facts

A bureau de change ('The Counter') had been doing business in a small town near the German border for a number of years when exchange offices became regulated, and it became subject to obligations to prevent money laundering. The Counter often had a surplus of bank notes with a high denomination, and the owner (Peter) knew these notes were not popular and therefore had them exchanged into smaller denomination notes at a nearby bank. Prior to the legislation taking effect persons acting on behalf of The Counter regularly exchanged amounts in excess of the equivalent to US$ 50 000, but immediately after the legislation took effect the transactions were reduced to amounts of US$ 15 000 to US$ 30,000 per transaction. The employees of the bank branch soon noticed the dubious nature of the exchanges which did not have any sound economic reason, and the transaction were reported.

Peter had a record with the police relating to fencing and dealing in soft drugs, and because of this he transferred the ownership of The Counter to a new owner with no police record (Andre). Andre reports The Counter to the Central Bank as an exchange office and is accepted on a temporary basis. The financial intelligence unit consults various police files and establishes that the police have been observing this exchange office for some time. The suspect transactions are passed on to the crime squad in the town where The Counter has its office, and it starts an investigation. A few months later, the crime squad arrests Andre, house searches are made, expensive objects and an amount equivalent to more than US$ 250 000 in cash are seized. The records of The Counter show that many transactions were kept out of the official books and records. For example, over a period of thirteen months The Counter changed the equivalent of more than US$ 50 million at a foreign bank without registering these exchange transactions in the official books and records. The investigation showed that The Counter and its owners were working with a group of drug traffickers, which used the exchange office to launder their proceeds, and this formed a substantial part of the turnover of the business.

Results

The drug traffickers were prosecuted and convicted and are now serving long prison sentences. Andre was sentenced to six years in prison for laundering the proceeds of crime and forgery. Peter moved abroad with his family. A separate legal action is still pending to take away Andre's profits, the confiscated objects and the cash found. The Counter has been closed and its registration as an exchange office was refused.

Lessons

The need for banks and large, legitimate bureaux de change to pay attention to their business relations with smaller bureaux, particularly when supplying or exchanging currency with them.

Case no. 7

Lawyers, real estate

Facts

The financial intelligence unit received information that a previously convicted drug trafficker had made several investments in real estate and was planing to buy a hotel. An assessment of his financial situation did not reveal any legal source of income, and he was subsequently arrested and charged with an offence of money laundering. Further investigation substantiated the charge that part of the invested funds were proceeds of his own drug trafficking. He was charged with substantive drug trafficking, drug money laundering and other offences.

In the same case the criminal's lawyer received the equivalent of approximately US$ 70 000 cash from his client, placed this money in his client's bank account and later made payments and investments on the client's instructions. He was charged with negligent money laundering in relation to these transactions. Another part of the drug proceeds was laundered by a director of an art museum in a foreign country who received US$ 15 000 for producing forged documents for the sale of artworks which never took place.

Results

The drug trafficker was convicted of drug trafficking, was sentenced to seven and a half years imprisonment, and a confiscation order was made for US$ 450 000. The lawyer was convicted and sentenced to 10 months imprisonment. The art museum director could not be prosecuted as there was insufficient evidence that he knew the money was the proceeds of drug trafficking, but he has accepted a writ to confiscate his proceeds.

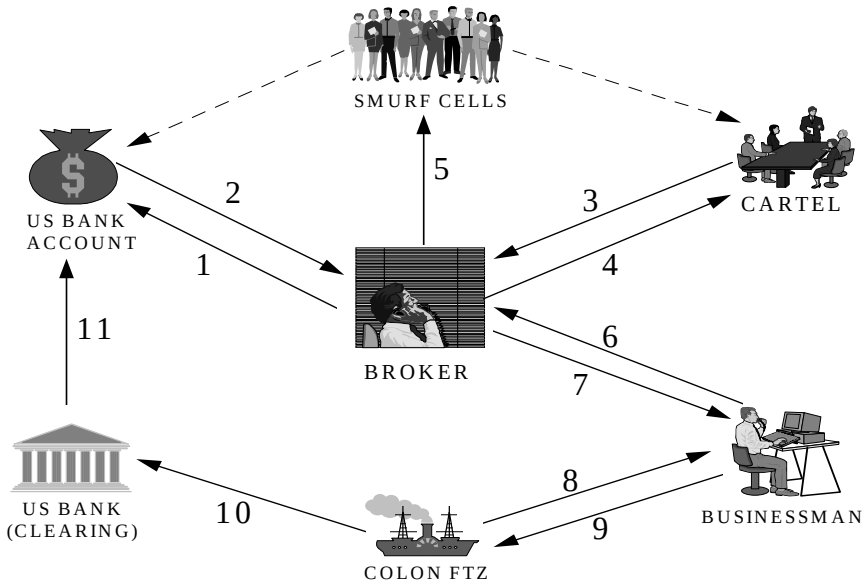
Lessons

1. The purchase of real estate is commonly used as part of the last stage of money laundering (integration). Such a purchase offers the criminal an investment which gives the appearance of financial stability, and the purchase of a hotel offers particular advantages, as it is often a cash intensive business.

2. The value of a money laundering offence with a lower scienter or mens rea requirement is shown in the prosecution of the lawyer in this case. There was insufficient evidence to prove that the lawyer knew the money was illegal drug proceeds, but sufficient evidence to show that he "should have known" on the facts available to him.

Case no. 8

Example of widely used money laundering technique - Colombian Black Market Peso Exchange, Casa de cambio, money laundering through trade, use of "shell accounts"



Drug traffickers in the U.S. collect and stockpile cash from illegal drug sales in "stash houses" located throughout the U.S. and this creates a logistical problem for the traffickers. The solution is as follows:

1. Black market money brokers in Colombia direct Colombians visiting or residing in the U.S. to open personal cheque accounts at U.S. banks, and deposit minimal amounts.

2. Cheques on these accounts are signed in blank by the customers and given to the brokers who pay them US$200-400 for each account. The brokers keep a stock of signed cheques on these "shell" U.S. accounts.

3. Colombian drug cartels sell their stockpiled cash at a parallel or "discounted" exchange rate to the Colombian money brokers in exchange for pesos which are paid in Columbia.

4. The brokers purchase the dollars at the discounted rate and the cartels lose a percentage of their profits but avoid the risks of laundering their own drug money.

5. Once the drug money is purchased, the broker directs his network *smurfs* to pick up the cash, and structure deposits into the various "shell" cheque accounts.

6. The broker then offers to sell cheques drawn on these accounts to legitimate Colombian businessmen (who need U.S. dollars to conduct international trade) at a "parallel" exchange rate.

7. The broker fills in the dollar amount on the signed cheque, but leaves the name of the payee blank. The broker also stamps his symbol on the cheque as a means to guarantee his payment on the cheque in the event there are ever insufficient funds in the "shell" checking account.

8. The businessman can then fill in the payees name when he uses the signed cheque as a U.S. dollar instrument to purchase goods (perfume, gold, etc.) in international markets such as Free Trade Zones.

9. The businessman then ships or smuggles the goods into Colombia.

10. The Free Trade Zone distributor, who is often a knowing participant in the black market exchange process, forwards the cheque to his U.S. bank account or it may even clear through his local bank account.

11. Once cleared, the cheque account is debited, and the distributor's U.S. account is credited.

Through this scheme:

Drug cartels in Colombia receive their profits from the U.S. drug trade in Columbia, without having the normal expenses of money laundering. The brokers make a profit on the "discounted" purchase of U.S. dollars from the drug cartels and a second profit on the subsequent sale of the dollars to Colombian businessmen at the "parallel exchange rate." The businessmen save money by exchanging their pesos for U.S. dollars on the "parallel" exchange market, and avoiding government scrutiny and taxes.

For more information about the Colombian Black Market Peso Exchange Process, visit the FinCEN Home Page at Http://www.ustreas.gov/treasury/bureaus/fincen. This information can be found in the advisory section.

FATF Secretariat, OECD
2, rue André-Pascal
75775 Paris Cedex 16, France

Tel: 33 (0)1 45 24 79 45
Fax: 33 (0)1 45 24 16 08
e-mail: fatf.contact@oecd.org

ANNEX D

FATF-IX SELF-ASSESSMENT SURVEY
COMPLIANCE WITH MANDATORY RECOMMENDATIONS ON LEGAL ISSUES

Recommendation No.	Members in compliance	Members in partial compliance	Other
1	23 (20)	-- (--)	3 (6)
2	25 (25)	1 (1)	-- (--)
3 et 34	23 (23)	2 (2)	1 (1)
4	23 (23)	3 (3)	-- (--)
5	26 (26)	-- (--)	-- (--)
7	21 (21)	5 (5)	-- (--)
32	26 (26)	-- (--)	-- (--)
33	20 (22)	2 (--)	4 (4)
36	23 (23)	3 (3)	-- (--)
37	23 (23)	3 (3)	-- (--)
38	18 (17)	5 (6)	3 (3)
39	19 (19)	-- (--)	7 (7)
40	23 (23)	2 (2)	1 (1)

Note

The figures in parenthesis indicate the number of members in the category in the 1996-1997 FATF-VIII survey.

FATF-IX SELF-ASSESSMENT SURVEY

COMPLIANCE WITH THE FORTY RECOMMENDATIONS ON FINANCIAL ISSUES

Recommendation		Members in Compliance	Members in Partial Compliance	Other
8 [n/a for 12 members]		12 (9)	2 (2)	-- (4)
9 [n/a for 4 members]		21 (18)	-- (1)	1 (3)
10	Banks	24 (24)	2 (2)	-- (--)
	NBFIs	20 (21)	6 (5)	-- (--)
11	Banks	23 (23)	1 (1)	2 (2)
	NBFI	22 (22)	1 (1)	3 (3)
12	Banks	26 (26)	-- (--)	-- (--)
	NBFIs	23 (23)	3 (3)	-- (--)
13		25 (15)	-- (11)	1 (--)
14	Banks	26 (26)	-- (--)	-- (--)
	NBFIs	18 (22)	5 (1)	3 (3)
15	Banks	25 (24)	-- (--)	1 (2)
	NBFIs	24 (23)	-- (--)	2 (3)
16	Banks	26 (26)	-- (--)	-- (--)
	NBFIs	26 (25)	-- (1)	-- (--)
17	Banks	25 (25)	1 (1)	-- (--)
	NBFIs	25 (24)	1 (--)	-- (2)
18	Banks	25 (25)	-- (--)	1 (1)
	NBFIs	24 (24)	-- (--)	2 (2)
19	Banks	23 (26)	3 (--)	-- (--)
	NBFIs	17 (19)	8 (5)	1 (2)
20	Banks [n/a - 2]	24 (18)	-- (6)	-- (--)
	NBFIs [n/a - 1]	21 (12)	3 (10)	1 (--)
21	Banks	22 (23)	3 (3)	1 (--)
	NBFIs	19 (19)	4 (6)	3 (1)
22		25 (22)	--	1 (4)
23		20 (17)	-- (2)	6 (7)

Recommendation		Members in Compliance	Members in Partial Compliance	Other
24		23 (22)	3 (4)	-- (--)
25		26 (19)	-- (6)	-- (--)
26	Banks	26 (26)	-- (--)	-- (--)
	NBFIs	25 (25)	1 (--)	-- (1)
27		11 (11)	-- (--)	15 (15)
28	Banks	24 (24)	-- (--)	2 (2)
	NBFIs	19 (14)	1 (6)	6 (6)
29	Banks	25 (26)	-- (--)	1 (--)
	NBFIs	19 (18)	6 (7)	1 (1)
30		12 (10)	7 (8)	7 (8)
32		20 (19)	5 (5)	1 (2)

Note

The figures in parenthesis indicate the number of members in the category in the 1996-1997 FATF-VIII survey.

NBFIs: Non-bank financial institutions.

ANNEX E

PROVIDING FEEDBACK TO REPORTING FINANCIAL INSTITUTIONS AND OTHER PERSONS

BEST PRACTICE GUIDELINES

I. INTRODUCTION

The importance of providing appropriate and timely feedback to financial and other institutions which report suspicious transactions has been stressed by industry representatives and recognised by the financial intelligence units (FIU) which receive such reports. Indeed, such information is valuable not just to those institutions, but also to their associations, to law enforcement and financial regulators and to other government bodies. However, the provision of general and specific feedback has both practical and legal implications which need to be taken into account.

2. It is recognised that ongoing law enforcement investigations should not be put at risk by disclosing inappropriate feedback information. Another important consideration is that some countries have strict secrecy laws which prevent their financial intelligence unit from disclosing any significant amount of feedback, or that more general privacy laws limit the feedback which can be given. However, those agencies which receive suspicious transaction reports should endeavour to design feedback mechanisms and procedures which are appropriate to their laws and administrative systems, which take into account such practical and legal limitations, and yet seek to provide an appropriate level of feedback. The limitations should not be used as an excuse to avoid providing feedback, though they may provide good reasons for using these guidelines in a flexible way so as to provide adequate levels of feedback for reporting institutions.

3. Based on the types and methods of feedback currently provided in a range of FATF member countries, this set of best practice guidelines will consider why providing feedback is necessary and important. The guidelines illustrate what is best practice in providing general feedback on money laundering and the results of suspicious transaction reports by setting out the different types of feedback and other information which could be provided and the methods for providing such feedback. The guidelines also address the issue of specific or case by case feedback and the conflicting considerations which affect the level of specific feedback which is provided in each country. The suggestions contained herein are not mandatory requirements, but are meant to provide assistance and guidance to financial intelligence units, law enforcement and other government bodies which are involved in the receipt, analysis and investigation of suspicious transaction reports, and in the provision of feedback on those reports.

II. WHY IS FEEDBACK ON SUSPICIOUS TRANSACTION REPORTS NEEDED

4. The reporting of suspicious transactions[15] by banks, non-bank financial institutions, and in some countries, other entities or persons, is now regarded as an essential element of the anti-money laundering program for every country. Recommendation 15 of the FATF forty Recommendations states :

> "15. If financial institutions suspect that funds stem from a criminal activity, they should
> be required to report promptly their suspicions to the competent authorities. "

5. Almost all FATF members have now implemented a mandatory system of reporting suspicious transactions, though the precise extent and form of the obligation varies from country to country. The requirement under Recommendation 15 is also supplemented by several other recommendations such as financial institutions and their staff should receive protection from criminal or civil liability for reports made in good faith (Recommendation 16), customers must not be tipped off about reports (Recommendation 17), and financial institutions should comply with instructions from the competent authorities in relation to reports (Recommendation 18).

6. It is recognised that measures to counter money laundering will be more effective if government ministries and agencies work in partnership with the financial sector. In relation to the reporting of suspicious transactions an important element of this partnership approach is the need to provide feedback to institutions or persons which report suspicious transactions. Financial regulators will also benefit from receiving certain feedback. There are compelling reasons why feedback should be provided :

- it enables reporting institutions to better educate their staff as to the transactions which are suspicious and which should be reported. This leads staff to make higher quality reports which are more likely to correctly identify transactions connected with criminal activity;

- it provides compliance officers of reporting institutions with important information and results, allowing them to better perform that part of their function which requires them to filter out reports made by staff which are not truly suspicious. The correct identification of transactions connected with money laundering or other types of crime allows a more efficient use of the resources of both the financial intelligence unit and the reporting institution;

- it also allows the institution to take appropriate action, e.g. to close the customer's account if he is convicted of an offence, or to clear his name if an investigation shows that there is nothing suspicious;

[15] In some jurisdictions the obligation is to report unusual transactions, and these guidelines should be read so as to include unusual transactions within any references to suspicious transactions, where appropriate.

- it can lead to improved reporting and investigative procedures, and is often of benefit to the supervisory authorities which regulate the reporting institutions; and

- feedback is one of the ways in which government and law enforcement can contribute to the partnership with the financial sector, and it provides information which demonstrates to the financial sector that the resources and effort committed by them to reporting suspicious transactions are worthwhile, and results are obtained.

7. In many countries the obligation to report suspicious transactions only applies to financial institutions. Moreover, the experience in FATF members in which an obligation to report also applies to non-financial businesses or to all persons is that the vast majority of suspicious transactions reports are made by financial institutions, and in particular by banks. In recent years though, money laundering trends suggest that money launderers have moved away from strongly regulated institutions with higher levels of internal controls such as banks, towards less strongly regulated sectors such as the non-bank financial institution sector and non-financial businesses. In order to promote increased awareness and co-operation in these latter sectors, FIUs need to analyse trends and provide feedback on current trends and techniques to such institutions and businesses if a comprehensive anti-money laundering strategy is to be put in place. The empirical evidence suggests that where there is increased feedback to, and co-operation with, these other sectors, this leads to significantly increased numbers of suspicious transaction reports.

III. GENERAL FEEDBACK

(i) Types of feedback

8. Several forms of general feedback are currently provided, at both national and international levels. The type of feedback and the way in which it is provided in each country may vary because of such matters as obligations of secrecy or the number of reports being received by the FIU, but the following types of feedback are used in several countries :

(a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures;

(b) information on current techniques, methods and trends (sometimes called "typologies"); and

(c) sanitised examples of actual money laundering cases.

9. The underlying information on which general feedback can be based is either statistics relating to the number of suspicious transaction reports and the results achieved from those reports, or cases or investigations involving money laundering (whether or not the defendant is prosecuted for a money laundering offence or for the predicate offences). As these cases or investigations could result from a suspicious transaction report or from other sources of information, it is important that those agencies which provide feedback ensure that all relevant examples are included in the feedback they provide. It is also important that all relevant authorities, together with the reporting institutions, agree on

the contents and form of sanitised cases, so as to prevent any subsequent difficulties to any institution or agency. It would also be beneficial if certain types of feedback, such as sanitised cases, are widely distributed, so that the benefits of this feedback are not restricted to the reporting institutions in that particular country.

(a) Statistics

What types of statistics should be made available?

10. Statistical information could be broken into at least two categories : (a) that which relates to the reports received and the breakdowns that can be made of this information, and (b) that which relates to reports which lead to or assist in investigations, prosecutions or confiscation action. Examples of the types of statistics which could be retained are :

- Category (a) - detailed information on matters such as the number of suspicious transaction reports, the number of reports by sector or institution, the monetary value of such reports and files, and the geographic areas from which cases have been referred. Information could also be retained to give a breakdown of the types of institutions which reported and the types of transactions involved in the transactions reported.

- Category (b) - information on the investigation case files opened, the number of cases closed, and cases referred to the prosecution authorities. Breakdowns could also be given of the year in which the report was made, the types of crimes involved and the amount of money, as well as the nationality of the parties involved and which of the three stages of a money laundering operation (placement, layering or integration) the case related to. Where appropriate, statistics could also be kept on the reports which have a direct and positive intelligence value, and an indication given of the value of those reports. This is because reports which do not lead directly to a money laundering prosecution can still provide valuable information which may lead to prosecutions or confiscation proceedings at a later date (see paragraph 18).

11. A cross referencing of the different breakdowns of category (a) information with the types of results achieved under category (b) should enable FIUs and reporting institutions to identify those areas where reporting institutions are successfully identifying money laundering and other criminal activity. It would also identify, for example, those areas where institutions are not reporting or are reporting suspicions which lead to below average results. As such it would be a valuable tool for all concerned. However, as with any statistics, care needs to be taken in their interpretion, and in the weight that is accorded to each statistic. In order to extract the desired statistics efficiently it is of course necessary that the suspicious transaction report form, whether it is sent on paper or on-line, is designed to allow the appropriate breakdowns to be made. Given the difficulties that many countries have in gathering and analysing statistics, it is essential that the amount of human resources required for this task are minimised, and that maximum use is made of technology, even if this initially requires capital expenditure or other resource inputs.

How often should statistics be published?

12. Statistics are the most commonly provided form of feedback, and are usually included in annual reports or regular newsletters, such as those published by FIUs. Having regard to the resource implications of collecting and providing statistics, and to the other types of feedback available, the publication of an annual set of comprehensive statistics should provide adequate feedback in most countries.

13. It is recommended that :

- **statistics are kept on the suspicious transaction reports received and on the results obtained from those reports, and that appropriate breakdowns are made of the available information;**
- **the statistics on the reports received are cross referenced with the results so as to identify areas where money laundering and other criminal activity is being successfully detected;**
- **technological resources are used to their maximum potential; and**
- **comprehensive statistics are published at least once a year.**

(b) Current techniques, methods and trends

14. The description of current money laundering techniques and methods will be largely based on the cases transmitted to the prosecution authorities, and the division of such cases into the three stages of money laundering can make it easier to differentiate between the different techniques used, though it must of course be recognised that it is often difficult to categorically state that a transaction falls into one stage or another. If new methods or techniques are identified these should be described and identified, and reporting institutions advised of such methods as well as current money laundering trends. Information on current trends will be derived from prosecutions, investigations or the statistics referred to above, and could usefully be linked with those statistics. An accurate description of current trends will allow financial institutions to focus on areas of current risk and also future potential risk.

15. In addition to any reports that are prepared by national FIUs, there are a number of international organisations or groups which also prepare a report of trends and techniques, or hold an exercise to review such trends. The FATF holds an annual typologies exercise where law enforcement and regulatory experts from FATF members, as well as delegates from relevant observer organisations review and discuss current trends and future threats in relation to money laundering. A public report is then published which reviews the conclusions of the experts and the trends and techniques in FATF members and other countries, as well as considering a special topic in more detail. This report is available from the FATF or at the FATF Website (http://www.oecd.org/fatf/). In addition, Interpol publishes regular bulletins which contain sanitised case examples.

16. Other international groups such as the Asia/Pacific Group on Money Laundering, the Caribbean Financial Action Task Force (CFATF), and the Organisation of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD) are holding or will also hold typologies exercises which could provide further information on the trends and techniques that are being used to launder money in the regions concerned. International trends could usefully be extracted and included in feedback supplied by

national FIUs where they are particularly relevant, but in relation to more general information, reporting institutions should simply be made aware of how they can access such reports if they wish to. This will help to avoid information overload.

17. It is recommended that :

- **new money laundering methods or techniques, as well as trends in existing techniques are described and identified, and that financial and other institutions are advised of these trends and techniques;**

- **feedback on trends and techniques published by international bodies be extracted and included in feedback supplied by national FIUs only if it is particularly relevant, but that reporting institutions are made aware of how to access such reports.**

(c) Sanitised cases

18. This type of feedback is sometimes regarded by financial sector representatives as even more valuable than information on trends. Sanitised cases[16] are very helpful to compliance officers and front line staff, since they provide detailed examples of actual money laundering and the results of such cases, thus increasing the awareness of front line staff. Two examples of methods used to distribute this type of feedback are a quarterly newsletter and a database of sanitised cases. Both methods provide a set of sanitised cases which summarise the facts of the case, the inquiries made, and a brief summary of the results. A short section drawing out the lessons to be learnt from the case is also provided in the database. The length of the description of each case could vary from a paragraph outlining the case through to a longer and more detailed summary.

19. Care and consideration needs to be taken in choosing appropriate cases and in their sanitisation, in order to avoid any legal ramifications. In the countries which use such feedback, the examples used are generally cases which have been completed, either because the criminal proceedings are concluded or because the report was not found to be justified. Inclusion of cases where the report was unfounded can be just as helpful as those where the subject of the report was convicted of money laundering.

20. It is recommended that sanitised cases be published or made available to reporting institutions, and that each sanitised case could include :

- **a description of the facts;**
- **a brief summary of the result of the case;**
- **where appropriate, a description of the inquiries made by the FIU; and**
- **a description of the lessons to be learnt from the reporting and investigative procedures that were adopted in the case. Such lessons can be helpful not only to financial institutions and their staff, but also to law enforcement investigators.**

(ii) <u>Other information which could be provided</u>

21. In addition to general feedback of the types referred to above, there are other types of information which can be distributed to financial and other institutions using the same methods. Often this information is provided in guidance notes or annual reports, but it provides essential background information for the staff of reporting institutions, and also keeps them up to date on current issues. Examples of such other information include :

- **an explanation of why money laundering takes place, a description of the money laundering process and the three stages of money laundering, including practical examples;**
- **an explanation of the legal obligation to report, to whom it applies and the sanctions (if any) for failing to report**;

[16] Sanitised cases are cases which have had all specific identifying features removed.

- **the procedures and processes by which reports are made, analysed, and investigated, and by which feedback is provided**. This allows FIUs to provide information on matters such as the length of time it can take for a criminal proceeding to be finalised or to explain that even though not every report results in a prosecution for money laundering, the report could be used as evidence or intelligence which contributes to a prosecution for a criminal offence, or provides other valuable intelligence information;

- **a summary of any legislative changes** that may have been recently made in relation to the reporting regime or money laundering offences;

- **a description of current and/or future challenges for the FIU.**

(iii) Feedback Methods

22. ***Written Feedback*** - As noted above, two of the most popular methods of providing general feedback are through annual reports and regular newsletters or circulars. As noted above, annual reports could usefully contain sets of statistics and a description of money laundering trends. A short (for example, four page) newsletter or circular which is published on a regular basis two or four times a year provides continuity of contact with reporting institutions. It could contain sanitised cases, legislative updates or information on current issues or money laundering methods.

23. ***Meetings*** - There are a range of other ways in which feedback is provided to the bodies or persons who report. Most FIU provide such feedback through face to face meetings with financial institutions, either for a specific institution and its staff, or for a broader range of institutions. Seminars, conferences and workshops are commonly used to provide training for financial institutions and their staff, and this provides a forum in which feedback is provided as part of the training and education process. Several countries have also established working or liaison groups combining the FIU which receives the reports and representatives of the financial sector. These groups can also include the financial regulator or representatives of law enforcement agencies, and provide a regular channel of communication through which feedback and other topics such as reporting procedures, can be discussed. Finally, staff of FIUs could use meetings with individual compliance officers as an opportunity to provide general feedback.

24. ***Video*** - many countries and financial institutions or their associations have published an educational video as part of their overall anti-money laundering training and education process. Such a method of communication provides an opportunity for direct feedback to front line staff and could include material on sanitised cases, money laundering methods and other information.

25. ***Electronic information systems*** - obtaining information from Websites, other electronic databases or through electronic message systems has the advantage of speed, increased efficiency, reduced operating costs and better accessibility to relevant information. While the need for appropriate confidentiality and security must be maintained, consideration should be given to providing increasing feedback through a password protected or secure Website or database, or by electronic mail.

26. When deciding on the methods of general feedback that are to be used, each country will have to take into account the views of the reporting institutions as to degree to which reporting of suspicious or unusual transactions should be made public knowledge. For example, in some countries, the banks have no objection to sanitised cases becoming public information, in part because of the objective and transparent nature of the reporting system. However, in other countries, financial institutions would like to receive this type of feedback, but do not want it made available to the public as a whole. Such differing views mean that slightly different approaches may need to be taken in each country.

IV. SPECIFIC OR CASE BY CASE FEEDBACK

27. Reporting institutions and their associations welcome prompt and timely information on the results of reports of suspicious transactions, not only so they can improve the processes of their member institutions for identifying suspicious transactions, but also so they can take appropriate action in relation to the customer. There is concern that by keeping a customer's account open after a suspicious transaction report has been made the institution may be increasing its vulnerability with respect to monies owed to them by the customer. However specific feedback is much more difficult to provide than general feedback, for both legal and practical reasons.

28. One of the primary concerns is that ongoing law enforcement investigations should not be put at risk by providing specific feedback information to the reporting institution at a stage prior to the conclusion of the case. Another practical concern is the question of the resource implications and the best and most efficient method for providing such feedback, which will often depend on the amount of reports received by the FIU. Legal issues in some countries relate to strict secrecy laws which prevent the FIU from disclosing specific feedback, or concern general privacy laws which limit the feedback which can be provided. Finally, financial institutions are also concerned about the degree to which such feedback becomes public knowledge, and the need to ensure the safety of their staff and protect them from being called as witnesses who have to give evidence in court concerning the disclosure. This was dealt with in one country by a specific legislative amendment which prohibits suspicious transaction reports being put in evidence or even referred to in court.

29. Given these limitations and concerns, current feedback information provided by receiving agencies to reporting institutions on specific cases is more limited than general feedback. The only information which appears to be provided in most countries is an acknowledgement of receipt of the suspicious transaction report. In some countries this is provided through an automatic, computer generated response, which would be the most efficient method of responding. The other form of specific feedback which is relied on in many countries is informal feedback through unofficial contacts. Often this is based on the police officer or prosecutor who is investigating the case following up the initial report, and serving the reporting institution with a search warrant, or some other form of compulsory court order requiring further information to be produced. Although this gives the institution some further feedback information, it will only be interim information not showing the result of the case, and the institution is left uncertain as to when it will receive this information.

30. Depending on the degree to which the practical and legal considerations referred to in paragraph 28 apply in each country, other types of specific feedback are provided - this includes regular advice on cases that are closed, information on whether a case has been passed on for investigation and the name of the investigating police officer or district, and advice on the result of a case when it is concluded. In most countries, feedback is not normally provided during the pendancy of any investigation involving the report.

31. Having regard to current practice and the concerns identified above, and taking into account the requirements imposed by any national secrecy or privacy legislation, and subject to other limitations such as risk to the investigation and resource implications, it is recommended that whenever possible, the following specific feedback is provided (and that time limits could also be determined by appropriate authorities so that it is assured that the feedback is timely), namely that :

a) receipt of the report should be acknowledged by the FIU;

b) if the report will be subject to a fuller investigation, the institution could be advised of the agency that will investigate the report, if the agency does not believe this would adversely affect the investigation; and

c) if a case is closed or completed, whether because of a concluded prosecution, because the report was found to relate to a legitimate transaction or for other reasons, then the institution should receive information on that decision or result;

V. CONCLUSION

32. In relation to both specific and general feedback, it is necessary that an efficient system exists for determining whether the report led or contributed to a positive result, whether by way of prosecution or confiscation, or through it's intelligence value. Whatever the administrative structure of the government agencies involved in collecting intelligence or investigating and prosecuting criminality it is essential that whichever agency is responsible for providing feedback receives the information and results upon which that feedback is based. If the FIU which receives the report is the body responsible, this will usually require the investigating officers or the prosecutor to provide the FIU with feedback on the results in a timely and efficient way. One method of efficiently achieving this could be through the use of a standard reporting form, combined with a set distribution list. Failure to provide such information will make the feedback received by reporting institutions far less accurate or valuable.

33. It is clear that there is considerable diversity in the volume, types and methods of general and specific feedback currently being provided. The types and methods of feedback are undoubtedly improving, and many countries are working closely with their financial sectors to try to increase the amount of feedback and reduce any limitations, but it is clear that the provision of feedback is still at an early stage of development in most

countries. Further co-operative exchange of information and ideas is thus necessary for the partnership between FIUs, law enforcement and the financial sector to work more effectively, and for countries to provide not only an increased level of feedback, but also where feasible, greater uniformity.

2 June 1998

Appendix L:

FATF, *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism: Canada* (Paris: FATF, 2008)

Financial Action Task Force
Groupe d'action financière

THIRD MUTUAL EVALUATION ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

CANADA

29 FEBRUARY 2008

TABLE OF CONTENTS

Tables

PREFACE - INFORMATION AND METHODOLOGY USED FOR THE EVALUATION[1]

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of Canada was based on the Forty Recommendations 2003 and the Eight Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004[2]. The evaluation was based on the laws, regulations and other materials supplied by Canada, and information obtained by the evaluation team during its on-site visit to Canada from 19 to 30 March 2007, and subsequently. During the on-site visit, the evaluation team met with officials and representatives of all relevant Canadian government agencies and the private sector. A list of the bodies met is set out in Annex II to the mutual evaluation report.

2. The evaluation was conducted by an assessment team which consisted of members of the FATF Secretariat, APG Secretariat and FATF and APG experts in criminal law, law enforcement and regulatory issues: Mr. John Carlson and Ms. Catherine Marty from the FATF Secretariat, Dr. Gordon Hook from the APG Secretariat, Ms. Anne Juniel, financial expert, Bank of France (France), Mr. Jack de Kluiver, legal expert, Department of Justice (United States), Mr. Marc Penna, law enforcement expert, Cellule de Traitement des Informations Financières (Belgium), Mr. Bill Peoples, law enforcement expert, New Zealand Police (New Zealand) and Mr. Jeremy Platts, financial expert, Hong Kong Monetary Authority (Hong Kong). Mr. Robin Sykes, Central Bank of Jamaica participated as an observer. The assessment team reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.[3]

3. This report provides a summary of the AML/CFT measures in place in Canada as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, and provides recommendations on how certain aspects of the system could be strengthened (see Table 2). It also sets out Canada's levels of compliance with the FATF 40+9 Recommendations (see Table 1).[4]

---

1 Generally, FATF reports are written in United Kingdom English; however, this report is written in Canadian English to avoid any confusion that may be caused by the spelling of Canadian agencies or citations from Canadian laws, regulations and other sources.

2 As updated in February 2007.

3 The list of all bodies met during the on-site mission, the copies of the key laws, regulations and other measures and the list of all laws, regulations and other materials received and reviewed by the assessors are available in the Annexes of this report.

4 Also see Table 1 for an explanation of the compliance ratings (C, LC, PC and NC).

EXECUTIVE SUMMARY

1. Background Information

4. This report provides a summary of the AML/CFT measures in place in Canada as of June 2007. The report describes and analyses those measures and provides recommendations on how certain aspects of the system could be strengthened. It also sets out Canada's levels of compliance with the FATF 40 + 9 Recommendations (see attached table on the Ratings of Compliance with the FATF Recommendations).

5. Canada has strengthened its overall AML/CFT regime since its last FATF mutual evaluation (1997) by implementing a number of changes both in terms of statutory amendments and structural changes. The most important developments were the enactment of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the creation of the Canadian Financial Intelligence Unit (FINTRAC) in 2000. With regard to the legal measures (ML and TF offences, confiscation, freezing mechanisms), the legal framework is generally in line with the FATF standards however further steps could be taken to enhance effective implementation. The Canadian FIU has been provided with extensive powers and responsibilities. Since it became operationally effective in November 2001, FINTRAC has undertaken extensive outreach and assistance to reporting entities and has developed close relationships with government partners. There are concerns about its effectiveness in disclosing money laundering and terrorist financing cases to law enforcement authorities.

6. Canada has recently introduced a significant set of new requirements for financial institutions that aim at implementing the FATF standards. A large number of these new requirements will only be in force in June 2008, and these, together with further amendments applicable to DNFBPs due to come into force in December 2008, have not been analysed in the context of this evaluation. As it currently stands however, the preventive system is generally insufficient to meet the FATF Recommendations. In addition, certain financial institutions that undertake financial activities, as defined by the FATF Recommendations, are not currently covered by the AML/CFT regime. Moreover, both the scope of coverage and the AML/CFT requirements for the designated non-financial businesses and professions (DNFBPs) are insufficient to meet the FATF standards. Although FINTRAC and the Office of the Superintendent of Financial Institutions (OSFI) are involved in comprehensive supervisory actions, there are varying degrees of supervision for AML/CFT purposes in the financial sector.

7. Illicit proceeds from a variety of criminal activities contribute to the ongoing money laundering situation in Canada with drug trafficking as the source of much of the money laundered. Other sources of proceeds of crime include, but are not limited to, prostitution rings, contraband smuggling, illegal arms sales, migrant smuggling, and white-collar crime such as securities offences, real estate fraud, credit card fraud and telemarketing fraud. While there is no estimate for the total annual proceeds of crime, drug sales are estimated to amount to several billion dollars.

8. The money laundering methods used in Canada have remained relatively consistent in recent years. They essentially consist of: smuggling; money service businesses and currency exchanges; casinos; purchase of real estate; wire transfers; establishment of offshore corporations; credit cards, stored value cards and new payment methods; use of nominees; use of foreign bank accounts; use of professional services (lawyers, accountants, etc.); and reinvestment and distribution in illicit drugs. At the placement stage, criminals are using money service businesses or casinos. Electronic funds transfers are being used for layering and at the integration stage, criminal proceeds are used to purchase high-value assets in attempts to conceal the origin of the funds. Most recently, there have been signs that criminals are turning to such methods as Internet payments or cross-border movement of gold bullion.

9. Canadian law enforcement authorities have identified a number of terrorist organisations operating in Canada. Investigations have shown that terrorist cells have a tendency to remain self-sufficient by generating funds locally. In some instances, they may do so by committing petty crimes, such as welfare fraud or credit card fraud. In other instances, cell members have started businesses to glean financial information from unsuspecting customers in order to clone credit cards and commit identity thefts. Law enforcement authorities have intelligence indicating that suspected terrorist entities in Canada are raising funds through drug trafficking.

10. The financial sector in Canada is diverse, mature, well developed and includes many service providers. The sector is significantly integrated, as many players offer similar services and a small group of "financial groups" or conglomerates offer a large variety of financial products directly or through subsidiaries. A wide range of financial institutions exist in Canada and are subject to AML/CFT requirements: banks; credit unions and *caisses populaires*; life insurance companies; trust companies (that offer services similar to those provided by banks but can also administer estates, personal and institutional trusts, trustee pension plans and agency contracts); securities firms and money service businesses (MSBs). Financial leasing, factoring, finance companies (*i.e.* entities specialised in consumer lending, credit cards, equipment financing and small business loans that are not loan companies), providers of e-money, Internet payment providers and cheque cashers are also engaged in financial activities as defined by the FATF.

11. The following DNFBPs are currently subject to AML/CFT requirements: casinos, real estate agents and accountants. In addition, the Government of Canada has recently enacted regulations to cover the following DNFBPs as of December 2008: lawyers, notaries (relevant in Québec and British Columbia only) and dealers in precious metals and stones. Trust and company service providers are not separately recognised nor regulated as a discrete category of entity in Canada and do not fall under the AML/CFT regime. Trust companies, accountants, lawyers and other independent legal professions provide most services of this nature, though it appears that some other businesses exist that engage in TCSP activity.

2. Legal System and Related Institutional Measures

12. The anti-money laundering offences are comprehensive and Canada generally meets the requirements under Recommendations 1 and 2. The money laundering offence (section 462.31 Criminal Code (CC)) is part of a broader proceeds of crime regime designed to cover all obligations in the 1988 Vienna Convention and the 2000 Palermo Convention. Section 462.31 encompasses acts of using, transferring the possession of, sending or delivering to any person or place, transporting, transmitting, altering, disposing of or otherwise dealings with, in any manner and by any means, any property or any proceeds of any property. The Section 462.31 offence is however technically inconsistent with the relevant UN Conventions in that it has a specific intent mental element that is not consistent with those Conventions. Designated offence refers to virtually all indictable offences and also covers all ancillary offences.

13. There is also a second offence of possession of proceeds of crime (s.354(1), CC), whereby it is an offence to knowingly possess money or property derived directly or indirectly from any indictable Canadian criminal offence or any foreign offence, that had it been committed in Canada would have been an indictable offence in Canada. The two offences cover almost all of the requirements of R.1 & 2, with only some minor technical deficiencies (see comments above). Despite this, the emphasis on and preference for pursuing the predicate crimes and the offence of possession of property obtained by crime, and the low number of s.462.31 convictions indicates that the statutes available for countering ML are not being used as effectively as they could be. Canada should develop a more proactive approach to prosecuting the specific money laundering charge under s.462.31.

14. Canada has three criminal offences related to the financing of terrorism (s. 83.02-83.04, CC). The offences are broadly defined and wide-reaching in effect. These offences cover the provision or collection of property intending or knowing that it will be used, in whole or in part, to carry out or

facilitate a "terrorist activity", to possess or use property for that purpose, or to benefit a terrorist group. The offences and related provisions cover all types of property; include ancillary offences; and generally meet all the requirements of the FATF standards. The offences have been in existence for several years and there have been a large number of investigations, but only three persons have been charged with terrorist financing and these charges have not been heard yet. There have been no convictions. Given these facts, the authorities should consider how the TF offence could be more effectively implemented. The overall effectiveness of the TF offence and regime is an issue that the authorities will need to pay close attention to going forward.

15. The CC and the Controlled Drugs and Substances Act (CDSA) contain extensive provisions that authorise the forfeiture of proceeds of crime and instrumentalities used in or intended for use in offences. Forfeiture is available for all money laundering and terrorist financing offences, as well as all predicate offences. Conviction for any indictable offence or a conspiracy or attempt to commit an indictable offence is a prerequisite to forfeiture. There are also discretionary provisions for a fine in lieu of forfeiture, which is the action that Canada has taken to seek to deprive criminals of property of equivalent value. If there are no assets to which such a fine can be applied the court must impose a jail sentence, otherwise the fine is enforced as a civil judgement against any other property of the offender, but cannot be applied against third party property in such cases.

16. Other legislative provisions are broad and allow the authorities to restrain or seize and search for proceeds of crime or instrumentalities. The definition of "property" is broad, and includes any benefit or advantage obtained or "derived directly or indirectly" as a result of the offence. The available data on seizure/restraint and forfeiture is not comprehensive and suggests that it could be more effective.

17. Canada's United Nations Act and its related regulations enable the Canadian government to implement the decisions contained in the resolutions of the United Nations Security Council. The United Nations Al-Qaida and Taliban Regulations (UNAQTR), and the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), were enacted under the authority of Canada's United Nations Act. These regulations allow Canada to list a terrorist individual or entity for the purpose of freezing the funds or assets owned or controlled by that individual or entity or its associates. A third listing mechanism exists under the Criminal Code for threats to Canada's domestic security. Canada has laws and regulations to freeze terrorist funds or other assets of persons designated in the context of S/RES/1267(1999) and S/RES/1373(2001) that are in line with the legal international requirements. However, although the lists are published in the Canada Gazette, there needs to be more communication on listed persons provided to certain categories of financial institutions and other potential asset holders as well as more clear and practical guidance to reporting entities (including DNFBPs and MSBs) that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms. Canada should also enhance the existing measures to monitor the compliance with the legislation governing the obligations under SRIII (except for federally regulated financial institutions supervised by OSFI).

18. In 2000, Canada established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a national centre for receiving, analyzing and disseminating information concerning suspected money laundering or terrorist financing. In addition to mandatory reporting by financial institutions and DNFBPs, FINTRAC can receive voluntary information concerning suspicions of money laundering or terrorist financing from the general public and various other sources, including information about cases being investigated by law enforcement agencies and foreign FIUs. FINTRAC has a high level of operational independence and information held by FINTRAC is securely protected.

19. Under the PCMLTFA, FINTRAC is authorized to disseminate financial information to domestic authorities for further action when it has reasonable grounds to suspect that the information would be relevant and useful to the investigation or prosecution of a money laundering or terrorist activity offence. FINTRAC provides comprehensive guidance to reporting entities regarding the manner of reporting and the procedures that should be followed when reporting. In February 2006, FINTRAC

launched an updated secure online report capture system that provides reporting entities with a reliable mechanism to file reports through the Internet. However, the format of reporting forms is perceived by certain reporting entities as being too rigid and reduces the capacity to communicate a maximum level of information. FINTRAC develops very few typologies and is not allowed by the PCMLTFA to ask (directly or indirectly) for additional financial information from reporting entities in line with the FATF requirements.

20. The information that FINTRAC can provide to a disclosure recipient is referred to as "designated information" and includes key details that identify individuals or entities and their financial transactions. Under the PCMLTFA, FINTRAC has the authority to collect information from databases maintained for law enforcement or national security purposes and in respect of which an agreement is entered into. FINTRAC currently has access to two major national police databases. However, FINTRAC has limited access to intelligence information from certain administrative authorities (such as the Canada Revenue Agency (CRA)).

21. There are serious issues in relation to effectiveness with respect to FINTRAC. Although Canada decided to establish a FIU that would make maximum use of advanced technologies in its analytical work, the number of staff dedicated to the analysis of potential ML/FT cases is low, especially in light of the number of reports FINTRAC receives, and FINTRAC has decided to concentrate its efforts on large or significant ML/TF cases. At the time of the on-site visit, the feedback provided by some organizations that receive FINTRAC disclosures was generally negative (unsatisfactory timelines for disclosures, relatively limited added value of FINTRAC disclosures in law enforcement investigations, FINTRAC disclosures positively contributed to existing investigations but rarely generated new ones). It seems that since March 2007, more positive feedback has been received from law enforcement authorities, especially with regard to the timeliness of disclosures. Another important issue is that, FINTRAC disclosures are largely based on voluntary information reports made by law enforcement authorities (80% of cases). This raises serious concerns with respect to the capability of FINTRAC to generate new ML/TF cases independent from existing investigations. Finally, until 2007, no conviction for ML or TF had directly resulted from a FINTRAC disclosure.

22. While all Canadian police forces can investigate money laundering and terrorist financing offences, the Royal Canadian Mounted Police (RCMP), and in particular its Integrated Proceeds of Crime Initiative, IPOC, Units, and, to a lesser extent, the provincial law enforcement authorities in Ontario (the Ontario Provincial Police) and Québec (*Sûreté du Québec*) undertake virtually all money laundering and terrorist financing investigations. The powers and capacity of the law enforcement services are sound and they have appropriate investigative techniques at their disposal. The RCMP acknowledges that, due to resources constraints, it essentially focuses its resources on large, complex ML investigations related to organised crime groups. The RCMP could undertake a larger number of investigations and tackle a larger spectrum of ML/TF cases with additional resources. In addition, consideration should be given to improving the educational and training programmes provided for judges and courts concerning ML and TF offences.

23. Canada has implemented comprehensive measures to detect the physical cross-border transportation of currency and bearer negotiable instruments that are related to ML or FT. These measures are fully in line with the FATF requirements and are effectively implemented.

3. Preventive Measures - Financial Institutions

24. To combat money laundering, the Canadian Parliament enacted the Proceeds of Crime (Money Laundering) Act which received Royal Assent on 29 June 2000. To help fight terrorism, it amended and renamed the legislation the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The PCMLTF Regulations and the PCMLTF Suspicious Transaction Reporting Regulations implement the provisions of the Act. In October 2006, a Bill proposing to further strengthen the PCMLTFA was introduced in Parliament to expand the scope of preventive measures. The Bill received Royal Assent in December 2006. Some new provisions of the PCMLTFA came into

force on 10 February 2007 and on 27 June 2007, the *Regulations Amending Certain Regulations Made Under the PCMLTFA* were enacted and published in the Canada Gazette. Some of these provisions came into force on 30 June 2007; others will take effect on 23 June 2008. A second package of regulatory amendments, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* setting out a framework for the registration of MSBs will come into force on 30 June 2008. Further regulations were enacted on 26 December 2007 that will come into force in December 2008. However, for the purpose of this report, none of the changes coming into force after June 2007 were considered.

25. FINTRAC (for all reporting parties), OSFI (for Federally Regulated Financial Institutions) and IDA (for securities dealers) have developed guidelines to assist persons and entities subject to the PCMLTFA and the Regulations to understand their obligations. IDA By-laws, Policies and Regulations are legally enforceable and can be considered as "other enforceable means". OSFI and FINTRAC Guidance are considered as non-binding guidance for the purpose of this report.

26. In Canada, certain entities that undertake financial activities, as defined by the FATF Recommendations, are not currently covered by the AML/CFT regime (except for entities that are caught because they also engage in financial activities which are captured under the regime). These include: financial leasing entities; factoring entities; finance companies (*i.e.* mostly entities specialized in consumer lending, issuing certain types of credit cards, equipment financing and unregulated small business lending entities); providers of e-money; Internet payment providers[5]; and cheque cashers[6] when their only activity is cashing cheques issued to denominated persons. Canada considers that these entities pose little or no threat of money laundering/terrorist financing. Canada's approach to risk is not in line with the FATF approach as defined in the Methodology where a list of activities and operations must be covered by the AML/CFT regime unless there is a proven low risk of ML/TF. Canada has applied the opposite approach and has extended coverage of the PCMLTFA only to activities for which there is a proven ML/TF risk. Moreover, the risk assessment process carried out by Canada to reach conclusions on the exposure of certain sectors to ML/TF risks is either non-existent or very fragmented and ad-hoc.

27. Customer identification measures in Canada are currently insufficient to meet the FATF standards[7]. Current legislation does not impose a requirement for financial institutions to conduct CDD in all cases covered by the FATF standards, including when there is a suspicion of ML or TF or when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. The current customer identification measures for natural persons are insufficient and, except for IDA supervised entities, financial institutions are not required to understand the ownership and control structure of the customer nor obliged to determine the natural persons that ultimately own or control the customer. There are currently no requirements (except for IDA supervised entities) to obtain information on the purpose and intended nature of the business relationship. There is no obligation to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction and the current approach is not in line with the FATF standards regarding situations of lower risk. Finally, the timing of verification of customer identity is inadequate for certain financial entities vis-à-vis certain customers. Financial institutions (except IDA supervised entities in some circumstances) are not prohibited from opening an account or commencing a business relationship or performing a transaction and they are not required to make a suspicious transaction report where they are unable to identify the customer.

---

5 Internet payment and e-money providers are only subject to the Act if they also offer funds remittance or transmission services and, as such, would be considered money services businesses.

6 Cheque cashing businesses that also offer money remittance services are included in the definition of MSBs under the PCMLTFA and are therefore subject to the requirements of the PCMLTFA.

7 New provisions will enter into force in June 2008 and December 2008. These provisions will impose a number of additional requirements including in the following areas: CDD, politically exposed persons, SR VII, record keeping, reporting of suspicious transactions, requirements for DNFBPs, and beneficial ownership information in company legislation. These changes were not assessed as the changes fall outside the period of the evaluation.

28. At the time of the on-site visit, there were no specific legislative or other enforceable requirements in relation to PEPs and limited requirements in relation to correspondent banking relationships. Provisions in relation to the prevention of misuse of technological developments in ML/TF schemes and the mitigation of risks associated with non-face to face business were not in compliance with the FATF requirements. New provisions entered into force in June 2007 for correspondent banking, and will enter into force in June 2008 in relation to PEPs. Although introduced business arrangements exist in Canada, Canada has not implemented adequate requirements in relation to third party introduced business.

29. There is no financial institution secrecy law that inhibits the implementation of AML/CFT requirements. Canada's record-keeping requirements are generally satisfactory. At the time of the on-site visit, Canada had not implemented SRVII on wire transfers.

30. Under the PCMLTFA, there is currently no explicit provision requiring financial institutions to pay special attention to all complex, unusual large transactions. Such a requirement may only be indirectly deduced from (a) the requirement to report to FINTRAC suspicious transactions that may be related to money laundering or terrorist financing, and (b) the obligation to report large international electronic funds transfers and large cash transactions. Canada should ensure that the new provisions coming into force in June 2008 will fully and effectively address these issues. The obligation to give special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations is also not fully met.

31. All financial institutions subject to the PCMLTFA are required to report to FINTRAC transactions of any amount for which there are reasonable grounds to suspect are related to the commission of a money laundering offence or a terrorist financing offence. However, certain categories of financial institution (see comments above) are not subject to the PCMLTFA and, consequently, to any mandatory reporting requirement to FINTRAC. Under the current legislation, reporting entities are only required to report completed transactions to FINTRAC. As from June 2008, the reporting requirement will be broadened to the reporting of any suspicious attempted transactions related to money laundering or terrorist financing. The total number of STRs sent by the financial sector appears satisfactory (an average of 20 000 every year since 2004). The different financial institutions however contributed unequally to the total number of STRs (securities dealers, life insurance companies and life insurance brokers and dealers have sent limited numbers of STRs).

32. No criminal or civil proceedings lie against persons and entities for making a suspicious transaction report, a terrorist property report, a large cash transaction report or an electronic funds transfer report in good faith or for providing FINTRAC with information about suspicions of money laundering or of the financing of terrorist activities. The provisions in relation to tipping off are also fully in line with the FATF standards. FINTRAC gives very detailed guidance related to STRs to assist financial institutions in implementing and complying with STR requirements and provides satisfactory general feedback to large financial institutions. Specific feedback is provided within the legislative limitations. The PCMLTFA requires reporting entities to submit reports to FINTRAC on large cash transactions and electronic funds transfers and the FATF requirements in that area are met.

33. The requirements in relation to internal procedures, policies and controls to prevent ML and FT are generally sound, but some changes are needed to bring them fully in line with the FATF standards. FRFIs have generally adopted enterprise-wide AML/CFT standards based on the OSFI Guideline and supervisory practice. There is no specific requirement regarding the enforcement of AML/CFT measures consistent with Canadian or FATF requirements in foreign branches and subsidiaries.

34. In addition, Canadian financial entities are prohibited from entering into a business relationship with shell banks or with foreign financial institutions that have correspondent banking relationships with shell banks. Canada is broadly in compliance with the FATF requirements in this regard.

35. FINTRAC is responsible for ensuring compliance with the PCMLTFA. FINTRAC's compliance program is based on a collaborative risk-based approach divided into two categories: the promotion of compliance and the monitoring of compliance. FINTRAC has signed MOUs with certain financial and gaming regulators or supervisors to share AML/CFT supervisory information. In addition, some regulators have provisions under their own legislation or codes of conduct that impose similar requirements to, or which complement the key provisions in the PCMLTFA. Globally, there are unequal degrees of regulation and supervision, depending on the sectors and provinces although OSFI is responsible for regulating well over 80% of the Canadian financial sector as measured by total assets. It is worth mentioning that the entities which are currently not subject to the PCMLTFA are not subject to prudential supervision either.

36. The number of examinations performed by FINTRAC appears to be relatively low compared with the total number of reporting financial entities (potentially more than 100 000) although a single FINTRAC examination can cover a large number of reporting entities (*e.g.* in the case of life insurance companies/agents and securities firms/dealers). Even including examinations conducted by FINTRAC's MOU partners, the figures remain rather low, except for the banking and federally regulated trust companies sectors which have a good supervisory coverage by OSFI. The use of a sophisticated risk-based model helps FINTRAC prioritise its supervisory activities. Those activities encompass not only examinations of reporting entities but also guidance, outreach, self-assessment tools and follow-up actions after examinations.

37. The securities sector is regulated by provincial securities regulatory authorities (SRAs) and has been subject to limited AML/CFT supervision. The on-site AML/CFT assessments conducted by OSFI since 2003 in the federally regulated life insurance sector amount to 90% of the industry measured by its assets but less than 10% of the supervised population. AML/CFT supervision by provincial financial supervisors appears to be less effective for life insurance agents because AML/CFT controls are mostly assessed by FINTRAC. In addition, despite the focus put on that sector, FINTRAC had managed to perform controls on only 60 credit unions and *caisses populaires* up to mid-2007, out of a total population of 1 250 reporting entities.

38. Under the current version of the PCMLTFA and its Regulations, FINTRAC has limited powers of enforcement against reporting entities and their directors or senior management for failure to comply with or properly implement AML/CFT requirements. Currently, FINTRAC cannot impose penalties and is limited to referring cases to law enforcement for investigation. Strengthening the sanctions regime in June 2008 with the introduction of administrative and monetary penalties should be a crucial enhancement of the system. The current PCMLTFA provides for a series of criminal sanctions for contraventions of various provisions of the Act. These can lead to criminal penalties of up to CAD 2 million in fines and five years in prison for non-compliance. The December 2006 amendments expanded the regime of criminal sanctions to the violations of most of the provisions of the PCMLTFA and regulations.

39. OSFI has a wider range of possible enforcement actions or sanctions than FINTRAC. Nevertheless, sanctions remain infrequently used, and do not appear to be sufficiently effective, proportionate and dissuasive, though this may be partially due to the early intervention strategy adopted by OSFI. In the securities sector, except for IDA which has effectively applied in a number of cases heavy sanctions to its members for non compliance with AML/CFT standards, it seems that the powers of sanction have generally not been used by SRAs or SROs in that area, as they have rarely issued specific rules or regulations related to AML/CFT and consider such issues to be mainly FINTRAC's responsibility.

40. Measures aimed at preventing criminals or their associates from holding a significant or controlling interest or holding a management function in a financial institution, as well as the "fit and proper" principle are widespread. There is no systematic harmonization of these requirements across the federal and provincial systems. At the time of the on-site visit, there was no compulsory obligation

for FRFIs to implement screening procedures for directors or senior management, after the initial incorporation or authorisation procedures are concluded.

41. There was no registration regime for MSBs at the time of the on-site visit although Canada has created a federal registration regime that will enter into force in June 2008. The preventive measures currently applicable to MSBs (especially in relation to CDD, reporting of suspicious transactions or SRVII) present serious weaknesses and the MSB sector is subject to a limited range of preventive measures that are not in compliance with international standards. In addition, the sanction regime applicable to MSBs that fail to comply with the PCMLTFA is currently not effective, proportionate and dissuasive. Canada should ensure effective implementation of the registration system for MSBs in force in June 2008 and ensure that the requirements applicable to MSBs fully meet the FATF requirements.

4. Preventive Measures – Designated Non-Financial Businesses and Professions (DNFBPs)

42. The PCMLTFA currently covers casinos, real estate brokers and sales representatives and accountants and accounting firms. Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, and TCSPs are not currently captured by the PCMLTFA and therefore are not subject to the requirements under Recommendations 5, 6 and 8-11. It should be noted that Internet casinos are illegal in Canada, but servers hosting such activity exists in Canada, and Canada should either take law enforcement action to eliminate this illegal activity, or regulate these casinos. The requirements in relation to Recommendation 5 and 13 applicable to land-based casinos, real estate brokers and sales representatives and accountants do not meet the FATF standards. Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs. There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes. The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. Provisions in relation to record-keeping with regard to casinos, real estate brokers and sales representatives and accountants are not fully in line with the FATF standards.

43. Because of limited staff resources, FINTRAC is not in a position to ensure an efficient monitoring of the effective application of AML/CFT legislation in the non-financial sectors captured by the PCMLTFA, especially in sectors/provinces where the primary regulators or SROs are not or insufficiently involved in AML/CFT compliance supervision. Canada should ensure that supervisory actions (especially on-site examinations) vis-à-vis casinos and more generally with regard to all DNFBPs are reinforced. With regard to DNFBPs, the sanction regime available to FINTRAC is currently inadequate but should be strengthened when administrative and monetary penalties are introduced in June 2008.

5. Legal Persons and Arrangements & Non-Profit Organisations

44. Canada's corporate registry and information collection system does not adequately focus on obtaining information relating to the beneficial owner or controller of bodies corporate in Canada. The information collected and maintained (including changes in information) relates almost solely to persons and other corporations that are the immediate owners or controllers of a corporation through shareholdings. The federal corporate registrar should consider measures to mitigate the threat that may arise from the use of legal persons to perpetrate money laundering and terrorist financing. Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis.

45. The Canada Business Corporations Act (CBCA) appears to allow for the ownership of corporations through the use of bearer shares, although it is likely that the number of bearer shares is limited. Nonetheless, there do not appear to be any special measures in place to ensure disclosure of beneficial owners of these shares in order to mitigate the ML or TF risk.

46. Except for the province of Quebec (where the *fiducie* is similar to the trust), all provinces are common law jurisdictions and have trust laws. Canada relies on the investigatory powers of law enforcement to obtain or have access to information concerning the beneficial ownership and control of trusts and *fiducies*. These powers are generally sound and widely used. In the case of trusts and *fiducies*, limited, partial information is available, and even where certain information is recorded by agencies such as CRA or FINTRAC, agencies can only share this information with law enforcement authorities in limited circumstances. Canada should implement measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts and *fiducie* in Québec.

47. Canada has a well-established registration system for charities and has taken considerable steps to implement SR VIII. Registered charities include most organizations that raise and distribute funds for social or humanitarian purposes. Charities represent the most significant portion of the financial resources of the NPO sector and account for a substantial share of the sector's foreign activities. Nevertheless, in line with the FATF's risk-based approach, Canada should continue to monitor risks in other segments of the NPO sector.

6. National and International Co-operation

48. Canada has developed a large number of initiatives to improve co-operation mechanisms among the different domestic stakeholders taking part in the fight against money laundering and terrorist financing. The interagency cooperation between the FIU and law enforcement authorities is not fully effective and should be enhanced in order for Canada to optimise its capacity to investigate ML and TF cases. Canada should consider encouraging more bilateral contacts among agencies.

49. Almost all of the provisions of the Palermo and Vienna Conventions have been fully implemented, and only some minor technical deficiencies remain. Canada has extensive formal and limited informal means of providing mutual legal assistance (MLA) to requesting countries. Where the evidence can only be gathered pursuant to a court order, Canada's Mutual Legal Assistance in Criminal Matters Act ("MLACMA" or "the Act") is the domestic legislation that enables a Canadian court to issue orders compelling the production or authorizing the seizure of evidence at the request of a treaty partner. Canada has a centrally-coordinated MLA regime involving: the Department of Justice, Crown prosecutors, the Judiciary and, on occasion, law enforcement agents who execute Canadian courts' orders. Canada should focus on improving the effectiveness of the current regime and the collection of adequate data.

50. Under the MLACMA, Canada can directly enforce foreign orders for the restraint, seizure and forfeiture of assets on receipt of a request from a treaty partner or designated entity in line with the FATF requirements. However, in terms of implementation, there is limited evidence of effective confiscation assistance, and Canada should consider how this could be enhanced.

51. The money laundering and terrorist financing offences are extraditable offences under Canada's Extradition Act. The current legal provisions on extradition meet the FATF standards; however Canada should maintain better extradition request data, so as to better assess the timeliness of assistance.

52. In general, law enforcement authorities can engage in a wide range of international co-operation. FINTRAC can also share its intelligence with foreign counterparts. As the AML/CFT supervisor, FINTRAC has the legal capacity to exchange supervisory information with foreign regulators, but has not yet entered into any MOUs that will allow it to share in practice. On the other hand, OSFI can exchange compliance information with foreign counterparts.

7. Other issues

53. Overall, authorities seem to be well-equipped, staffed, resourced and trained. There are concerns about the availability of resources within FINTRAC to undertake a sufficient number of comprehensive examinations. The number of staff at FINTRAC dedicated to the analysis of ML/TF cases is also too low. Finally, the authorities in charge of processing MLA requests should acquire additional resources to fulfil their tasks.

54. Canada collects a large set of statistics although more comprehensive data should be gathered regarding ML investigations and sentencing, MLA and extradition requests.

MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General Information on Canada

55. Canada consists of 10 provinces (Alberta, British Columbia, Manitoba, Newfoundland and Labrador, New Brunswick, Nova Scotia, Ontario, Prince Edward Island, Québec and Saskatchewan), and three territories (the Northwest Territories, Nunavut and Yukon). Ottawa, Ontario, is the national capital. Geographically, it is the second-largest country in the world, with a land area of 9.9 million square kilometres. Canada is bordered by the United States of America to the south and northwest (Alaska), with coastlines on the Pacific Ocean to the west, the Arctic Ocean to the north and the Atlantic Ocean to the east. Approximately 86 % of Canada's 32 million people live in the country's four largest provinces: Ontario (39 %), Québec (24 %), British Columbia (13 %) and Alberta (10 %). Canadians have an average life expectancy of 80 years and the median age is currently 39 years. Canada's two official languages are English and French.

56. Canada is the eighth-largest economy in the world with about 70% of the economy devoted to services. Manufacturing now accounts for just over 25% and the primary sectors account for around 5%. In 2006, Canadian per capita gross domestic product (GDP) was CAD 44 083.

System of government

57. Canada is a federal state. Pursuant to the Constitution Act, 1867, the governing power of the country is divided between the federal government and provincial governments. The federal government is responsible for matters that affect all of Canada, including national defence, criminal law, banking, citizenship and foreign relations. Provincial and territorial governments look after such matters as education, health care and social services. They share responsibilities with the federal government in some areas. For instance, the federal government has legislative jurisdiction over criminal law and procedure, while the provinces are responsible for the administration of the courts of criminal jurisdiction including federal courts constituted under section 96 of the Constitution. This provincial jurisdiction includes the constitution, maintenance and organization of provincial courts in both civil and criminal jurisdictions, and civil procedure as applied in provincial courts. There is also a third level of government at the community level, known as municipal (or local) government, which is responsible for local matters.

58. Canada has a Westminster parliamentary system of government. Parliament is divided into three heads of power: the Queen, the Senate (the upper house of 105 members) and the House of Commons (the lower house of 308 members). Canada is a constitutional monarchy; Her Majesty Queen Elizabeth II is Canada's official head of state. She is represented in Canada by the Governor General, who gives Royal Assent, in the name of the Queen, to all legislation passed by Parliament. The Queen appoints the Governor General on the advice of the Prime Minister. One of the most important roles of the Governor General is to ensure that Canada always has a Prime Minister. The House of Commons, the Senate and the Governor General must approve all parliamentary bills before they become law. The government introduces most parliamentary legislation, but the Senate can also introduce its own bills, except bills to spend public money or impose taxes.

Legal system and hierarchy of laws

59. Canada is governed by the common law, or rule of precedent, and by a civil law system in Québec. Every federal law must be drafted in both official languages but, because of Canada's dual legal system, it must also respect both the common law and civil law traditions in the provinces. Provinces have a similar system for passing legislation into force with the exception that provincial legislatures do not have an upper house. As such, in order for provincial legislation to become law, it

requires enactment by the provincial legislature. The Queen's provincial representatives, the lieutenant governors, give Royal Assent, in the name of the Queen, to all legislation enacted by provincial legislatures. Territorial and local governments are not sovereign units. The powers of territories are delegated by Parliament, while those of local governments are delegated mainly by provincial governments.

60. Legislation and regulations are developed in a transparent manner to ensure they reflect the values of society and to ensure that use of the government's legislative and regulatory powers result in the greatest net benefit to Canadian society.

61. When a legislative proposal is made to the Cabinet, it is up to the sponsoring Minister to demonstrate that there are no other ways to achieve the policy objectives effectively. The decision to address a matter through a bill or regulation is made by Cabinet on the basis of analysis of the matter and its alternative solutions, consultations with partners and stakeholders, analysis of impacts of the proposed solution and analysis of the resources that the proposed solution would require. A bill must pass through a series of parliamentary stages (in the House of Commons and the Senate) before it becomes law. The final stage is Royal Assent. The Constitution Act, 1867 states that the approval of the Crown, signified by Royal Assent, is required for any bill to become law after passage by both Houses. Royal Assent can be given by the Governor General as the Queen's representative in Canada or a Deputy of the Governor General.

62. Regulations are another form of law that often stem from the introduction or amendments to legislation. Regulations are not made by Parliament but are made by persons or bodies to whom Parliament has delegated the authority to make them (such as the Governor in Council, a Minister or an administrative agency). Authority to make regulations must be expressly delegated by an Act.

63. The Statutory Instruments Act and the Regulatory Policy of the Government of Canada guide the development of regulations. The Statutory Instruments Act establishes a process designed to ensure that regulations are made on a legally secure foundation. A key element of the Policy is that Canadians are consulted, and that they have an opportunity to participate in developing or modifying regulations and regulatory programs. Each proposed regulation must pass through a series of steps before coming into force, including pre-publication, "making" the regulation, registration, publication, and distribution.

64. Draft regulations are pre-published in Part I of the Canada Gazette to give those who are interested in a regulatory proposal an opportunity to express their views. The length of pre-publication depends on the type of regulation, but typically lasts between 30 and 75 days. Following the period of pre-publication, regulations are "made" by the authority designated in the enabling Act and then transmitted to the Clerk of the Privy Council (within 7 days) for registration. Registration is a crucial step in the case of regulations because it determines when they take effect. Typically, regulations that must be registered come into force on the day they are registered. Following registration, regulations are published, in Part II of the Canada Gazette within 23 days after their registration.

The Canadian Charter of Rights and Freedoms

65. Canada has always sought to protect individual rights and freedoms through legislative enactments such as the Canadian Bill of Rights. This bill became law in 1960 and, as a federal statute, is limited in scope and has no application to provincial laws. On the other hand, the Canadian Charter of Rights and Freedoms enacted in 1982 is part of Canada's Constitution. Unlike the Bill of Rights, it constitutionally entrenches the basic principles and values by which Canadians live and govern themselves. It applies to both federal and provincial jurisdictions and guarantees, among other things, that everyone, regardless of colour, religion, race, belief or a ground analogous thereto, has certain fundamental rights and freedoms "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

66. The Charter outlines fundamental rights and freedoms such as the right to life, liberty and security of the person; equality rights, such as the right to protection against discrimination; legal rights of persons accused of crimes, such as the right to a fair trial; freedom of conscience; freedom of religion; freedom of thought and freedom of association.

Canada's Privacy Laws

67. *Public Sector*. Privacy laws regulating the collection, use and disclosure of personal information by governments and the public sector have been in place in Canada since the early 1980s. On 1 July 1983, the Canadian federal government enacted the Privacy Act. This Act imposes obligations on some 150 federal government departments and agencies to respect privacy rights. Companion freedom of information legislation, called the Access to Information Act, was enacted at the same time. Most of Canada's provincial governments have followed suit with similar legislation covering both access to information and protection of privacy in provincial and municipal operations.

68. In relation to the fight against money laundering and terrorist financing, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) sets out numerous provisions specifically designed to protect the privacy of individuals and defines the circumstances under which the Canadian Financial Intelligence Unit (the Financial Transactions and Reports Analysis Centre of Canada, FINTRAC) may disclose personal information. The impact of the PCMLTFA on the privacy of Canadians and the existence of sufficient safeguards in the anti-money laundering and counter terrorist financing legislation has raised discussions in Canada[8]. The amendments that are being brought to the AML/CFT legislation are scrutimized to ensure that the new requirements do not unduly compromise the privacy of Canadians.

69. *Private Sector*. As of 2007, Canadian business and private sector organizations are also subject to federal or provincial privacy protection legislation governing both customer and, with some exceptions, employee information. Québec was the first Canadian jurisdiction to introduce privacy protection legislation applicable to the private sector when it implemented its Act Respecting the Protection of Privacy in the Private Sector in 1994. The federal government enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) effective January 1, 2001. PIPEDA applies to federally-regulated private sector organizations (*i.e.* organizations in the transportation, communications, broadcasting, federal banking and offshore sectors, as well as in Canada's three territories), and to other private sector organizations in provinces that have not enacted "substantially similar" legislation. It applies to personal information and health information that is collected, used or disclosed in the course of commercial activity that takes place across the Canadian border, between provinces, and within a Canadian province that has not enacted "substantially similar" legislation. To date, Alberta and British Columbia have joined Québec in enacting their own private sector privacy legislation. The Privacy Act gives individuals the right to access and request correction of personal information about themselves held by these federal government organizations.

70. The governments of all provinces and territories in Canada, except for Newfoundland and Labrador, also have legislation governing the collection, use and disclosure of personal information. The legislation varies from province to province, but the general right to access and correct personal information exists in all, and each has a commissioner or ombudsman who is authorised to handle complaints.

Court System

71. Canada's court system comprises four levels of courts with varying jurisdictions. First there are provincial and territorial courts, which handle the great majority of criminal cases and some civil cases (*e.g.* family law). Second are the provincial and territorial superior courts (which are federally constituted but provincially administrated, Courts under 96 of the Constitution). Generally, these

[8] See for instance Bill C-25, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the* Opening Statement by the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/parl/2006/parl_061213_e.asp.

courts deal with more serious crimes. They may also take appeals from provincial and territorial court judgments. On the same hierarchical level is the Federal Court, which is responsible for various matters of federal jurisdiction, including immigration and tax cases. At the next level in the hierarchy are the provincial and territorial courts of appeal (again federally constituted) and the Federal Court of Appeal. The final arbiter of the law and highest court of appeal for all matters is the Supreme Court of Canada. The Supreme Court of Canada also plays a special role as adviser to the federal government on interpretation of law. In such a case, a specific question reaches the Supreme Court not after making its way through the court system, but via a direct referral from the government. Such cases are often called "Supreme Court references." Under the Canadian Charter of Rights and Freedoms, individuals accused of the most serious criminal offences (classified as indictable offences) generally have the right to choose to be tried by a judge and jury.

Measures against corruption

72. Corruption is considered to be a serious offence and the Canadian authorities have indicated that it is given high priority in Canadian domestic law. The federal government has amended existing legislation (including the Income Tax Act) and enacted new legislation (Corruption of Foreign Public Officials Act), parliamentary rules and administrative provisions to prevent and prohibit corruption.

73. Most recently, the Government adopted the Federal Accountability Act which puts in place a five-year lobbying ban, eliminates corporate and union donations, and protects whistleblowers, among other reforms. It also updated indictable offences for fraud with respect to public money or money of a Crown corporation, as well as penalties for these offences that include fines and imprisonment. An amendment to the Criminal Code makes persons convicted of those fraud offences ineligible for employment by the Crown, as well as being unable to otherwise contract with the Crown or benefit from contracts between the government and another person.

74. Canada plays an active role in the fight against corruption in a number of fora, such as the United Nations (UN), the Organisation for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC) and the Organization of American States (OAS). In 1998, Canada ratified the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, thus triggering the convention's entry into force. Canada also ratified the OAS's Inter-American Convention Against Corruption at the OAS. More recently, efforts have focused on the negotiation of the UN Convention Against Corruption (UNCAC) on 31 October 2003, and Canada signed the UNCAC on 21 May 2004, and ratified it on October 2, 2007.

Ethics

75. Under the Constitution, the judiciary is separate from and independent of the other two branches of government, the executive and the legislative. Judicial independence is a guarantee that judges will make decisions free of influence and based solely on fact and law. It has three components: security of tenure, financial security and administrative independence. The Canadian Judicial Council, which is responsible for federally appointed judges, consists of the chief justices of all of the federal courts and provincial and territorial superior courts. The federal government created it to promote efficiency, consistency and good service in these courts. The Council has developed a set of ethical principles for judges, designed to assist judges in maintaining their independence, integrity and impartiality.

76. Prosecutors, known in Canada as Crown counsel, exercise their independence as representatives of an Attorney General. As such, the "independence" of Crown counsel is a delegated independence. Federal Crown counsel are obliged to make decisions in accordance with the policies of the Attorney General in the Federal Prosecution Deskbook. In general, each province also has a deskbook or a similar document to guide the provincial Crown counsel in their day-to-day work. Crown counsel is obliged to exercise independent judgment in making decisions. They are accountable for their decisions, and they must consult where required. Police officers are also subject to strict professional and ethical codes of conduct.

1.2 General Situation of Money Laundering and Financing of Terrorism

Predicate offences

77. Illicit proceeds from a variety of criminal activities contribute to the ongoing money laundering situation in Canada although drug trafficking is considered the source of much of the money laundered. Other sources of proceeds of crime include, but are not limited to, prostitution rings, contraband smuggling, illegal arms sales, migrant smuggling, and white-collar crime such as securities offences, real estate fraud, credit card fraud and telemarketing fraud.

78. The sales of illegal drugs in Canada amount to several billion dollars annually. Marijuana is one of the few drugs produced on a large scale in Canada. As such, an increasing amount of drugs is being smuggled into other countries, primarily the United States. There is evidence that in certain areas, both cocaine- and marijuana-trafficking organizations use money service businesses and currency exchanges to convert Canadian and U.S. dollars without going through formal exchange channels.

FINTRAC disclosures to law enforcement

79. Financial transactions in FINTRAC's drug-related case disclosures were cash intensive and, very often, of significant dollar value. Related financial activity frequently involved the use of foreign currency exchanges and casinos, and the physical or electronic movement of funds into or out of Canada. The vast majority of 2005/2006 disclosures fell into two readily identifiable categories of predicate offences: suspected illegal drugs and suspected fraud.

80. Suspected drug case disclosures were most prevalent and revealed the activity of small, homogenous networks of individuals. Suspected fraud cases were the largest in terms of scope, volume of transactions and dollar value. As opposed to the drug cases, suspected fraud cases appeared more complex and more organized. Many had a significant international dimension, and usually involved more than four businesses and four individuals. These companies often made heavy and uneconomical use of electronic funds transfers, and used multiple companies to conceal criminal funds.

Types of Criminal Organizations

81. Increasingly over the last several years, the Integrated Proceeds of Crime Units[9] (IPOC Units) have focused their investigation and assistance work on organized crime. Overall, more than 80% of the major files involved organized crime groups, climbing from 74% prior to 2001 to over 85% in the years since. Outlaw motorcycle gangs and other types of organised crime are present in Canada.

Money Laundering Methods

82. The money laundering methods used in Canada have remained relatively consistent in recent years. They essentially consist of: smuggling; money service businesses and currency exchanges; casinos; purchase of real estate; wire transfers; establishment of offshore corporations; credit cards, stored value cards and new payment methods; use of nominees; use of foreign bank accounts; use of professional services (lawyers, accountants, etc.); and reinvestment and distribution in illicit drugs.

83. At the placement stage, criminals are using money service businesses or casinos. Electronic funds transfers are being used for layering and at the integration stage, criminal proceeds are used to purchase high-value assets – such as cars, boats, jewellery, gold, diamonds and collectible items – in attempts to conceal the origin of the funds. Most recently, there have been signs that criminals are turning to such methods as Internet payments or cross-border movement of gold bullion.

---

[9] The IPOC Initiative brings together the skills, knowledge and abilities of a diverse group of experts including law enforcement officers, lawyers from the Department of Justice, forensic accountants and property managers from Public Works and Government Services Canada, Officers from Canada Border Services Agency, as well as Tax Agents from Canada Revenue Agency. The integration of the partner agencies facilitates a coordinated approach towards combating organized crime. For more information, see Section 2.6 of the report.

84. **Currency smuggling**. Cash continues to be a vehicle of choice for money laundering in Canada. Investigators regularly make large cash seizures of Canadian and U.S. currency and seize assets purchased with cash, such as real property, vehicles, personal property (jewellery, furniture and appliances), collectibles (antiques, coins, stamps) and other assets. Money launderers seem to be increasingly using the most rudimentary forms of money laundering, such as physically smuggling cash domestically and across international borders. Since 1994, nearly CAD 3 billion worth of contraband and cash has been seized as a result of the Pipeline/Convoy/Jetway Program[10].

85. **Money Service Businesses and Currency Exchanges**. Money service businesses (MSBs) and currency exchanges (F/Xs) play a role in money laundering activities, especially in large marijuana-producing areas, such as the Greater Vancouver region of British Columbia, where proceeds from sales in the U.S. must be converted into Canadian dollars. Both cocaine- and marijuana-trafficking organizations use some F/Xs to handle transactions involving different currencies used in cross-border activities. It appears that some foreign exchange dealers have also purposely dealt with other MSBs or foreign exchange dealers to avoid more traditional financial services, thereby limiting potential suspicions of links to criminal activity. Cheque cashing businesses have also been used as fronts for money laundering.

86. **Casinos**. Criminals use the Canadian casino industry extensively to launder illicit funds. They employ various techniques, including refining, exchanging currency, and chip purchases.

87. *Refining*. This term usually refers to the exchange of CAD 20 bills for CAD 50 or CAD 100 bills at the cash counter. In a variation often called the "ticket in ticket out" technique, criminals feed street-level money (CAD 5, CAD 10 and CAD 20 bills) into video lottery terminals. After minimal play, they cash the ticket stub at the counter for CAD 100 bills. In some instances, organized groups divide money to be refined among a number of individuals. They then enter the casino and go their own way. Once they have refined the money, they meet again outside the casino to assemble the total amount.

88. *Currency exchange*. Criminals are using casinos more frequently for currency exchange services. Several individuals associated with marijuana grow operations have used casinos to convert their proceeds of crime from U.S. currency into Canadian currency. Also, on occasion, they try to obtain casino cheques. In one case, a known chemical drug trafficker travelled to a casino outside his province of residence to exchange U.S. currency, obtained in Canada from drug-trafficking activities, for Canadian currency. Groups of people will also divide U.S. currency into small amounts to be exchanged for Canadian currency. They tend to use multiple casino locations. After exchanging the currencies, they meet again to assemble the total amount.

89. *Chip Purchases*. Buying casino chips in excess of the level of play and then cashing them out for a casino cheque is a known money laundering technique, frequently used by groups attempting to launder large sums of money. Some groups will travel outside their province of residence to use this technique. Reports from casinos to FINTRAC show that criminals tend to divide this money laundering activity into two separate tasks: some individuals buy casino chips, while others redeem these chips for a casino cheque. The group meets outside the casino to assemble the total amount. The separation of tasks makes it difficult to identify the individuals involved and to introduce detection methods. There is also evidence that casino chips are used as currency to purchase narcotics and contraband.

90. **Front companies**. Businesses that are especially attractive to money launderers are ones that customarily handle a high volume of cash transactions, such as retail stores, restaurants, bars, video rental stores, arcades, gas stations and food markets. As mentioned earlier, F/Xs, MSBs, and payday loan and cheque cashing businesses can also be used as fronts.

---

[10] The RCMP program's focus is the detection and seizure of contraband moving across Canada in cars and transport trucks.

91. **Real Estate**. Ongoing trends related to money laundering in the real estate sector include the following: (1) the use of nominees to register and make payments associated with real properties; (2) the use of facilitators — lawyers, real estate agents and mortgage brokers — to circumvent legal procedures, falsify documents and obscure the true nature of real estate transactions; and (3) the use of private mortgages (often involving the previous owner of a real property), and loan-back schemes.

92. **Gatekeepers**. Professionals such as accountants and lawyers act as "gatekeepers" when they provide access to the financial sector for their clients. This fact is open to abuse by criminals, who seek to use the gatekeeper to access the financial system, while themselves remaining anonymous. These professionals can also help clients move or conceal the proceeds of illegal activity.

93. **Credit Cards**. Credit cards are being used more frequently in every step of the money laundering process. In the initial placement stage, such techniques as "smurfing" or "structuring" can be used. Credit cards can be used to "commingle" legitimate revenues with proceeds of crime. At the layering stage, credit cards can be used in various ways: to transfer funds between accounts, to buy financial instruments and to carry out transactions in offshore jurisdictions. In the final integration stage, criminals primarily use credit cards to buy financial investments and luxury, "big ticket" items.

94. **Precious Stones**. Some investigations have revealed that the Canadian diamond industry is vulnerable to the threat of organized crime and money laundering.

95. **Stored Value and New Payment Methods**. Canadian law enforcement agencies have identified the use of credit cards, stored value cards and prepaid credit cards as an element of a growing number of money laundering schemes in Canada.

96. Internet payment systems (IPSs) are still quite new; one of the most popular systems, PayPal, was founded in 1998. IPSs allow users to send money around the world without going through the normal paths of the world's banking system. IPS accounts could be used to settle purchases of narcotics, contraband items, cigarettes, alcohol or stolen properties, for example.

97. **Trade-Based Money Laundering (TBML).** The Canadian law enforcement authorities have identified cases of TBML in relation to Colombian criminal organizations and cocaine importation in Canada.

98. **White-Label ATMs**. The Canadian law enforcement authorities have been confronted with cases involving White-Label automated teller machines (ATMs) which are owned and operated by independent service operators — individuals or companies — rather than banks. There are limited requirements on who can own or operate a white-label ATM due to a Competition Tribunal decision[11]. The owners of white-label ATMs have access cards that enable them to load cash into the machine. However, they are asked to identify the source of those funds only once, when they first set up the machine.

Terrorist Financing

99. Canadian authorities have identified a number of terrorist organisations operating in Canada. Investigations have shown that terrorist cells have a tendency to remain self-sufficient by generating funds locally. In some instances, they may do so by committing petty crimes, such as welfare fraud or credit card fraud. In other instances, cell members have started businesses to glean financial information from unsuspecting customers in order to clone credit cards and commit identity thefts. The RCMP has intelligence indicating that suspected terrorist entities in Canada are raising funds through drug trafficking or donating a portion of their criminal proceeds to support terrorism.

[11] In its decision of June 20, 1996, (CT-95 / 2) the Federal Competition Tribunal made an order that opened up the ATM market to independent operators. Prior to this decision, only banks and other deposit taking financial institutions had been allowed to join the *Interac Association* and operate ATMs.

100. Terrorists use techniques similar to those used by money launderers to evade authorities' attention and to protect the identity of their sponsors and the ultimate beneficiaries of the funds. Terrorist financing methods seen in Canada include the following: (1) the physical transportation of cash and other valuables; (2) the formal banking system; (3) MSBs and F/Xs; and (4) Internet value transfer systems. The most common venue for moving funds for the purpose of terrorism is the traditional banking system, since terrorism-related transactions can be camouflaged in the sheer volume of normal banking transactions.

101. In the course of fiscal year 2005/2006[12], FINTRAC made 34 case disclosures with a value of some CAD 256 million related to other threats to the security of Canada. FINTRAC observed that a large percentage of its case disclosures had an international component, where funds were wired to locations known to be terrorist hot spots. A number cases involved large cash deposits, made to personal or business accounts, where the funds were subsequently wire transferred out of the country.

102. **Value Cards.** Apart from wire transfers, value cards used to transfer funds for the purposes of terrorism are a relatively new trend in Canada and internationally. Value cards can be assets to terrorist supporters as they offer a convenient mechanism to quickly and easily transfer funds, often under the cloak of anonymity.

103. **Internet Payment Systems**. The newest terrorist financing method observed in RCMP investigations is the use of the Internet, where terrorist entities have set up accounts with electronic money services. These accounts can be credited from anywhere in the world by any person, and credits can be transferred from one account to another. These accounts can then be used to make purchases online. Credits can be purchased with cash at participating stores in the form of value cards in increments such as CAD10 or CAD20, similar to pre-paid telephone calling cards. Each card has a serial number. Once that number is entered on the money services website, the value of the card can be credited to a specific account. Such money services accounts facilitate the issuing of credit card accounts where electronic money services have agreements with banks. Users can transfer credits from these electronic money services accounts to credit card accounts, then use the credit cards in the normal fashion. These electronic money services are of particular concern because they are managed outside Canada.

104. **Charities**. Charities may collect donations from the public to support humanitarian causes overseas and forward the funds to overseas locations via the regulated banking system. At the receiving end, however, a portion of the funds may be diverted to support terrorism, with or without the complicity of Canadian donors and collectors. Analysis shows that charities and other non-profit organizations (NPOs) have figured in over one-third of FINTRAC disclosures related to suspected terrorist activity financing. These cases appeared to be associated with the collection of funds and financial movement suspected of being related to terrorist financing activity. These included: the use of multiple accounts by several NPOs, making the tracing of funds more difficult; the movement of funds to locations/countries of conflict, making it difficult to determine whether or not they are used for legitimate charitable purposes; and finally, the use of personal accounts by individuals or business accounts directly associated to NPOs, suggesting the possibility that accounts, other than the NPO accounts, are being used to collect and move funds.

Terrorist Financing Charges Brought Before Canadian Courts

105. Since the Anti-Terrorist Act came into effect in Canada in December 2001, there have been two instances where terrorist financing charges have been laid. Those two cases are currently before the courts.

106. The first case involves an individual named Momin Khawaja. He has been charged with seven offences under the Anti-Terrorist Act, including one charge related to terrorist financing under

[12] As is standard practice for the Government of Canada, fiscal years cover the period of April 1st to March 31st of the following year.

section 83.03 of the Criminal Code (providing property or services for terrorist purposes). This case has not been adjudicated yet. The case is linked to ongoing court proceedings in the U.K., where a terrorist allegedly attempted to build a 600-kilogram fertilizer-based bomb to attack targets in that country.

107. The second case involves the "Toronto 18" group. In June 2006, 18 individuals were arrested and charged in Canada with various offences under the Anti-Terrorist Act. Three of the 18 individuals were charged with terrorist financing offences under section 83.03 of the Criminal Code. None of these cases have been adjudicated yet. The most notable activities of this group included undergoing para-military training in Canada in December 2005, allegedly for terrorist purposes. This training allegedly spawned the formation of a sub-group in March 2006 that had the clear intention of building truck bombs to carry out terrorist attacks in the Toronto area.

1.3 Overview of the Financial Sector and DNFBP

Overview of the financial sector

Background

108. Overall, the financial sector contributes 6 percent of Canada's gross domestic product and has a yearly payroll of over CAD22 billion. The city of Toronto – located in Canada's most populous province, Ontario – is recognized as the centre of Canada's financial sector, with most of the large banks' headquarters, the country's equity exchanges (the Toronto Stock Exchange), the country's sole central securities depository (the Canadian Depository for Securities), the country's largest securities regulator (the Ontario Securities Commission), and offices of various regulators and other financial institutions. Two other major cities – Montréal, located in the province of Québec, and Vancouver, in the province of British Columbia – have vibrant financial sector activities.

109. While the financial sector in Canada is diverse and includes many service providers, it should be noted that the sector is significantly integrated, as different players offer similar services and "financial groups" or conglomerates offer a variety of financial products. Most notably, banks represent the largest portion of the Canadian financial services industry, reporting CAD1 257 billion in domestic assets in 2003, or over 70% of total assets within the financial sector. This integration is even more significant in light of the fact that Canada's six largest domestic banks account for the bulk of the activity, holding over 90% of all banking assets. Further, in the securities industry, the 11 largest firms (six of which are owned by the same largest domestic banks) account for 71% of total industry revenues. The five largest life insurance companies account for over 60% of the net premiums written by life insurers in Canada.

110. The following table compares the financial activities that define financial institutions under the FATF standards with financial sector entities subject to Canada's AML/CFT requirements:

Financial Activities as Defined by the FATF	Banks	Credit Unions, Caisses Populaires, Cooperative Credits Societies	Trust and Loan Companies	Investment Dealers	Mutual Fund Dealers	Portfolio Managers/ Investment Counsellors	Life Insurance Companies, Brokers and Agents	Money Service Businesses	Credit Card Companies	Crown Corporations That Accept Deposits	Canada Post (Money Orders)
1. Accepting deposits	✓	✓	✓							✓	
2. Lending	✓	✓	✓	✓	✓	✓	✓		✓		
3. Financial leasing	✓		✓				✓				
4. Transferring money or value	✓	✓	✓				✓	✓			
5. Issuing or managing means of payment	✓	✓	✓						✓		✓
6. Providing financial guarantees and commitments	✓	✓	✓				✓				
7. Trading: money market instruments, foreign exchange, securities, futures	✓	✓	✓	✓	✓	✓	✓				
8. Participating in securities issues	✓	✓	✓	✓	✓	✓	✓				
9. Managing portfolios	✓	✓	✓	✓	✓	✓	✓				
10. Safekeeping and custodial services	✓	✓	✓								
11. Investing and managing funds on behalf of others	✓	✓	✓	✓	✓	✓	✓				
12. Providing life insurance		✓					✓				
13. Changing money and currency	✓	✓	✓					✓			

Notes

1. There are businesses that specifically provide financial leasing arrangements. However, based on a risk analysis, the government has decided not to impose AML/CFT requirements on financial leasing companies.
2. Some businesses are involved solely in providing the credit card payment infrastructure to allow information to flow from the merchant to the company that manages the credit card accounts. These businesses have been excluded from the AML/CFT requirements due to their limited involvement in financial transactions.

Banking sector

111. *Background*. As of October 2006, there were 21 domestic banks, 25 foreign bank subsidiaries and 25 foreign bank branches operating in Canada (20 full-service branches and 5 lending branches). At the end of 2005, these institutions had over CAD2.1 trillion in global assets, including CAD1.5 trillion in domestic assets – accounting for about 70% of the total assets within the Canadian financial services sector. The six largest domestic banks account for the bulk of the activity, holding over 90% of banking assets as of the end of 2005[13]. The market concentration is as follows (December 2005):

[13] This does not include the assets of non-bank deposit-taking institutions, such as credit unions and caisses populaires.

Bank	Number of Deposit-taking branches in Canada	Number of ATMs in Canada	112. Assets (CAD billions)	Market Share (%)
Royal Bank of Canada	1 104	3 906	486	23.6
Toronto Dominion Bank	1 014	2 400	369	17.9
The Bank of Nova Scotia	950	2 500	324	15.8
Bank of Montreal	968	2 700	301	14.6
Canadian Imperial Bank of Commerce	1 100	4 000	289	14
National Bank of Canada	457	788	104	5.1
Total	5 593	15 994	1 872	91.0

Source: Office of the Superintendent of Financial Institutions.

113. Canada's banks operate through an extensive network that includes close to 6 000 branches and about 15 000 automated teller machines (ATMs) across the country. Canadians have access to an additional 35 000 ATMs operated by non-bank third parties. Canada has the highest number of ATMs per capita in the world and benefits from the highest penetration levels of electronic channels such as debit cards, Internet banking and telephone banking.

114. *Regulation and supervision*. Under the Bank Act, the federal government is responsible for the regulation of banks in Canada. However, given the diverse nature of the banks' activities, some of their subsidiary activities – such as trustee services and securities dealing – are provincially regulated. FINTRAC is responsible for ensuring compliance with AML/CFT requirements by banks and the Office of the Superintendent of Financial Institutions (OSFI) is the federal agency responsible for supervising banks in Canada. The Bank of Canada, Canada's central bank, works with other agencies and market participants to promote the safe and efficient operation of the financial system's key elements.

Credit Unions and *Caisses Populaires*

115. *Background.* Credit unions and *caisses populaires* are cooperative financial institutions owned and controlled by their members. Their ownership and corporate governance are based on cooperative principles, and their primary commitment is to serve their members' financial needs. In most provinces, each customer is required to become a member of the credit union or *caisse populaire*. Each member of a credit union or *caisse populaire* becomes a shareholder and has one vote, regardless of the size of deposit or share capital held. Members may run for election to the board, attend the annual meeting and vote on the election of directors and other matters. As shareholders, members are also entitled to yearly dividends and profit sharing.

116. In Québec, the provincially regulated Desjardins Group is the largest financial institution and consists of a network of *caisses populaires*. Outside Québec, all credit unions are shareholders in one of the nine provincial centrals, which are responsible for ensuring liquidity at the provincial level and providing services as a trade association. In turn, all nine provincial centrals are the primary shareholders of Credit Union Central of Canada (CUCC), which is responsible for establishing liquidity policy and overseeing liquidity maintenance at the national level.

117. Credit unions and *caisses populaires* are diversifying their services into non-traditional areas including full-service brokerage functions, mutual funds, commercial lending and wealth management. Some credit unions and *caisses populaires* are active in the insurance market as well. Credit union and caisse populaire membership was approximately 10.7 million by the end of 2005, or one third of Canada's population. Membership is highest in Québec, where 68 % of the population belongs to a caisse populaire.

118. At the end of 2005, the cooperative financial sector had 3 450 locations and about 4 800 ATMs. Credit unions and *caisses populaires* have also been purchasing bank branches, particularly in isolated

areas, helping to ensure that all Canadians continue to have access to financial services. At the end of 2005, Canada's credit union sector consisted of some 1 250 institutions. Credit unions and *caisses populaires* have maintained strong market shares in such key service areas as residential mortgage financing (14% as of 2005), consumer credit (7%) and deposit services (13%).

119. *Regulation and Supervision*. All credit unions and *caisses populaires* are provincially or territorially incorporated, as there is no federal legislation providing for the incorporation of credit unions or caisse populaires. As a result, the sector is regulated at the provincial / territorial level for prudential soundness and market conduct. As with the banking sector, FINTRAC is responsible for ensuring compliance with AML/CFT requirements by credit unions and *caisses populaires*. Both the provincial centrals that elected to be regulated by the federal level and the CUCC are supervised for prudential purposes by OSFI.

Insurance sector

120. In Canada, insurance companies are categorized as either life and health, or property and casualty. Consistent with FATF standards, AML/CFT requirements apply only to life and health insurance companies. Insurance products are sold by agents and brokers, some of them selling exclusively a single company's products (tied agents) while others sell insurance products of multiple companies (independent agents and brokers). AML/CFT requirements also directly apply to these insurance agents and brokers.

121. *Background*. In 2004, about 24 million Canadians and their dependants were covered by some form of life and health insurance. The total value of life insurance owned by Canadians was over CAD2.6 trillion. In 2004, Canada's life and health insurance industry comprised 105 firms, down from 120 firms in 2004 and 163 firms in 1990. This decline is largely the result of foreign insurers selling their operations to Canadian insurance companies, although there has been significant merger and acquisition activity among Canadian companies as well. In 2004, the 5 largest companies accounted for approximately 64% of the net premiums written by life insurers in Canada. Four of these firms, and 7 of the top 10 firms, are Canadian companies, as noted with a (C) in the following table. In the insurance industry, the market concentration is as follows (December 2005):

Company	Market share (%)
Great-West Life (C)	17.8
Manulife (C)	16.8
Sun Life (C)	15.4
Munich Re	6.9
Desjardins Life (C)	6.7
Total (top five)	**63.7**
Industry Total	**100.0**

Sources: Department of Finance calculations, using data from OSFI, l'Autorité des marchés financiers du Québec and corporate annual reports.

122. *Regulation and Supervision*. The federal and provincial governments share jurisdiction over the regulation of life insurance companies. In practice, the industry is largely regulated for financial soundness by OSFI, as federally incorporated companies account for over 90% of the total premium income of life insurers. While provinces reserve the power to ensure that federally incorporated companies conducting business in their jurisdictions are financially sound, all provinces except Québec accept federal regulation in this regard. FINTRAC is responsible for ensuring compliance with AML/CFT requirements for all life insurance companies.

Trust and Loan Companies

123. *Background*. Trust and loan companies offer services similar to those provided by banks; for instance, they accept deposits and make personal and mortgage loans. Trust companies, however, can

also administer estates, personal and institutional trusts, trusted pension plans and agency contracts. Although banks themselves are not permitted to undertake these activities directly, banks own the largest trust companies.

124. Before the 1990s, trust and loan companies – with their wide network of branches – provided major competition to the banks. In 1992, prohibitions on the ability of banks to acquire trust companies were removed. As a result the landscape in this industry changed dramatically. The recession and subsequent drop in the real estate market at that time also dealt a heavy blow to trust companies. As a result, the independent trust industry, as measured by assets owned, declined by more than half from 1990 to 1999.

125. Currently, 81 relatively small trust and loan companies operate in Canada. They account for less than 2% of the assets in the financial sector. The few remaining independent trust companies – among them Equitable Trust, Home Trust and Effort Trust – deal primarily in mortgage lending.

126. *Regulation and Supervision.* Both levels of government regulate trust and loan companies. Market conduct is regulated at the provincial level, and federally incorporated trust and loan companies are regulated for prudential purposes by OSFI under the Trust and Loan Companies Act. FINTRAC is responsible for ensuring compliance with AML/CFT requirements for all trust and loan companies.

Securities

127. *Background*. The Canadian securities industry plays a key role in Canada's financial services sector. The securities industry is made up of integrated, institutional and retail firms. Integrated firms offer products and services that cover all aspects of the industry for both the institutional and retail markets. Their functions include raising debt and equity capital for companies, helping governments raise capital to fund their operations and serving retail investors. Institutional firms provide services to large corporate clients such as pension funds, insurance companies, mutual fund organizations, banks and trust companies. Retail firms, which include full-service firms and discount brokers, offer a wide range of products and services to retail investors. Some 90 000 Canadians are licensed or registered as dealers and advisers participants.

128. There are a large number of firms in Canada that are involved in the securities industry. Generally speaking, the firms can be broken down into four categories: investment dealers firms that can sell all types of securities, mutual fund dealers firms that can only sell mutual fund products, investment counsel and portfolio management firms that provide investment advice and counselling, and restricted dealers/limited market dealers that can only sell restricted types of securities.

129. The number of firms participating in the Canadian securities industry has risen consistently throughout the last two decades. In the investment dealers firms category, the market is dominated by retail firms, followed by institutional firms and integrated firms. However, integrated securities firms, the six largest of which are owned by the big six domestic banks, account for 71% of total industry revenues. Retail firms accounted for 18% of revenues, while institutional firms accounted for 11%.

130. *Regulation*. In Canada, securities regulation is an area of provincial responsibility. FINTRAC is responsible for ensuring compliance with AML/CFT requirements for all securities dealers. Provincial and territorial securities regulatory authorities are members of Canadian Securities Administrators (CSA), an umbrella organization of the 13 regulators that serves as a forum for coordinating and harmonizing the regulation of Canadian capital markets. Securities regulators also delegate certain aspects of securities regulation to self-regulatory organizations, including the Investment Dealers Association of Canada, Market Regulation Services, Inc. and the Mutual Fund Dealers Association of Canada.

Money Service Businesses (MSBs) including Foreign Exchange Dealers

131. *Background*. Money service businesses (MSBs) in Canada refer to firms that remit or transmit funds by any means, through any person, entity or electronic funds transfer network. It also applies to those parties who issue or redeem money orders, travellers' cheques or other similar negotiable instruments. MSBs include alternative money remittance systems (such as hawala, hundi or chitti). They also include financial entities that remit or transfer funds – or issue or redeem money orders, travellers' cheques or other similar negotiable instruments – for anyone who is not an account holder. Banks, trust companies, *caisses populaires* and credit unions, for example, are only considered to be MSBs when they do occasional transactions, such as transactions for non-account holders.

132. The MSB sector includes currency exchange dealers and comprises many different businesses in Canada, including established money transfer companies such as Western Union and MoneyMart; and one-person businesses that offer money transfer or currency exchange services in tandem with another activity, such as operating a convenience store, video rental service or ethnic store. FINTRAC has identified some 700 businesses offering money transfer or currency exchange services throughout Canada. A number of these MSBs entered into a contract with agents to offer their products at various locations.

133. *Regulation and Supervision*. Although MSBs are not specifically covered by prudential or market conduct regulation in Canada, these businesses are subject to AML/CFT requirements and FINTRAC assesses AML/CFT compliance standards of MSBs.

Overview of the Designated Non-Financial Businesses and Professions (DNFBPs)

Background

134. The following designated non-financial businesses and professions (DNFBPs) are subject to Canada's AML/CFT requirements: casinos, real estate agents and accountants. In addition, the Government of Canada is currently in discussion with the following DNFBPs to cover these entities under AML/CFT requirements: lawyers, notaries (in Québec and British Columbia only) and dealers in precious metals and stones. Trust and company services providers are not separately recognised nor regulated as a separate business category and do not fall under the AML/CFT regime. Trust companies, accountants, lawyers and other independent legal professions provide such services.

135. The DNFBPs in Canada are as follows:

Reporting Entities	# of Reporting Entities	Primary Regulator	AML/CFT Regulator
Casinos	91	Provincial authorities	FINTRAC
Real estate agents	100 000	Provincial authorities and SRO	FINTRAC
Accountants	157 000	SRO	FINTRAC
Lawyers/notaries	89 000	SRO	FINTRAC
Dealers in precious metals and stones	4 000	None	FINTRAC

136. It should be noted that the number of reporting entities generally represents the entire sector. As some DNFBPs are subject to the PCMLTFA only in specific circumstances, only a small fraction of the sector will actually be required to comply with the AML/CFT requirements. For example, the majority of accountants are employed by corporations or in public practice, while only a small fraction of the 157 000 are actually employed within professional firms in private practice.

Casinos

137. *Permanent casinos*. Permanent casinos were established in Canada starting in the early 1990s. Currently, there are casinos in seven provinces (Nova Scotia, Québec, Ontario, Manitoba, Saskatchewan, Alberta and British Columbia) and one territory (Yukon). These include 34 commercial

casinos, 23 charity casinos, 22 Slot facilities and 8 First Nation casinos. Combined revenues for commercial casinos only were CAD3.5 billion in 2004 and CAD3.7 billion in 2005.

138. Gaming products include a wide variety of card games, roulette and slot machines. Varied financial services area available at casinos, including some that resemble services provided by financial institutions. Depending on the province, casinos can open customer deposit or credit accounts, have facilities for transmitting and receiving funds transfers directly from other institutions, and offer cheque cashing and foreign exchange dealer services. These services are ancillary to their core financial services, which are the sale and redemption of chips/tokens.

139. In Canada, provinces are responsible for licensing, operating and regulating legal forms of gaming, a responsibility that includes creating the rules for gaming products and financial services available within the casinos. FINTRAC is responsible for ensuring that casinos have implemented AML/CFT requirements outlined in the PCMLTFA. Gaming regulators are provincial agencies and exchange information through the Canadian Association of Gaming Regulators (CAGRA). This informal group provides a forum for exchanging regulatory information and techniques; collecting and disseminating regulatory and enforcement information, procedures and experiences; and providing ongoing education and training.

140. *Internet and cruise ship casinos*. Internet casinos do not fall in the scope of the PCMLTFA as no province has approved an Internet casino to date. Despite this, servers hosting illegal online casino gaming facilities exist within Canada. In addition, cruise ships can offer casino facilities under strict conditions in Canadian waters and are not covered by the AML/CFT legislation.

Real Estate Agents

141. The real estate industry in Canada consists of approximately 100 000 licensed real estate brokers and sales representatives working through 99 local real estate boards, 10 provincial associations, a territorial association and a national association. Brokers and sales representatives work with either a purchaser or a seller of real estate to manage a real estate transaction.

142. Provinces are responsible for the regulation of real estate industry professionals. In addition to provincial regulators, industry associations or boards at the national, provincial and local levels provide support, advocacy and training for real estate professionals. The Canadian Real Estate Association (CREA) comprises all provincial real estate associations and local boards throughout the country and is concerned with improving real estate practices across Canada. A key focus of CREA's activities is educating members about federal issues, including AML/CFT issues. There are 11 provincial and territorial real estate associations whose members are local real estate boards within the province or territory. The associations offer educational programs. Many provincial associations also provide real estate licensing courses. Local real estate boards maintain close contact with practising agents and provide detailed information about the local market. Local boards promote standards and make their members aware of publications and training courses available from federal and provincial associations. FINTRAC is responsible for ensuring that real estate agents have implemented the AML/CFT requirements outlined in the PCMLTFA.

Accountants

143. The accounting industry consists of firms and individuals providing a range of accounting services, which include auditing and reviewing financial records, preparing financial statements and accounting reports, developing budgets, designing accounting systems and providing advice on accounting matters. Accountants may also provide other related services, such as bookkeeping and payroll services, tax return preparation, and management consulting and insolvency services. In 2005, almost 22 000 establishments provided accounting services. The largest 20 firms generated 54% of the total operating revenues.

144. There are three main categories of professional accountants in Canada: chartered accountants (CAs), certified general accountants (CGAs) and certified management accountants (CMAs). There

are approximately 60 000 CAs, 51 000 CGAs and 35 000 CMAs. All of these accountants may be required to report to FINTRAC, depending on the types of financial transactions they undertake for clients. Each of the three categories of accountants is represented by a national association: the Canadian Institute of Chartered Accountants, the Certified General Accountants Association of Canada or the Society of Management Accountants of Canada. The associations representing CAs and CGAs are working to form a single body.

145. Provinces are primarily responsible for regulating the professional activities of accountants. Provincial accounting associations within each designation enforce the by-laws, codes of ethics and rules of professional conduct established by each designation to ensure that accountants are protecting the public interest. Provincial associations can discipline members for violations of the standards by imposing sanctions and revoking registration. FINTRAC is responsible for ensuring that accountants have implemented the AML/CFT requirements outlined in the PCMLTFA.

Lawyers and Notaries

Legal Counsel

146. The Federation of Law Societies of Canada is the national coordinating body of the 14 law societies in Canada (one for each of the 10 provinces except Québec, which has two societies and one for each of the three territories), which are responsible for regulating Canada's 88 500 lawyers and Québec's 3 500 notaries in the public interest. The Federation addresses key issues associated with the legal profession in Canada and sponsors two major national continuing legal education programs and intervenes in cases where protection of the public is of national concern.

147. The legal profession in Canada is governed by the laws, rules and regulations of the provincial or territorial law society of which a lawyer is a member. Provincial law societies regulate provincial legal professionals to ensure a competent and ethical bar. Provincial legislation authorises law societies to educate and license lawyers, and to regulate conduct, competence and capacity. Law society by-laws and rules of professional conduct set out the professional and ethical obligations of all members of the profession. Members failing to meet these obligations are subject to the provincial society's complaints and disciplinary process.

148. The Canadian Bar Association is a professional, voluntary organization formed in 1896. It was incorporated by a Special Act of Parliament on April 15, 1921. Today, the association represents some 35 000 lawyers, judges, notaries, law teachers and law students from across Canada. The main functions of the Canadian Bar Association are to act as an advocate and to provide personal and professional development and support.

Notaries

149. Unlike notaries in the province of Québec, who provide legal advice under Québec's civil code, notaries in British Columbia do not provide legal advice and are governed by the British Columbia Notaries Act. They are permitted to undertake only limited activities and they are allowed to hold trust accounts to carry out their duties.

150. It should be noted that notaries in provinces other than Québec and British Columbia are restricted to oath taking and document certification, except in Prince Edward Island where the profession is prohibited by law. These notaries do not conduct any financial transactions and the transfer of property is done exclusively through lawyers in these provinces.

151. British Columbia notaries are a self-governing profession under the Society of Notaries Public in British Columbia. The society enacts rules and by-laws, and regulates and sanctions its members, in a manner similar to that of a provincial law society. The governing legislation assigns the number of notaries that can be active in each of 84 specified provincial districts. The total number of notaries allowed in the province is 332.

Dealers in Precious Metals and Stones (DPMSs)

152. The precious metals and stones[14] industry in Canada consists of many stages and intermediaries. Canadian companies are active in sectors of the industry ranging from mining to retailing. While large firms predominate in the mining and production sector, dealers in precious metals and stones are primarily small firms. Of the more than 4 400 businesses in Canada involved in retailing, wholesaling, repairing and manufacturing jewellery, 90% have 20 or fewer employees. Estimates are that these activities employ 30 000 to 35 000 people, with over 60% working in the retail segment. Membership in industry associations and regulatory bodies is voluntary.

153. Canada has risen to become the world's third largest diamond-producing country by value. The rise in standing is due largely to the recovery of higher-quality stones than previously expected. The RCMP (see its Annual Report 2004) believes that accompanying the increase in diamond production is a corresponding increase in vulnerabilities and potential points of infiltration by organized crime groups. In general, more mines are in operation, more diamond-related companies are formed and a larger secondary diamond industry is developing. Organized crime interest in the diamond industry is monitored by the RCMP-led diamond protection service with the cooperation of the Canadian diamond and diamond exploratory industry.

154. The Canadian Jewellers Association is the dominant industry association, with a membership base that includes the majority of Canadian jewellery wholesalers and retailers. The Jewellers Vigilance Committee of Canada plays a role in preventing money laundering and fraud in the jewellery industry. As a voluntary, not-for-profit association, its mandate includes promoting consumer protection, publishing ethical guidelines, assisting law enforcement agencies and providing information on illegal activities, including fraud, smuggling and money laundering. It is funded in large part by industry contributions.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

Types of legal persons or arrangements recognised in Canada

155. Various types of business structures are available to Canadian entrepreneurs, including sole proprietorships, partnerships, limited or incorporated companies, and cooperatives. While the most appropriate corporate structure depends on factors such as the number of people involved, the type of business, tax issues, liability concerns and financial requirements of the firm, most Canadian businesses are incorporated to create a distinct legal entity separate from their owners. For this reason, most businesses elect to use the corporation as their legal form. There are an estimated 1.5 million corporations in Canada.

156. Incorporation may be done provincially, territorially or federally, giving a company the right to operate under its corporate name in a particular province or territory, or throughout Canada. However, a federally incorporated business must still register in each province in which it does business. A provincially or territorially incorporated corporation must also register in other provinces and territories, and can also conduct business in those other jurisdictions and nationally. While roughly 15% of corporations are incorporated federally, these firms are generally the largest companies and the most active ones, nationally and internationally. The main federal law establishing the legal and regulatory framework for corporations is the Canada Business Corporations Act (CBCA). Most provinces and territories have incorporation systems with measures broadly similar to the requirements in this Act. Cooperatives may also be incorporated either federally or provincially.

157. Most corporations in Canada are structured as private corporations, public corporations, unlimited liability companies or cooperatives, which are defined as follows:

[14] Precious metals and stones refer to high-value commodities used in the jewellery industry, such as gold, platinum, diamonds, tanzanite, emeralds, rubies and sapphires.

- *Private corporations*: One or more people can form a private corporation. A private corporation cannot sell shares or securities to the public. Most small businesses are private companies, and virtually all corporations start out that way.
- *Public corporations*: A public corporation is one that issues securities for public distribution. Besides filing incorporation documents, a public corporation must employ outside auditors and must distribute audited financial statements. It is subject to extensive disclosure and other requirements imposed by provincial securities regulators and corporate law. See section (c), below.
- *Unlimited liability companies*: These are currently permitted in Nova Scotia and Alberta only. They shelter shareholders from liability in most circumstances except on liquidation, when shareholders are liable for the excess of debts over assets.
- *Cooperatives*: These enterprises are jointly owned by the members who use their services. All members of a co-op are equal decision-makers in the cooperative, using a democratic system of one member, one vote. Federal cooperatives may issue shares and, therefore, have both members and shareholders.

158. Although the corporation is the most popular type of legal arrangement for Canadian businesses, the following types of legal persons and arrangements are also available in Canada:

- *Trusts*: A trust encompasses any relationship in which the legal and equitable (beneficial) titles to property are separated. Various types of trusts can be created in Canada. They are discussed in more detail in section 5.2 of this report.
- *Not-for-profits*: A not-for-profit organization is an organization not intending or intended to earn a profit for its members. Both provincial and federal not-for-profit legislation exists. The federal law governing not-for-profit organizations is the Canada Corporations Act, Part II.
- *Sole proprietorships*: A sole proprietorship is an unincorporated business that is owned by one individual and has no legal existence apart from the owner. Its liabilities are the owner's personal liabilities.
- *General partnerships*: A general partnership is the relationship between two or more persons who carry on a trade or business together. Each person contributes money, property, labour or skill, and expects to share in the profits and losses of the business.
- *Limited partnerships*: A limited partnership is an unincorporated business with at least one general partner and one or more limited partners. General partners have unlimited liability and limited partners have limited liability up to the amount of their investment.
- *Limited liability partnerships*: Most Canadian jurisdictions permit the formation of limited liability partnerships (LLPs). Under such a structure, which is generally restricted to eligible professions such as lawyers and accountants, a partner is not personally liable for any debts, obligations or liabilities of the LLP that arise from any negligent act by another partner or by any person under that partner's direct supervision and control. The law does not reduce or limit the liability of the firm. All of the firm's assets and insurance protection remain at risk. In addition, all partners of an LLP remain personally liable for their own actions and for the actions of those they directly supervise and control.

1.5 Overview of strategy to prevent money laundering and terrorist financing

a) AML/CFT Strategies and Priorities

159. Canada has continuously increased the responsibilities, funding and powers of domestic organizations working to identify, disrupt and dismantle money laundering and terrorist financing networks. It has also committed to engaging more actively in international fora.

160. Canada's AML/CFT regime has three primary objectives: detecting and deterring money laundering; preventing terrorist financing; and facilitating the investigation and prosecution of money laundering and terrorist financing offences. To do this, Canada has targeted the three stages of money laundering – placement, layering and integration – in its legislation (this report provides detailed information on this particular point).

Role of the Private Sector

161. As Canada moves forward with new legislation and regulations, some time and effort is invested in comprehensive discussions – with reporting entities in particular, and with the private sector generally – to get views and comments. These views are generally taken into account in rolling out new processes or requirements, or in amending existing ones.

Balance with Privacy Rights

162. The PCMLTFA strikes a careful balance between the privacy rights of Canadians and the needs of law enforcement and national security agencies. The Act upholds the principles outlined in the Canadian Charter of Rights and Freedoms (part of the Canadian Constitution), where Section 8 establishes a constitutional protection against unreasonable search and seizure, and the Privacy Act, which regulates the dissemination of personal information collected by government agencies. As a result, the PCMLTFA contains significant provisions specifically designed to balance the obligation to submit reports with an obligation to strictly control the release of information obtained from submitted reports.

Assessments

163. Canada's AML/CFT regime has undergone three separate, independent evaluations in recent years. Two of the evaluations – one performed by the Office of the Auditor General (OAG[15]) and the other by EKOS Research Associates, Inc., an independent research group – occurred in 2004[16]. The last assessment was a parliamentary review that a committee of the Senate of Canada carried out in the summer of 2006; its interim report was tabled in October 2006 (see Section 6.1 of the report for further information).

Parliamentary Review of the PCMLTFA

164. Section 72 of the PCMLTFA calls for a parliamentary review of the administration and operation of the Act five years after the legislation was passed. Therefore, in the summer of 2006, the Standing Senate Committee on Banking, Trade and Commerce held hearings in which witnesses from both the private sector and federal public service provided comments on Canada's AML/CFT regime and its effectiveness.

165. The Senate Committee tabled a report[17] that highlighted the need for the AML/CFT regime to meet domestic requirements, as well as the importance of meeting international obligations to ensure that the world is "safer and more secure." The report reiterated the importance of an appropriate balance between providing law enforcement and security agencies with the proper information to fight money laundering and terrorist financing, and protecting the privacy rights of Canadians. The review was conducted in the knowledge that the federal government had proposed legislative changes stemming from a consultation paper released by the Department of Finance in June 2005. The

---

15 To ensure accountability and transparency, the Office of the Auditor General (OAG) independently audits federal government departments and agencies, most Crown corporations, and many other federal organizations. The OAG reports publicly up to four times a year to the House of Commons on matters that the Auditor General believes should be brought to the attention of the House. In addition, the OAG testifies before parliamentary committees on the Office's audits.

16 See report at: http://www.fin.gc.ca/activty/pubs/nicml-incba_e.pdf.

17 *Stemming the Flow of Illicit Money: A Priority for Canada*. Parliamentary Review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Ottawa: Standing Senate Committee on Banking, Trade and Commerce, October 2006.

recommendations made in the Senate report reinforced the proposed amendments to the PCMLTFA (see below).

Recent Initiatives

166. In June 2005, the federal government issued a consultation paper "*Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*". Extensive consultations took place with financial intermediaries and professional groups following the release of the paper. A description of the key amendments to the PCMLTFA enacted on December 14, 2006 can be found in Section 3 of the report.

167. Further to the above amendments, complementary initiatives are planned (for instance, FINTRAC is working to provide more frequent and more valuable feedback to reporting entities and FINTRAC will issue guidance for new requirements including the reporting of suspicious attempted transactions, the implementation of the risk-based approach and the treatment of politically exposed persons and for new reporting sectors)[18]..

The Institutional Framework for Combating Money Laundering and Terrorist Financing

b) Key Partners in the AML/CFT Regime

168. The current AML/CFT regime is grounded in the "National Initiative to Combat Money Laundering" (NICML), which was established in 2000. The original partners of the NICML included the following.

Department of Finance

169. Along with broad responsibility for regulation of the financial sector, the Minister of Finance has had – since 1999 – responsibility for Canada's AML/CFT regime (originally known as the NICML). However, as noted, a number of key departments and agencies in the federal government are responsible for implementing different aspects of the regime.

170. As the lead organization, the Department of Finance develops AML/CFT policy, including the PCMLTFA and its associated regulations. The department coordinates all activities under the AML/CFT regime, including consultations with stakeholders. It does so in conjunction with other government departments and agencies, provincial governments, the private sector – including industry associations – and non-governmental bodies. The department also participates in strategic domestic and international activities that support the Canadian government's AML/CFT commitments. Specifically, the department leads the Canadian delegation to the FATF, the Caribbean Financial Action Task Force and the Asia/Pacific Group on Money Laundering.

Financial Transactions and Reports Analysis Centre (FINTRAC)

171. FINTRAC, Canada's financial intelligence unit was established in July 2000 under the PCMLTFA to help detect and deter money laundering and terrorist financing activity. FINTRAC is an independent government agency that reports to Parliament through the Minister of Finance. It operates as an independent agency at arm's length from law enforcement, security and other agencies to which it discloses information (see further developments in Section 2.5 of the report).

18 In addition, an AML/CFT advisory committee was created in late 2007, and comprises both public and private sector representatives. This body will work to enhance cooperation and coordination (see Section 6.1 of the report).

Department of Justice

172. A single minister, holding the twin titles of Minister of Justice and Attorney General of Canada, heads the Department of Justice. Criminal law, as a statute of national jurisdiction exclusively under the constitutionally legislative authority of Canada, includes criminal offences and criminal procedure. Authority to develop that law and procedure is given to the minister of justice. The minister is responsible for the Criminal Code of Canada and the development of criminal offences, as well as all laws on criminal procedure. The minister is responsible for the Mutual Legal Assistance in Criminal Matters Act and the Extradition Act.

Public Prosecution Service of Canada (PPSC)

173. The PPSC is a federal government organization, created on December 12, 2006, pursuant to the *Director of Public Prosecutions Act*. The PPSC fulfills the responsibilities of the Attorney General of Canada in the discharge of his criminal law mandate by prosecuting criminal offences under federal jurisdiction and by contributing to strengthening the criminal justice system. The PPSC is an independent organization, reporting to Parliament through the Attorney General of Canada.

Public Safety and Emergency Preparedness Canada (PSEPC)

174. PSEPC is responsible for providing support to the minister of public safety on all matters of public safety and national security, including money laundering and terrorist financing. PSEPC support is multi-dimensional and touches on many aspects of Canada's AML/CFT regime. PSEPC provides the minister with policy development and advice on AML/CFT policies and programs. In addition, PSEPC also works with other regime partners – the RCMP, CSIS and CBSA – that are accountable to the minister on issues of horizontal or mutual interest. PSEPC chairs the Interdepartmental Working Group on Terrorist Listings, in support of the minister's statutory responsibilities to recommend entities to be listed under the Criminal Code.

175. The Minister of Public Safety, with the Minister of Revenue, is also responsible for a critical aspect of Canada's AML/CFT regime under the Charities Registration (Security Information) Act (CRSIA) to prevent the use of charities for terrorist financing.

Canada Revenue Agency (CRA)

176. One of the CRA's responsibilities is to ensure that each person pays the taxes associated with all of his or her income and activities. If FINTRAC discloses information suspected of being relevant to the investigation or prosecution of a money laundering offence or terrorist activity financing offence to law enforcement, and also determines that the information is relevant to an offence of evading or attempting to evade taxes or duties under an Act of Parliament, it will disclose the same information to the CRA. The information received from FINTRAC may lead the CRA to initiate a new enforcement action or serve as additional information in support of an ongoing enforcement action.

177. The CRA's mandate to administer the Income Tax Act in respect of registered charities gives it a responsibility to ensure that the tax benefits reserved for Canada's charities are not used to provide terrorist financing in the guise of charity. The enactment of the CRSIA as Part V of the Anti-Terrorism Act redefined the CRA's role and the importance of protecting the integrity of Canada's registration system for charities.

Canadian Security Intelligence Service (CSIS)

178. CSIS has a mandate to collect, analyze, and retain information or intelligence on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. CSIS is the Government of Canada's principal advisor on national security. CSIS's role in the regime is to receive FINTRAC disclosures regarding suspected threats to the security of Canada and to gather intelligence,

which may be passed to the RCMP for potential criminal proceedings. CSIS also provides voluntary information reports to FINTRAC.

Royal Canadian Mounted Police (RCMP)

179. As the national police force – and as the provincial or local police force, in many jurisdictions across Canada – the RCMP plays a fundamental role in Canada's AML/CFT regime. The RCMP investigates money laundering and terrorist financing cases and acts as a liaison in exchanging criminal intelligence with international police forces. RCMP liaison officers around the globe assist Canada in pursuing AML/CFT cases.

180. In response to the September 11, 2001 terrorist attacks on the U.S., the RCMP Financial Intelligence Branch was created to address the issue of terrorist fundraising. This intelligence/investigative body was established to support national security efforts to identify financial intelligence and enforcement opportunities related to terrorist financing, as well as to provide direction and support to field units. An Internet investigation team was established as part of the branch to investigate terrorist fundraising on the Internet.

181. Finally, the RCMP plays a significant training and awareness-raising role among AML/CFT partners and the private sector, and in international fora. Indeed, the RCMP has provided direct technical assistance and training to police forces in developing countries to help them conduct AML and terrorist financing investigations and enhance their investigative techniques.

Canada Border Services Agency (CBSA)

182. The PCMLTFA requires that all large amounts of currency and monetary instruments imported or exported to or from Canada, including those transported by mail, be reported to a border services officer (BSO). In addition, BSOs now have the responsibility to enforce the physical cross-border reporting initiative, which includes the authority to examine baggage and conveyances, and to question and search individuals for unreported or falsely reported currency and monetary instruments. CBSA also plays a key role in denying admission to Canadian territory to non-citizens who pose security threats to Canada.

Office of the Superintendent of Financial Institutions (OSFI)

183. OSFI regulates and supervises federally regulated financial institutions, which comprise banks, federally regulated insurance companies, cooperative credit associations, and federally regulated trust and loan companies. It administers financial institution governing statutes (the Bank Act, the Insurance Companies Act, the Trust and Loan Companies Act, and the Cooperative Credit Associations Act). OSFI issues guidance to federally regulated financial institutions, as well as warning notices regarding entities that it believes may be of concern to the business community and the public.

Other Participants in AML/CFT Efforts

184. In addition to the nine key partners in the AML/CFT regime discussed above, other departments also participate in the fight against money laundering and terrorist financing.

Department of Foreign Affairs and International Trade

185. The Department of Foreign Affairs and International Trade (DFAIT) has responsibility for international elements of Canada's efforts to address money laundering and terrorist financing. The Minister of Foreign Affairs is responsible for the designation of entities and individuals in Canada associated with terrorist activities listed by the United Nations 1267 Sanctions Committee or under Resolution 1373 of the United Nations Security Council. This designation effectively freezes their

assets and prohibits fundraising on their behalf. DFAIT is also the primary interlocutor and negotiator for Canada in terms of international conventions and treaties that address money laundering, terrorist financing and other related public safety issues, such as bribery, corruption or illicit drugs.

Industry Canada

186. The Minister of Industry is responsible for the Canada Business Corporations Act, under which companies can federally incorporate their business with Industry Canada. When a business does so, the department collects information about the enterprise, including the business name and address, and information about the directors.

Office of the Privacy Commissioner of Canada

187. The Office of the Privacy Commissioner plays an important role in ensuring that the necessary safeguards protecting privacy are upheld. The Privacy Commissioner is an officer of Parliament who reports directly to the House of Commons and the Senate and who regularly provides views on Canada's AML/CFT regime. The Privacy Commissioner has the ability to audit FINTRAC and financial institutions etc. to ensure privacy laws are respected.

Public Works and Government Services Canada, Seized Property Management Directorate

188. The Seized Property Management Directorate is responsible for the management and disposition of assets – including movable property, real estate, cash and securities – that have been seized or forfeited for illicit drug trafficking and money laundering offences. It also acts as a holding facility for currency and monetary instrument seizures.

Provincial Bodies

189. A number of provincial department and agencies, regulators and self-regulatory organizations have a role to play in the fight against money laundering and terrorist financing. These organizations include the following (further information is provided in Sections 2, 3 and 4 of the report):

- Provincial, territorial and municipal law enforcement agencies, such as the Ontario Provincial Police, la Sûreté du Québec and city police forces, who participate as part of various IPOC units.
- Provincial Crown prosecutors and courts.
- Provincial and territorial financial sector regulators, such as the Financial Services Commission of Ontario, the Ontario Securities Commission, l'Autorité des marchés financiers du Québec and the British Columbia Gaming Commission.
- Self-regulatory organizations, such as the Law Society of Upper Canada, the Investment Dealers Association and Canadian Institute of Chartered Accountants.

c) Approach concerning risk (see Section 3.1 of the report)

Application of AML/CFT obligations to certain sectors

190. In Canada, certain financial institutions as defined by the FATF Recommendations are not covered by the AML/CFT regime since Canada considers that these entities pose little or no threat of money laundering/terrorist financing. Canada's risk based approach is centred around the principle that financials sectors are brought into the AML/CFT regime if there is a proven risk of ML/TF. This differs from the FATF approach to risk as defined in the Methodology where a list of activities and operations must be covered by the AML/CFT regime unless there is a proven low risk of ML or TF (see Section 3.1 of the report for further analysis).

Risk-based approach taken by financial institutions

191. The government takes risks into account at various levels for regulatory purposes. For example, the PCMLTFA requires reporting entities to file reports with FINTRAC for cash transactions of CAD10 000 or more. However, a specific risk assessment identified legitimate cash-intensive businesses, such as big box stores and grocery store chains, whose large cash transactions would not have to be reported to FINTRAC. Further, reporting entities are not required to identify clients that are publicly listed companies in Canada, since such companies already have to meet comprehensive disclosure and other filing requirements set by provincial securities regulators.

Use of a Risk-Based Approach in Supervision of Compliance by Competent Authorities

192. The competent authorities use a risk-based approach when supervising reporting entities for compliance with the legislation. FINTRAC and OSFI have taken a risk-based approach in developing and implementing their supervisory programs (see Section 3.1 of the report).

d) Progress since the last mutual evaluation or assessment

193. Since the last mutual evaluation report (1997), Canada has implemented a large number of developments in its AML/CFT regime both in terms of statutory amendments and structural changes. The most high-profile development was the enactment of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. This report discusses these changes in detail.

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1 & R.2)

2.1.1 Description and Analysis

Recommendation 1

194. In Canada, all criminal offences must be set out in national law, as passed by the Parliament of Canada. Most criminal offences are found in the Criminal Code[19]. However other federal laws, including a number of profit motivated criminal offences (for example drug offences) are established in other federal laws, such as the Controlled Drugs and Substances Act[20].

195. *Criminalisation of ML on the basis of the UN Conventions*. The Vienna and Palermo conventions require countries to establish as a criminal offense the following intentional acts: conversion or transfer of proceeds; concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to proceeds; and the acquisition, possession or use of proceeds (Article 3(1)(b)(i)-(ii) of Vienna; Article 6(1)(a)(i)-(ii) of Palermo). This obligation is subject to the fundamental/constitutional principles and basic concepts of the country's legal system (Article 2(1), Vienna convention; Article 6(1), Palermo convention).

196. In Canada, the money laundering offence, which can be found under section 462.31 of the Criminal Code (CC) is part of a broad proceeds of crime regime designed to cover all obligations in the 1988 Vienna Convention and the 2000 Palermo Convention to criminalize the concealment or laundering of proceeds of crime and the possession of such proceeds or criminal instrumentalities. Section 462.31 encompasses acts of using, transferring the possession of, sending or delivering to any person or place, transporting, transmitting, altering, disposing of or otherwise dealings with, in any manner and by any means, any property or any proceeds of any property. The prohibited activity must be undertaken with an intent to conceal or convert that property or those proceeds, and knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or

19 R.S.C. , 1985, c. C-46 as amended-See http://laws.justice.gc.ca/en/C-46/index.html.

20 S.C. 1996, Chap. 19, see http://laws.justice.gc.ca/en/c-38.8/229593.html.

indirectly as a result of the commission of a designated offence. A designated offence means *(a) any offence that may be prosecuted as an indictable offence under the Criminal Code or any other Act of the Parliament, other than an indictable offence prescribed by regulation or (b) a conspiracy or an attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to, an offence referred to in paragraph a)* (see s. 462.3 (1) CC). The possession of proceeds of crime is covered in section 354(1) of the Criminal Code. That section makes it an offence to knowingly possess money or property derived directly or indirectly from any indictable Canadian criminal offence or any foreign offence, that had it been committed in Canada would have been an indictable offence in Canada. There is also an offence covering the importation of property derived from foreign crimes into Canada (s.357).

197. The elements of Canada's primary money laundering offence are for the most part criminalised in line with all of the requirements of the Vienna and Palermo Conventions. However, in one aspect the Canadian money laundering offence in Section 462.31 requires an additional mental element that is not required under either Convention. Namely, Section 462.31 requires that the person handling property or proceeds of property has the intent to conceal or convert same. ("Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property ***with intent to conceal or convert that property or those proceeds***, knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of (*a*) the commission in Canada of a designated offence; or (*b*) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence" (emphasis supplied).

198. The Conventions require the conversion or transfer of property to be an offence where the defendant knows that the property involved is the proceeds of crime and does so for one of the following two purposes: (1) concealing or disguising its illicit origin; *or* (2) for the purpose of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action (Palermo, Article 6(1)(a)(i) and Vienna, Article 3(1)(b)(i)). However, section 461.31 sets out only one purpose element (for the purpose of concealing or disguising its illicit origin) instead of the two alternatives required by the Convention. Canada notes that in the alternative the relevant conduct may be covered by s.354, though the assessment team believes that will not be the case for many of the factual scenarios criminalised by s.462.31. This is a minor technical deficiency that could inhibit some prosecutions.

199. *Property that represents the proceeds of crime*. As indicated above, the money laundering offence extends to property or proceeds of property that was obtained or derived directly or indirectly as a result of the commission of a designated offence. The concept of "property" is broadly defined in section 2 of the Criminal Code and meets the FATF requirements. Under this section, property includes "*(a) real and personal property of every description and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, and (b) property originally in the possession or under the control of any person, and any property into or for which it has been converted or exchanged and anything acquired at any time by the conversion or exchange"*.

200. The Criminal Code includes a wide definition of possession in subsection 4(3). It provides that a person possesses anything when he has it in his personal possession or knowingly (i) has it in the actual possession or custody of another person, or (ii) has it in any place, whether or not that place belongs to or is occupied by him, for the use or benefit of himself or of another person. Where one of two or more persons has anything in his custody or possession, with the knowledge and consent of the rest, it shall be deemed to be in the custody and possession of each and all of them.

201. It is not necessary that a person is convicted of a predicate offence when proving that property is the proceeds of crime, only proof that the property emanates from a criminal acquisition is sufficient (beyond a reasonable doubt is the standard of proof). This principle has been confirmed by case law.

Further clarity is provided in the forfeiture provision in subsection 462.37(2) CC: *(2) where the evidence does not establish to the satisfaction of the court that the designated offence of which the offender is convicted, or discharged under section 730, was committed in relation to property in respect of which an order of forfeiture would otherwise be made under subsection (1) but the court is satisfied, beyond a reasonable doubt, that that property is proceeds of crime, the court may make an order of forfeiture under subsection (1) in relation to that property.* The targeted property is subject to forfeiture without a conviction for the predicate offence.

202. *Predicate offences for ML*. Canada essentially applies an all crime approach to its money laundering scheme by including all indictable offences *i.e.* those offences subject to imprisonment for more than six months, as designated (or predicate) offences (see the definition above) with some exceptions. Summary conviction offences as those with a fine of not more than two thousand dollars or imprisonment for up to six months or to both. For example, the financing of terrorism is an indictable offence subject to up to 10 years in prison.

203. In addition, the Canadian offence classification system includes a hybrid offence classification approach to some offences. That approach provides that the offence may be treated as a less serious summary conviction offence or a more serious indictable offence at the discretion of the prosecutor. For example, theft can be an indictable offence with varying jail terms or a summary conviction offence depending on the amount stolen. Section 34 of the Interpretation Act (that provides interpretation of legislation) applies to hybrid offences, providing: "*(1) where an enactment creates an offence, (a) the offence is deemed to be an indictable offence if the enactment provides that the offender may be prosecuted for the offence by indictment; (b) the offence is deemed to be one for which the offender is punishable on summary conviction if there is nothing in the context to indicate that the offence is an indictable offence; and (c) if the offence is one for which the offender may be prosecuted by indictment or for which the offender is punishable on summary conviction, no person shall be considered to have been convicted of an indictable offence by reason only of having been convicted of the offence on summary conviction"*. As a result, any hybrid offence is treated as an indictable offence until the prosecutor makes an election.

204. The offence of possession of property derived from a crime under Section 354 and Section 357 are essential elements in Canada's broader money laundering and proceeds of crime approach. The possession offence covers the possession of any property or thing, or any proceeds of any property or thing, where there is knowledge that all or any part of the property, thing, or of the proceeds was obtained directly or indirectly from: (a) the commission in Canada of an offence punishable by indictment; or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence punishable by indictment. Again, the predicate offences for the offence of possession of property derived from crime cover all serious (indictable) offences in Canada. There is no excluded predicate offence for the offence of possession of property derived from crime. This offence, which is broad in scope, also covers factual circumstances that amount to possession of stolen property offences *e.g.* stolen motor vehicles, or simple cases of persons caught in possession of small quantities of drugs and cash. While the assessors were advised that a large majority of s.354 cases dealt with such conduct, a statistical breakdown of s. 354 offences prosecuted by the Attorney General of Canada indicated that none of those offences were cases where the particular charge was receiving of stolen property.

205. There is also a separate criminal offence, which is a designated offence for the purposes of the definition of proceeds of crime, in section 357 of the Criminal Code. Section 357 creates an offence where importing anything into Canada that a person obtained outside Canada by an act that, if it had been committed in Canada, would have been the offence of theft or an offence under Section 342 (theft, forgery, etc., of credit card) or 354 (possession of property obtained by crime). This is an indictable offence in Canada.

206. As mentioned earlier, the money laundering offence specifies that the predicate offence must be a designated offence. The definition of designated offences, in section 462.3 of the Criminal Code,

provides that some indictable offences, prescribed by regulation, will not be designated offences for the purposes of money laundering[21]. The following provides the list of excluded offences:

The indictable offences under the following Acts are excluded from the definition of "designated offence" in subsection 462.3(1) of the Criminal Code:

(a) Budget Implementation Act, 2000.
(b) Canada Agricultural Products Act.
(c) Copyright Act.
(d) Excise Act, except for the indictable offences under subsections 233(1) and 240(1).
(e) Excise Tax Act.
(f) Feeds Act.
(g) Fertilizers Act.
(h) Foreign Publishers Advertising Services Act.
(i) Health of Animals Act.
(j) Income Tax Act.
(k) Meat Inspection Act.
(l) Nuclear Safety and Control Act, except for the indictable offence under section 50 (offence to possess certain nuclear substances, etc.
(m) Plant Protection Act.
(n) Seeds Act.

207. Indictable offences in these 14 Acts have been excluded from the scope of relevant indictable offences for the purposes of Section 462.31 ML offences as these offences are penalized through other Acts. However, if charges were instituted under other federal laws, including the Criminal Code, and they were prosecuted by indictment, they would fall within the money laundering offence since all other indictable offences are covered by the money laundering offence[22]. The absence of provisions on copyright offences in the Criminal Code means that copyright related offences are not predicate offences for Section 462.31 ML, although offences involving trademarks and trade descriptions (Sections 406 to 410, Criminal Code) are predicate offences for Section 462.31 ML. Canada takes the position that Section 354 criminalizes possession of the proceeds of copyright offences. However, Section 354 covers only one portion of the three types of ML offences that Canada should criminalize under the relevant Conventions, and thus gaps still exist as Section 354 does not cover all varieties of ML offences contemplated by this Recommendation. Although this constitutes a minor technical failure and is a relatively small gap in the regime, this deficiency should be addressed by the Canadian authorities. To avoid any potential gaps of this sort, the assessors suggest the removal of the list of excluded offences and recommend that Canada include all indictable offences (including those prescribed by regulations) as predicate offences for Section 462.31 ML.

208. The scope of the offence category lists, as set out in the FATF 40 Recommendation's Glossary Description of Designated Categories of Offences, are covered as money laundering offences in the Criminal Code and offences in specific federal statutes. The FATF categories are cross-referenced to some of the Criminal Code or other indictable offences, in relevant federal laws, as follows:

- Participation in an organised criminal group and racketeering- *Criminal Code sections 467.11, 467.12 & 467.1.*
- Terrorism, including terrorist financing- *Criminal Code sections 83.02, 83.03, 83.94 83.12 and 83.18 to 83.231.*

[21] Regulations Excluding Certain Indictable Offences from the Definition of "Designated Offence". SOR/2002-63 see- http://canadagazette.gc.ca/partII/2002/20020213/html/sor63-e.html.

[22] Canadian provinces and territories also enact laws that contain provincial offence provisions. No province may enact a criminal law, with the result that none of the provincial offences are offences for the purposes of money laundering or possession of property derived from crime provisions in the Criminal Code.

- Trafficking in human beings and migrant smuggling- *Criminal Code section 279.01 and sections 117 & 118 of the Immigration and Refugee Protection Act.*
- Sexual exploitation, including sexual exploitation of children- *Criminal Code section 212.*
- Illicit trafficking in narcotic drugs and psychotropic substances -*Sections 5 to 7 of the Controlled Drugs and Substances Act.*
- Illicit arms trafficking- *Criminal Code sections 99 to 108.*
- Illicit trafficking in stolen and other goods- *Criminal Code sections 354 & 462.31.*
- Corruption and bribery- *Criminal Code sections 119 to 125; 426 and Section 3 of the Corruption of Foreign Public Officials Act.*
- Fraud- *Criminal Code sections 341, 342(3), 371, 374 to 376, 378, 380, 381, 385 to 394 and 396.*
- Counterfeiting currency- *Criminal Code sections 449 to 460.*
- Counterfeiting and piracy of products- *Criminal Code sections 406 to 411.*
- Environmental crime- *Sections 272 to 274 and 276 of the Canadian Environmental Protection Act, 1999.*
- Murder, grievous bodily injury- *Criminal Code sections 229 to 240 and 264.1 to 273.*
- Kidnapping, illegal restraint and hostage-taking- *Criminal Code sections 279 to 283.*
- Robbery or theft- *Criminal Code sections 343 and 322 to 334.*
- Smuggling-*Sections 153 to 160 of the Customs Act.*
- Extortion- *Criminal Code section 346.*
- Forgery- *Criminal Code sections 57, 342 & 342.1 369 to 378.*
- Piracy- *Criminal Code sections 74 & 75.*
- Insider trading and market manipulation- *Criminal Code section 382.1.*

209. *Extraterritorial predicate offences*. Jurisdiction to prosecute the money laundering and possession of property offences under Canadian law is established so long as the foreign conduct would have been an offence had it occurred in Canada (and whether or not the offence constitutes an offence in the foreign country). This explicit extension of jurisdiction is permitted under the general rule found in subsection 6(2) of the Criminal Code, which states that no person can be convicted of an offence committed outside Canada unless federal law explicitly extends jurisdiction to do so.

210. As is the case with money laundering, Canadian courts may assert criminal jurisdiction over acts taking place in another state if they are connected to other acts that take place in Canada in furtherance of criminal behaviour, or if the acts in the other state have some injurious consequence within Canada. For example, as defined in subsection 4(3) of the Criminal Code, possession of property derived from crime or the laundering of such property give rise to jurisdiction in Canada.

211. The leading Supreme Court of Canada case on jurisdiction is R. v. Libman, [1985] 2 S.C.R. 178, in which the Court held that "all that is necessary to make an offence subject to the jurisdiction of our courts is that a significant portion of the activities constituting that offence took place in Canada. As it is put by modern academics, it is sufficient that there be a "real and substantial link" between an offence and this country, a test well-known in public and private international law. (par. 74)". The Court stated that Canada "should not be indifferent to the protection of the public in other countries" (par.77).

212. The determination of what a "significant portion" or a "real and substantial link" will depend on the particular fact situation, but does not depend on an extensive physical connection between the offence and Canada[23]. In summary, if the crime giving rise to the possession of property occurred outside of Canada but the possession element of the offence occurs in Canada, the crime could be prosecuted in Canada.

[23] See Canada (Human Rights Commission) v. Canadian Liberty Net, [1988] 1 S.C.R. 626; United States of America v. Lépine, [1994] 1 S.C.R. 286 and R v. Hammerbeck (1993), R.F.L. (3d) 265, 26 B.C.C.A.

213. *Self-money laundering*. In Canada, an individual who launders their own proceeds commits a money laundering offence given the extensive definition of "person" and "property" in section 2 of the Criminal Code. Canadian case law supports this position[24].

214. *Ancillary offences*. Canada's Criminal Code includes ancillary or inchoate criminal offences. Section 21 CC criminalizes being party, which includes aiding and abetting, to the offence of money laundering[25]. Section 22 CC provides for a general counselling offence[26]. Section 23 CC provides for accessory after the fact. The *actus reus* and *mens rea* of an attempt are set out in Section 24(1) CC that creates liability for attempting to commit an offence regardless of whether it was, in fact, possible to commit the offence. It is a question of law whether an act or omission by a person who has the intent to commit an offence is mere preparation or an attempt to commit the offence. To illustrate how the courts normally draw the line between mere preparation and attempt, see the following two cases: R. v. Deutsch, [1986] 2 S.C.R. 2 and R. v. Sorrell and Bondett (1978), 41 C.C.C. (2d) 9.

215. Section 465 CC contains the relevant provisions on conspiracy. Section 465(1)(c) states that everyone who conspires with anyone to commit an indictable offence is guilty of an indictable offence and liable to the same punishment as that to which an accused who is guilty of the offence would, on conviction, be liable. Section 465(3) makes it an offence to conspire in Canada to do anything abroad referred to in section 465(1), if it is an offence under the laws of that place. Additionally, it is an offence under section 465(4) to conspire outside Canada to do anything in Canada referred to in 465(1). Canada explains that it is not a defence to a charge of conspiracy that an accused, having agreed to carry out the unlawful act with the intention to carry out the common design, later withdraws from the conspiracy, as the offence is complete upon the making of the agreement. Further to subsection 34(2) of the Interpretation Act, section 465 of the Criminal Code (conspiracy) would apply to the offences in the Act.

216. Section 463 CC sets out the sentence for anyone convicted of the inchoate offence. Section 464 provides for the offence of counselling offences that are not committed. Finally, to clarify any possible ambiguity in respect to the concept of designated offences for money laundering, Section 462.3 (b) CC refers to inchoate offences in the definition of "designated offences". Therefore, every indictable offence, including ancillary offences, is covered by the money laundering offence, unless they have been excluded by regulation as described above.

217. *Additional elements*. As discussed above, Canada's money laundering and possession of property offences establish jurisdiction so long as the foreign conduct would have been an offence if it had occurred in Canada. Whether or not the offence constitutes an offence in the foreign country is not taken into account. More specifically, the concept of "proceeds of crime" establishes the parameters of

---

[24] See R. v. Falahatchia (1995) 99 C.C.C. (3d) 420 (On C.A.); R. v. Cazzetta [2003] J.Q. N. 43 (Que C.A.).

[25] Section 21 (1) CC: "Everyone is a party to an offence who (a) actually commits it; (b) does or omits to do anything for the purpose of aiding any person to commit it; or (c) abets any person in committing it. (2) Where two or more persons form an intention in common to carry out an unlawful offence and to assist each other therein and any one of them, in carrying out the common purpose, commits an offence, each of them who knew or ought to have known that the commission of the offence would be a probable consequence of carrying out the common purpose is a party to that offence". For case law, see R. V. Fraser (1984), 13 C.C.C. (3d) 292 (B.C.C.A.) or R. V. Dunlop and Sylvester [1979] 2 S.C.R. 881 or R. V. Thatcher [1987] 1 S.C.R. 652.

[26] Section 22 CC: 22. (1) Where a person counsels another person to be a party to an offence and that other person is afterwards a party to that offence, the person who counselled is a party to that offence, notwithstanding that the offence was committed in a way different from that which was counselled. (2) Every one who counsels another person to be a party to an offence is a party to every offence that the other commits in consequence of the counselling that the person who counselled knew or ought to have known was likely to be committed in consequence of the counselling.

the nature of the property that may be relevant to a money laundering offence[27]. See also Sections 462.31 and 354(1) and Section 357 CC as described above).

Recommendation 2

218. *Natural persons that knowingly engage in ML activities*. Authority to prosecute a natural person has always existed in Canada. The criminal offences of money laundering and possession of property derived from crime clarify any ambiguity. They provide that the offence covers activity undertaken by "everyone". The Criminal Code defines "everyone" in section 2 in an expansive fashion to include an "organization". An "organization" is itself defined to mean a public body, body corporate, society, company, firm, partnership, trade union, municipality, or an association of persons that is created for a common purpose and has an operational structure. The concept includes natural and legal persons.

219. As regards knowledge, or intent, it is an essential element in all criminal offences, including the money laundering and possession of property derived from crime offences. Since these are criminal offences, the onus to prove the knowledge element beyond a reasonable doubt rests on the prosecution (known as the Crown in Canada). However, in Canada the prosecutor does not have to establish actual knowledge. A prosecutor can establish the required knowledge element by establishing that the accused was wilfully blind or reckless. In R. v. Sansregret, [1985] 1 S.C.R. 570, the Supreme Court held that recklessness and wilful blindness can be used to establish the criminal law requirement for intention. In addition, for the money laundering offence in Section 462.31 of the Criminal Code, further clarification was provided by an amendment adding the words "or believing" to the knowledge element in that offence[28].

220. *Inference from objective factual circumstances*. Canadian prosecutors may rely upon both direct and circumstantial evidence to prove their case in any criminal prosecution. The authority to use such evidence was recently canvassed by the Manitoba Court of Appeal in R. v. Jenner (2005), 195 C.C.C. (3d) 364 at paragraph 20: *"…It was contended that proof of knowledge as to the character of the substance would place upon the Crown a difficult, if not impossible, burden. I cannot agree with the contention. Proof of knowledge is no more difficult than the proof of intent in any criminal prosecution. Knowledge, like intent, is a state of mind. It cannot, generally speaking, be proved as a fact but can only be inferred from facts which are proved. A jury, on properly established facts, should experience no more difficulty in finding knowledge than it does in finding intent*".

221. The Ontario Court of Appeal, in R. v. Aiello (1978), 38 C.C.C. (2d) 485 affirmed 46 C.C.C. (2d) 128n (S.C.C.), opined, at page 488, on the same point: *"…The trial Judge in our view should have further directed the jury that it was not necessary for the prosecution to prove the required knowledge by direct evidence, but that it could be inferred from the surrounding circumstances, such as, for example, the finding of the drug on the accused person in his trouser pant leg, his evidence that he figured that it must be a drug, the circumstances in which, and the place where he had picked up the package*".

222. The ability to rely on circumstantial evidence in a ML case is more specifically enhanced by Section 462.39 CC, which provides that: "*…the court may infer that property was obtained or derived as a result of the commission of a designated offence where evidence establishes that the value, after the commission of that offence, of all the property of the person alleged to have committed the offence exceeds the value of all the property of that person before the commission of that offence and the court*

---

[27] Section 462.3 CC: "*in this Part, "proceeds of crime" means any property, benefit or advantage, within or outside Canada, obtained or derived directly or indirectly as a result of (a) the commission in Canada of a designated offence, or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence*".

[28] An amendment in May 1997 added "belief" to the money laundering offence, so as to overcome the problem that "sting" operations could not be conducted by the police as the use of government money as "proceeds" meant that no offence was committed.

is satisfied that the income of that person from sources unrelated to designated offences committed by that person cannot reasonably account for such an increase in value".

223. *Criminal liability for legal persons*. Authority to prosecute a legal person exists in Canada. As indicated above, the scope of any relevant criminal offence is found in the specific money laundering and possession of property derived from crime offences. These offences refer to "everyone" and the Criminal Code defines "everyone" to include an "organization". Section 2 defines "organization" expansively to mean a public body, a body corporate, a society, a company, a firm, a partnership, a trade union or an unincorporated association.

224. Following recent modifications to the Criminal Code to deal with legal persons, corporations may be held criminally liable: (a) as a result of the actions of those who oversee day-to-day operations but who may not be directors or executives; (b) when officers with executive or operational authority intentionally commit, or direct employees to commit, crimes to benefit the organization; (c) when officers with executive or operational authority become aware of offences being committed by other employees but do not take action to stop them; and (d) when the actions of those with authority and other employees, taken as a whole, demonstrate a lack of care that constitutes criminal negligence.

225. Fines imposed against corporations that are found criminally liable can range from up to CAD100 000 for a prosecution on summary conviction, a less serious offence, to no set limit for indictable or more serious offences. The Criminal Code was also amended with respect to sentencing and the concept of corporate probation[29].

226. *Sanctions for ML*. Canada's possession of property derived from crime (Subsection 354(1) CC carries a maximum penalty of 10 years imprisonment if the property involved is a "testamentary instrument," or exceeds CAD5 000 in value (otherwise it is only a 2 year maximum), as does the separate offence of bringing into Canada property obtained by crime (Section 357). The Section 462.31 ML offence also carries a maximum penalty of 10 years, regardless of the value of the property involved. A person convicted of an attempt to commit such a crime or as an accessory after the fact may be subjected to a penalty of one-half of that available for actual committing the underlying offence (Section 463). If the charge is for counselling an offence that is not committed, the maximum penalty is the same as if the person was convicted of an attempt, namely one-half of that available for actual committing the underlying offence (Section 464). If the person is convicted of a conspiracy, the maximum penalty is five years imprisonment (subparagraph 465(1)(b)(ii)). It should also be noted that the proceeds of crime are forfeitable. If the property that would otherwise be forfeitable is no longer available for forfeiture, Section 462.37 provides for a fine in lieu of forfeiture alternative with consecutive jail time in default ranging from a maximum of six months to ten years depending on the amount of the fine.

227. All of the referenced terms of incarceration can apply to a natural person, but it is not possible to incarcerate a legal person. As a result, the Criminal Code deals with this reality in Sections 718.21 and 735(1) and imposes an additional fine ranging from a maximum of CAD100 000 for summary conviction offences to an amount determined by the court for the more serious indictable offences.

228. Limited information was given to the assessment team on ML sentencing (a sample of 28 ML sentences from 1993 to 2006 was provided and no example was given of a Section 462.31 ML sentence of a legal person). In the examples that were provided, penalties for Section 462.31 ML ranged from 6 months (for CAD29 000 laundered) to 10 years (conviction for laundering proceeds, conspiracy to launder, drug trafficking and CAD30 million laundered). No comprehensive statistics are available on Section 462.31 ML sentencing, nor on possession of proceeds cases and the data provided is a snap shot of cases that cover a long period of time. A lack of statistics on sanctions imposed on natural and legal persons means that the effectiveness of sanctions for ML cannot be properly assessed.

[29] See Section 718.21CC which sets out sentencing factors that the court must consider while sections 721, 730, 732.1, 734 and 735 updated other sentencing considerations for convicted corporations.

Statistics (Recommendation 32)

229. The following table provides the number of charges pursuant to Section 462(31) CC (ML offence) and the outcomes of the trials.

Year	2003/2004	2004/2005	2005/2006	**Total**
Charges laid down pursuant to S.462(31) CC	220	292	211	**723**
Guilty pursuant to S.462(31) CC	5	6	10	**21**
Committed for trial (ongoing case) pursuant to 462(31) CC	8	6	3	**17**

230. There is no figure on the number of Section 462.31 ML cases that are either self-money laundering or third-party money laundering.

231. The following table provides the number of charges pursuant to Section 354 (possession of property obtained by crime) and the outcomes of the trials. The assessment team was not provided with information to indicate how many of these cases were more in the nature of simple possession of stolen goods type offences as compared to possession of the proceeds of serious offences *i.e.* what is considered as traditional money laundering. Nor was data available on how many offences involved more than CCAD5 000 in assets. The team was advised that the data in the s. 354 table includes a large majority of minor possession offences involving either minor cases of possession of small quantities of drugs and cash or receipt of stolen goods. Canada analysed a sample of approximately 1 000 cases which showed a large majority were linked to funds derived from drug offences and a much smaller number were linked to thefts.

Year	2003/2004	2004/2005	2005/2006	**Total**
Charges laid down pursuant to S.354 CC	24 434	24 410	16 971	**65 815**
Guilty pursuant to S.354 CC	3 962	4 025	2 163	**10 150**
Committed for trial (ongoing case) pursuant to S.354 CC	587	579	249	**1 415**

232. The following table provides an overview of the number of charges laid by the RCMP's IPOC units in money laundering and possession of proceeds of crime cases. The other category includes weapons related charges, drug related charges, breach of probation and fraud charges, to name a few.

Charge Type	**Files**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**Total**
Possession of POC	Number	28	231	157	78	31	16	**541**
	Percent	52.8%	40.3%	52.3%	17.5%	10.8%	34.9%	**31.7%**
Money laundering	Number	4	319	109	57	97	25	**611**
	Percent	7.6%	55.7%	36.3%	12.8%	33.7%	54.4%	**35.8%**
Other	Number	21	23	34	311	160	5	**554**
	Percent	39.6%	4.0%	11.3%	69.7%	55.6%	10.9%	**32.5%**
TOTAL	Number	**53**	**573**	**300**	**446**	**288**	**46**	**1,706**
	Percent	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

2.1.2 Recommendations and Comments

233. The anti-money laundering offences are comprehensive and Canada generally meets the requirements under Recommendations 1 and 2. The primary ML offence set forth in Section 462.31 is broad in its scope, but the assessors recommend that all indictable offences, including those prescribed by regulations, should be predicate offences for ML, since copyright offences are currently not covered by this provision. Conversely, the Section 354 possession of property offence covers property from all indictable offences, and the two offences should thus be consistent in their scope. The Section 462.31 offence is technically inconsistent with the relevant UN Conventions in that it injects an additional specific intent mental element that is not required by those Conventions. Section 462.31 should be rewritten to make clear that the perpetrator need not have the specific intent to conceal (or disguise), but that that instead that only "purpose" or result of the particular transaction must be such. In addition, Canada should craft language that makes sure Section 462.31 covers transfers and conversions that have as their purpose helping any person who is involved in the commission of a predicate offence or offences evade the legal consequences of his or her actions. Alternatively, Canada should consider removing the purpose element from Section 462.31 completely, thus making it consistent with s.354, albeit it broader than the Convention requirements.

234. The assessment team has concerns on whether prosecutions of ML offences have been effectively implemented. A reasonable number of charges are laid for section 462.31 ML offences (723 from 2003 to 2006) in a country where, based on the information made available, money laundering is considered to be a significant criminal problem. However, the number of convictions in that period for that offence is very limited, 21 from 2003 to 2006. In addition there are 17 charges currently committed to trial. This means less than 3% of Section 462.31 charges laid have resulted in convictions. There have been more than 65,000 charges laid under s.354 from 2003 to 2006, with 10 150 convictions for that offence. Another 1 415 charges are pending trial. The team was advised that this was because prosecutors either pursue predicate offences or a s.354 possession offence which they are more familiar with, and which is easier to prove as it does not require the additional intent element set forth in Section 462.31. Canada advised the assessment team that the volume of s.354 offences charged and convicted shows that it is aggressively pursuing the crime of money laundering. However, in summary, the team is concerned about the overall effectiveness of action taken to convict money launderers, due to the following considerations:

(a) The very low number of convictions for s.462.31 (which is the offence focussed on active money laundering).

(b) The information which suggests that the bulk of s.354 offences are not ML offences as contemplated by FATF (an examination of the Criminal Code shows that this offence, which was created in 1974, is closely linked to actions to be taken in relation to possession of stolen property – Canada also indicated in paragraph 152 above that s.354 (and also s.462.31) are offences dealing with illicit trafficking in stolen goods and other property) or that the charges laid under s.354 often involve minor offence.

(c) Other important government agencies that combat ML and TF are focused on s.462.31 e.g.FINTRAC can only make disclosures to law enforcement when it has reason to believe a TF offence or s.462.31 ML offence is implicated, but cannot make such a disclosure when a s.354 offence is suspected. Moreover, when FINTRAC receives law enforcement VIRS, it focuses its analytical resources on VIRS that involve s.462.31 offences, and not VIRS that involve s.354 offences. IPOC units lay more s.462.31 charges than s. 354 charges in spite of the 99 to 1 ratio in favour of s.354 that exists elsewhere.

235. (d) If the property is valued at less than CAD5 000 and does not involve a "testamentary instrument" the maximum penalty is 2 years as opposed to the 10 year sentence that is available for the more serious Section 354 offences as well as all Section 462.31 offences.

(e) Even if the assessment team where to credit s.354 offences as ML offences in all cases (which it does not), the fact remains that only 17% of s. 354 charges laid resulted in convictions or have been committed to trial, which is still very low.

236. The emphasis on and preference for pursuing the predicate crimes and the offence of possession of property obtained by crime, in addition to the lack of comprehensive data on investigations and prosecutions at federal and provincial levels, lead the evaluation team to conclude that the statutes available for countering ML are not being used as effectively as they could be. Canada should develop a more proactive approach to prosecuting the specific money laundering charge under s.462.31.

2.1.3 Compliance with Recommendations 1 & 2

Rec.	Rating	Summary of factors underlying ratings
R.1	LC	▪ The ML offence does not cover all designated categories of predicate offences (copyright related offences). ▪ Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions or R.1. ▪ The number of convictions for Section 462.31 ML is very low, as is the percentage of convictions in comparison to charges laid.
R.2	LC	▪ The number of convictions for Section 462.31 ML is very low. ▪ Due to the lack of data on ML sentencing, is not possible to assess whether natural and legal persons are subject to effective, proportionate and dissuasive sanctions for ML.

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

237. *The terrorist financing offence*. In 2001, the Anti-terrorism Act (ATA) amended the Criminal Code to create three criminal offences related to the financing of terrorism. These amendments to the Criminal Code enabled Canada to implement international obligations under the UN Security Council Resolution 1373 and the UN International Convention for the Suppression of the Financing of Terrorism. The three terrorist financing offences under the Code are broadly defined and operate in an expansive fashion.

238. Section 83.02 of the Criminal Code makes it an offence to "wilfully and without lawful justification or excuse, directly or indirectly provide or collect property intending or knowing that it will be used, in whole or in part, to carry out a "terrorist activity" as defined in section 83.01(1) or any other act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act".

239.

240. Section 83.03 makes it an offence to "directly or indirectly collect property or to make available, provide, or invite a person to provide property or financial or other related services: (a) intending or knowing that they be used, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity, or for the purpose of "benefiting" a person who is facilitating or carrying out a terrorist activity; or, (b) knowing that, in whole or part, they will be used by or will benefit a terrorist group".

241. Section 83.04 makes it an offence to "*use property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity*". It is also an offence under this section to possess property, intending or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity.

242. Under Section 83.01 of the Criminal Code, "terrorist activity" means:

> (*a*) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences:
>
> (i) the offences referred to in subsection 7(2) that implement the *Convention for the Suppression of Unlawful Seizure of Aircraft*, signed at The Hague on December 16, 1970,

(ii) the offences referred to in subsection 7(2) that implement the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on September 23, 1971,

(iii) the offences referred to in subsection 7(3) that implement the *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents*, adopted by the General Assembly of the United Nations on December 14, 1973,

(iv) the offences referred to in subsection 7(3.1) that implement the *International Convention against the Taking of Hostages*, adopted by the General Assembly of the United Nations on December 17, 1979,

(v) the offences referred to in subsection 7(3.4) or (3.6) that implement the *Convention on the Physical Protection of Nuclear Material*, done at Vienna and New York on March 3, 1980,

(vi) the offences referred to in subsection 7(2) that implement the *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*, supplementary to the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on February 24, 1988,

(vii) the offences referred to in subsection 7(2.1) that implement the *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, done at Rome on March 10, 1988,

(viii) the offences referred to in subsection 7(2.1) or (2.2) that implement the *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf*, done at Rome on March 10, 1988,

(ix) the offences referred to in subsection 7(3.72) that implement the *International Convention for the Suppression of Terrorist Bombings*, adopted by the General Assembly of the United Nations on December 15, 1997, and

(x) the offences referred to in subsection 7(3.73) that implement the *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations on December 9, 1999, or

(*b*) an act or omission, in or outside Canada,

(i) that is committed

(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and

(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and

(ii) that intentionally

(A) causes death or serious bodily harm to a person by the use of violence,

(B) endangers a person's life,

(C) causes a serious risk to the health or safety of the public or any segment of the public,

(D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or

(E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),

and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.

243. In line with the UN Convention, safeguards have been incorporated into the ATA with respect to the terrorist financing offences, including the legal threshold of knowledge and intention. In addition, the Attorney General's consent is required to institute proceedings.

244. In Canada's criminal code, the provisions that criminalize terrorist financing use the term "property", as opposed to the term "funds" that is used in the TF convention. As seen in Sections 83.02, 83.03, and 83.04 of the Criminal Code, terrorist financing offences refer to "property", which is defined in section 2 as including *(a) real and personal property of every description and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, (b) property originally in the possession or under the control of any person, and any property into or for which it has been converted or exchanged and anything acquired at any time by the conversion or exchange"* (see Section 2.1 of the report). This definition is very broad and is consistent with the definition of "funds" in the Terrorist Financing Convention.

245. The TF Convention states that the terrorist financing offence need not require that the funds: (i) were actually used to carry out or attempt a terrorist act(s); or (ii) be linked to a specific terrorist act(s). The wording in the Canadian terrorist financing offence makes reference to the collection of property with the intention that it be used, or knowing that it will be used for terrorist activity. The threshold of criminal conduct is met here if there is an intention to carry out terrorist activity and therefore does not require that funds are actually used to carry out the activity. This is consistent with the requirements of the TF Convention and the Recommendation. The Code, unlike the TF Convention, does not make reference to specific acts of terrorism, the use of funds by a terrorist organisation or to an individual terrorist, but uses the broadly defined term "terrorist activity". Terrorist activity as defined in the code includes an act or omission, committed to achieve specific ends. The Code also requires that the act be concluded with intention to achieve specific listed outcomes. The Code does not make direct reference to a specific terrorist individual, but the existing terrorist offences in part II.1 of the Criminal Code, together with the definition and jurisdiction sections in s. 7 can be used to define and cover the issue. The terrorist offences in Part II.1 of the Code and the reference to "terrorist activity" are specifically designed to interrelate. A terrorist activity is an act or omission, in other words conduct. That conduct is undertaken by individuals and terrorist groups. Indeed "terrorist groups" are defined as an "entity". An "entity" is defined as a person and the definition includes an "organization". Section 2 of the Criminal Code reinforces this by providing an expansive definition of an "organization" as any legal person. Finally every criminal offence that could be committed is structured to cover natural and legal persons by the word "everyone". As a result a specific terrorist individual is included in every relevant offence.

246. Section 24 of the Criminal Code provides that "every one who, having an intent to commit an offence, does or omits to do anything for the purpose of carrying out his intention is guilty of an attempt to commit the offence whether or not it was possible under the circumstances to commit the offence." As such, the Criminal Code offences referred to above include attempts to commit them. Further, the definition of "terrorism offence" in the Criminal Code (see above) specifically includes attempts to commit them as part of the definition of this term.

247. The terrorism financing offences include a conspiracy or attempt to commit, being an accessory after the fact or counselling in relation to the offences. This covers "participating as an accomplice" in the Terrorist Financing Convention. Further, sections 21 (parties to an offence), 22 (counselling an

offence), 23 (accessory after the fact), and 465 (conspiracy) of the Criminal Code confirm that the specific offences include being an "accomplice".

248. Regarding organizing or directing others to commit an offence, section 83.03 in its prohibition of inviting others to provide property, financial or other services would cover most of this activity. Further, the offence of instructing to carry out activity for a terrorist group (section 83.21) and instructing to carry out terrorist activity (section 83.22) could cover as well the activity of organizing or directing others to commit terrorist financing offences.

249. Finally, the terrorist financing offences and the definitions of terrorist activity and terrorist group provide that individuals alone or as part of a group of persons that act intentionally to further criminal purposes would be covered.

250. *FT as a predicate offence for ML*. Terrorism offences, as indictable offences under the Criminal Code, are predicate offences to which Canada's proceeds of crime legislation apply. These offences fall within the definition of "designated offences" found in section 462.3 of the Criminal Code. A conspiracy, an attempt, being an accessory after the fact in relation to, or counselling in relation to, a terrorism offence are also "designated offences" that are subject to this regime.

251. The terrorist financing regime in the Criminal Code includes provisions on the freezing, seizure/restraint, forfeiture and disposition of property as well. They are found in sections 83.08-83.15 and link with the existing provisions on proceeds of crime and forfeiture of offence-related property (Part XII.2 and sections 490.1-490.9).

252. *Jurisdiction over FT offences*. The specific terrorism financing offences apply in Canada regardless of whether the person alleged to have committed the offence is in Canada or in a different country than that of the terrorist group or in which the terrorist activity has or will occur. In addition, terrorism financing offences could be prosecuted, under certain limitations as required by the general principle of international criminal law jurisdiction, even if these offences have taken place in another country (see Sections 3.73 to 3.75 of the Criminal Code).

253. Finally, of note is the expansive territorial reach of section 354 (possession of property obtained by crime includes act or omission outside Canada) and section 462.3 ("proceeds of crime" includes any property outside Canada derived from an act or omission occurring outside Canada).

254. *Inference from objective factual circumstances*. In Canada, the intentional element of terrorism offences may be inferred from objective factual circumstances that are themselves proven through admissible evidence.

255. It is a well-established principle of criminal evidence that "any fact from which may be inferred a fact in issue or a fact relevant to an issue is admissible; it is called "circumstantial evidence" (McWilliams' Canadian Criminal Evidence, 4th ed., 2003). As regards knowledge, or intent, it is an essential element in all criminal offences, including the money laundering and possession of property derived from crime offences. Since these are criminal offences, the onus to prove the knowledge element beyond a reasonable doubt rests on the prosecution (known as the Crown in Canada). However, in Canada the prosecutor does not have to establish actual knowledge. A prosecutor can establish the required knowledge element by establishing that the accused was wilfully blind or reckless. In R. v. Sansregret, [1985] 1 S.C.R. 570, the Supreme Court held that recklessness and wilful blindness can be used to establish the criminal law requirement for intention. The rules of evidence apply with equal force to proof by circumstantial evidence as to proof by direct evidence. The evidence in both instances must be equally credible, admissible and relevant[30].

[30] See Re R. v. Truscott [1967] 2 C.C.C. 285 (S.C.C.).

256. *Criminal liability of legal persons.* In Canada, criminal liability for terrorism offences, including financing of terrorist activities and groups, applies to "everyone", which includes "an organization", defined in section 2 of the Criminal Code (see Section 2.1 of the report).

257. Section 22.2 defines the liability of an organization as a party to an offence, where the offence is one that requires proof of fault other than negligence. The prosecution must prove that one of the "senior officers" at least had the intent in part to benefit the organization and either: (a) such officer acting within the scope of his authority was a party to the offence; (b) the senior officer had the requisite mens rea (mental element) for the offence, was within the scope of his authority and directed others to do the required act, or (c) the officer did not take reasonable measures to stop the commission of the offence by others. In addition, corporations may be held criminally liable for actions of employees who are their directing minds[31].

258. *Parallel criminal, civil or administrative proceedings.* There is no prohibition on such parallel proceedings in Canada. Section 11 of the Criminal Code provides that "no civil remedy for an act or omission is suspended or affected by reason that the act or omission is a criminal offence."

259. *Sanctions*. A person or organization that is convicted of a terrorist financing offence (sections 83.02, 83.03 or 83.04 of the Criminal Code) may be sentenced to up to 10 years imprisonment in Canada.

260. The actual sentence imposed will reflect the purpose and principles of sentencing set out in sections 718 and following of the Criminal Code. The purpose of sentencing is to contribute to respect for the law and maintenance of a just, peaceful and safe society by imposing just sanctions that denounce unlawful conduct, deter the offender and others from committing offences, separate the offenders from society where necessary, assist in rehabilitating offenders and provide reparation for harm done to victims or to the community. The fundamental principle of sentencing is that a sentence must be proportionate to the gravity of the offence and degree of responsibility of the offender.

261. The fact that the offence is a terrorist offence is an aggravating circumstance that should result in an increase in the sentence (section 718.2(a)(v) of the Criminal Code.)

262. In respect of criminal liability of legal persons (organizations), section 735 of the Criminal Code provides for fines in lieu of imprisonment in certain circumstances.

Statistics (Recommendation 32)

263. The RCMP's National Security branch maintains a summary of key activities and milestones which contain the following statistics for a two month period:

- Number of terrorist groups disrupted.
- Cases submitted for prosecutions.
- Number of active anti-terrorism financing investigations.
- Number of tactical intelligence packages disseminated to field units.
- Number of disclosures to FINTRAC.
- Number of hours spent listing terrorist entities, and the number of charities de-registered.

264. For example for the time period of 1 April – 30 June 2006, the following statistics were recorded:

Active Anti-Terrorist Financing Investigations in Canada –	52
Disclosures to FINTRAC	7
Number of requests responding to Foreign Governments –	72
Number of Files Successfully concluded	601

[31] See Canadian Dredge & Dock Co. v. The Queen, [1985] 1 S.C.R. 662.

Number of Terrorist Groups disrupted	6

265. Other mechanisms which are reported are monthly reports in a narrative format with respect to central coordination of Anti-terrorism financing investigations, anti-terrorism training and the coordination and monitoring the status of charities.

266. Regarding prosecutions, one person, Mohammad Momin Khawaja has been charged with 7 terrorism offences, including providing, inviting a person to provide, and making available property and financial services, to a terrorist group in the United Kingdom, intending or knowing that they would be used, in whole or in part, for the purpose of facilitating or carrying out terrorist activity, or for the purpose of benefiting the terrorist group or others who were facilitating or carrying out terrorist activity, contrary to Section 83.03(a) of the Criminal Code. This case has not been adjudicated yet.

267. A total of 20 individuals have been charged with terrorist offences in two cases, including three persons charged under, Section 83.03 of the Criminal Code. Neither of these cases have been adjudicated yet, and since 2001 there have been no other prosecution or convictions. Given the not insignificant number of investigations, and the more than 600 files successfully concluded, the lack of any convictions since 2001 indicates a lack of effectiveness, despite the two prosecutions that are now before the courts.

2.2.2 Recommendations and Comments

268. The definition of "terrorist activity" in the Criminal Code incorporates by reference to specific offences set out in the Code, acts committed in a large number of international conventions. Canadian authorities should give consideration to ways to rationalise the references currently found in disparate locations, without losing the applicability within their country of the additional acts defined in the conventions.

269. The statistics compiled by the RCMP provide a clear indication of an increase in levels of terrorist related activity in Canada, with a large number of investigations and files. Only three persons have been charged with terrorist financing and these charges have not yet been heard. Nobody has been convicted. Given these facts it does not appear that as yet the TF offence is being effectively used. The overall effectiveness of the TF offence and regime is an issue that the authorities will need to pay close attention to going forward.

2.2.3 Compliance with Special Recommendation II

Rec.	Rating	Summary of factors underlying ratings
SR.II	LC	▪ The lack of any TF convictions and the very limited number of prosecutions shows that the offence has not yet been fully and effectively used.

2.3 Confiscation, freezing and seizing of proceeds (R.3)

2.3.1 Description and Analysis

270. *Confiscation*. Canada's Criminal Code contains provisions that authorise the confiscation (hereinafter "forfeiture") of proceeds of crime while the Criminal Code and its Controlled Drugs and Substances Act (CDSA) each have provisions to forfeit "offence-related property," which is Canada's term used to cover "instrumentalities." Forfeiture of "proceeds of crime" is fully covered in Criminal Code in sections 462.37, 462.38, and 462.43. Forfeiture of "offence-related property" is accomplished under the Criminal Code sections 490.1 and 490.2 and the CDSA sections 16 & 17. Offence related property includes instrumentalities intended for use in the commission of specified crimes (see definition of "offence-related property," Criminal Code Section 2). Only simple possession of controlled substances, which is a standalone offence in the CDSA, is not included in that Act's definition of "offence related property." Forfeiture is available for all money laundering and terrorist financing offences, as well as direct forfeiture as an option for all predicate offences. Conviction for any indictable offence or a conspiracy or attempt to commit an indictable offence can give rise to

forfeiture (see definition of "designated offence," Criminal Code section 462.3(1)). Subsection 462.3(1) of the Criminal Code exempts, by regulation, certain offences arising under 14 designated Acts of Parliament from the money laundering predicates and hence also the forfeiture regime.

271. Subsections 462.37 (3) & (4) of the Criminal Code provides for a fine or imprisonment in lieu of forfeiture. Canada considers this alternative as the forfeiture of property of equivalent value. However, the fine in lieu option is discretionary as subsection 462.37(3) states "the court may" impose same rather than "shall." The fine in lieu option arises in a proceeds of crime case where counsel for the Attorney General applies for forfeiture, thus it is an option completely in the control of the prosecutor and one that is rarely pursued in practice as only CAD3.3 million has been collected through this method. Moreover, the court, in theory could, elect not to impose such a fine. Nor is it clear that "fines," which are generally deemed to be a form of punishment, are to be treated the same way as "forfeitures" would be under Canadian law. For example, it does not appear that Criminal Code section 491.1 could be used to disburse such a fine to victims. Fines in lieu of forfeiture can be imposed for the amount of proceeds of crime that have been dissipated or located outside Canada. If there are no assets to which such a fine can be applied the court "shall" impose a jail sentence. The fine is enforced as a civil judgement against any other property that the offender owns at that time or may acquire in the future. It does not apply to non proceeds property the perpetrator transferred to third persons before the fine was imposed. If the accused later obtains wealth or accesses hidden illicit wealth not discovered at sentencing, he or she can be forced to comply with the monetary fine previously imposed. The prosecutor would have to anticipate such a windfall in advance and take the extra steps in the prosecution to obtain such an order, which does not seem to be a very practical solution. It is not prosecution service policy to get such an order in all cases in which forfeiture is an issue, and likely is only done if proceeds are spent and the prosecutor learns that non-tainted assets exist before sentencing. Section 734.7 of the Criminal Code provides the Attorney General with the flexibility to enforce the fine rather than apply to the court to have the offender serve the mandatory time in default. The fine and imprisonment in lieu of forfeiture option is an awkward attempt to ameliorate the problem of dissipated forfeitable assets.

272. Section 2 of the Criminal Code broadly defines "property" to include all real and personal property of every description and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods as well as property originally in the possession or under the control of any person, and any property into or for which it has been converted or exchanged and anything acquired at any time by the conversion or exchange. The definition of "proceeds of crime," in section 462.3(1) of the Criminal Code specifically includes any property, benefit or advantage obtained or "derived directly or indirectly" as a result of the commission of a designated offence. Thus, in light of the definitions of "property" and "proceeds of crime" Canada's forfeiture provisions appear to permit the forfeiture of "income, profits or other benefits" as proceeds of crime[32].

273. Property is forfeited to Canada, whether it is held by the criminal defendant or a nominee third party. The relevant Canadian forfeiture provisions focus on identity of the property as either the "proceeds of crime" or "offence-related property" as the deciding factor as to whether it can be forfeited, rather than the actions or relationship of a property's owner to the offence committed. However, the latter inquiry may be relevant to the issue of the "innocent ownership" in any challenges made to the restraint, seizures and forfeiture of property by purported *bona fide* third-party owners of property that might be subject to forfeiture.

274. *Seizure.* Canada has a wide range of search and seizure or restraint authorities in its criminal laws to assist in confiscation matters. Canada does not use the term "freezing" in its law with the only exception being terrorist property as described and provided for in section 83.08 of the Criminal Code. In Canada, "freezing" is simply accomplished via restraint orders.

---

[32] See the Quebec Court of Appeal decision of R. v. 170888 Canada Ltée, (1999), 135 C.C.C (3d)367.

275. *Search Warrants.* Criminal Code section 487 and section 11 of the CDSA permit the police or a "public officer" to obtain judicial warrants, on the basis of reasonable grounds to believe that in a building, place or receptacles items described in the warrant will be found, and gives one authority to enter, search and seize the things set out in the warrant. The things to be searched for may include anything "in respect of which" an offence against any Act of Parliament has been or is suspected of having been committed, anything that will afford evidence of an offence, and anything intended to be used to commit an offence, and any offence-related property. *See, e.g.* subsections 487(1)(a) through (c.1). Section 487 of the Criminal Code sets out a broad search and seizure authority in Canadian criminal law but other Acts, including the CDSA, have stand alone search warrant provisions as well. In spite of those provisions, in light of Canada's Interpretation Act and case decisions, a Criminal Code section 487 search warrant is available in the investigation of every criminal offence. The authority to issue a search warrant to search and seize almost "anything" does have some limitations. The most significant is that intangible items, such as money on deposit in a bank account or real property, cannot be seized under the authority of a search warrant[33].

276. These Criminal Code search warrants can be issued by a justice of the peace and are available at any relevant stage in the investigative process. In the course of any execution of a search warrant, section 489 of the Criminal Code authorises the peace officer executing a search warrant to seize other things not listed in the warrant which he or she discovers that are obtained from the commission of crime, used in the commission of crime or afford evidence of another offence under any Act of Parliament. The issuing court, may order the detention and preservation of the property for three months (see Subsection 490(2)). However, the detention period can be extended and it is automatically extended as soon as charges are instituted.

277. *Special search warrant for proceeds of crime*. Section 462.32 of the Criminal Code provides authority for counsel for the Attorney General (*i.e.* the crown prosecutor) to obtain a special search warrant to seize property that is subject to forfeiture, which includes the proceeds of crime, but is obtained from a Judge, as opposed to a Justice of the Peace. Once a special search warrant against proceeds of crime is obtained and executed, section 462.35 provides that any seizure is effective for six months after execution. This period of detention may be extended and such an extension is continued once a criminal charge is initiated where a forfeiture of the property may occur. Pursuant to subsection 462.32(2.1) a special search warrant's search authority, once issued, is effective throughout Canada. It is not possible to obtain a special search warrant to search and seize proceeds of crime that may be forfeitable pursuant to the relevant forfeiture provisions when the relevant thing (*i.e.* the property) is outside of Canada. The Attorney General is required to give undertakings for damages and costs when obtaining such warrants, which according to Canadian officials "has not presented any problems" because since 1993, Canada has paid less than CAD50,000 in undertakings.

278. *Restraint order provisions for proceeds of crime and offence related property.* Sections 462.33 and 490.8 of the Criminal Code, respectively, permit the Attorney General to apply for restraint orders to restrain forfeitable proceeds of crime and forfeitable offence-related property. Such restraint orders are *in personam* orders prohibiting the persons named in the order from disposing or dealing with any property specified in the order. The order, once issued before a judge, is effective throughout Canada but also applies to property all over the world, and the persons subject to, *i.e.* served with, the order will commit an indictable offence for knowingly breaching the order (see Subsections 462.33 (3.01), (3.1) and (11), and 490.8 (3.1) and (9). The restraining order, to be effective, must be served upon all relevant parties in Canada, and it applies only against such served persons. The Attorney General must provide undertakings for damages and costs when restraining forfeitable proceeds of crime, which, according to Canadian officials, has not presented any problems (Criminal Code section 462.33(7). No undertaking is required for the restraint of offence-related property (Criminal Code section 490.8).

[33] See *R. v. Banque Royale du Canada* (1985), 18 C.C.C. (3d) 98 (Que. C.A.).

279. For forfeitable property located abroad, with the exception of a restraining order served on a person in Canada who controls property located abroad, Canada, like most nations, would have to rely upon its treaty relationships to obtain the restraint or seizure of such foreign property.

280. *Seizure made ex parte*. An ordinary search warrant for evidence or offence related property, under either section 487 the Criminal Code or section 11 the Controlled Drugs and Substances Act, are in practice *ex-parte* applications. The regular Criminal Code search warrant provisions do not expressly state that the application may be made *ex-parte* as a matter of right[34]. The CDSA Section 11, as well as Criminal Code section 490.8, for the restraint of offence-related property, the special search warrant for proceeds of crime under Criminal Code section 462.32, the restraint order for proceeds of crime under Criminal Code section 462.33, and the CDSA's restraint order for offence related property under section 14, all specify that the application may be *ex-parte*. However, in the case of the seizure or restraint of proceeds of crime the provisions include an additional consideration for the issuing judge. Subsections 462.32(5) and 462.33(5) each provide that the issuing judge may require that the applicant Attorney General provide notice of the application to any person, unless giving such notice before the issuance of the warrant would result in the disappearance, dissipation or reduction in value of the property or otherwise affect the property so that all or a part thereof could not be seized pursuant to the warrant. The Attorney General's filed materials in support of the application must make showing of factors that justify an *ex-parte* hearing as a matter of course, or only after the issue is raised by the court. There were no statistics showing how often Canadian judges required the Attorney General to provide notice. Canada advised that the practice is that courts grant such orders *ex-parte*.

281. *Criminal Code search warrant.* Criminal Code section 487 search warrants are available to law enforcement officers to help trace assets subject to forfeiture (see above). A law enforcement officer applying for a search warrant must provide the issuing justice or judge with reasonable grounds to believe an offence has occurred and that there is evidence in the place to be searched. The officer need not disclose the entirety of the investigation but must disclose information which would tend to call into question the reliability of the grounds relied on to obtain the warrant. Law enforcement agents pointed out that in response to Canadian case law on the reliability of evidence in search warrants, the applications for regular search warrants have become very lengthy, and often hundreds, even thousands, of pages in length. In practice, there often is a full-disclosure of all evidence that might be relevant to the case, rather than just evidence relevant to the specific search in question. This extra detail, although possibly not legally required, is provided in an abundance of caution. Thus, in practice, this makes obtaining a search warrant a very time-consuming and labour-intensive process.

282. *A Criminal Code confirmation order.* Section 487.013 of the Criminal Code provides authority for law enforcement to obtain essential information confirming the existence of an account relationship from any financial institution, as defined in section 2 of the Bank Act or any other entity covered by the PCMLTFA. A law enforcement officer applying for a confirmation order must provide the issuing justice or judge with reasonable grounds to suspect an offence has occurred or will occur and that the financial institution's information will assist the investigation of the offence. The single restriction on the confirmation order is that the person or organization named in the order that is required to confirm information must not be a target of the investigation. Finally, section 487.017 creates an offence when the person subject to the confirmation order fails to produce the documents or data. Confirmation of an account relationship will allow a law enforcement official to aver that such records exist whenever they seek a search warrant or production order against the relevant entities.

283. *Criminal Code Production order.* Frequently there are cases where evidence is required, but the more invasive search warrant is unnecessary. The Criminal Code also provides for a less intrusive obligation to produce documents or data in section 487.012. Section 487.015 allows that party subject to a production order to apply to the court for an exemption if disclosure would breach legal privilege

[34] See *Nova Scotia (Attorney General) v. MacIntyre*, [1982] 1 S.C.R. 175 at 179-180 ("The issuance of a search warrant is a judicial act on the part of the justice, usually performed ex parte and in camera, by the very nature of the proceedings").

or the documents or data are not in the person's possession or control. Section 487.016 specifically provides that the person may not object to production on the basis of self incrimination while insuring that the documents or data may not be used against the producing person except for perjury charges. Finally, section 487.017 creates an offence when the person subject to the production order fails to produce the documents or data. The production order, similar to a confirmation order, provides that the person or organization named in the order to produce must not be a target of the investigation.

284. *A Criminal Code general warrant*. The Criminal Code confirmation order reveals the existence of an account relationship and a production order will result in the production of existing data and documents. A search warrant will allow for the seizure of things, including documents or data that exist in the place at the time the place is searched. The problem with all of these provisions is that they provide a means to obtain existing evidence, rather than anticipatory evidence that may come into existence at a known or reasonable time in the future. There are cases where the financial data or other information will come into existence at a period in the future. There are also cases where law enforcement may wish to undertake a surreptitious search and inspection. The Criminal Code addresses these scenarios in its section 487.01 general warrant authority. The court issuing a general warrant must be satisfied, by information on oath in writing that an offence has or will occur and that information, but not necessarily evidence, concerning the offence will be obtained. Provided that the judge is satisfied that a general warrant is in the best interests of the administration of justice and that no other specific authority exists for would provide for a warrant, authorisation or order then the requested authority for the required technique, procedure or device to be used or thing to be done is authorised by the general warrant. Using this authority it is possible to obtain a general warrant for a financial monitoring order for a specified time into the future.

285. *Tax Information.* Section 462.48 of the Criminal Code provides a specific process to properly obtain the production of income tax information in a criminal investigation, at the investigatory stage. Such production is limited to investigations of drug, organised crime, money laundering offences with a drug or organised crime predicate, and terrorism offences. Hence, it is not available to trace assets pre-indictment in cases that do not involve organised crime, drug or terrorism charges. The importance of a Criminal Code production order for tax information in any investigation for the offences set out in subparagraph 462.48(1.1) is that the tax authorities, pursuant to section 241 of the Income Tax Act, are otherwise immune from criminal search warrants.

286. *Voluntary Disclosures and Privacy Laws*. Canada's professional law enforcement relies on cooperation from voluntary witnesses for much criminal investigation activity. This cooperation is reinforced by means of a safe harbour protection in respect to proceeds of crime in Criminal Code section 462.47, which states in the relevant part: "*. . . subject to section 241 of the Income Tax Act, a person is justified in disclosing to a peace officer or the Attorney General any facts on the basis of which that person reasonably suspects that any property is proceeds of crime or that any person has committed or is about to commit a designated offence.*[35]"

287. Subsection 7(2) of PIPEDA provides that an organization may elect to use "personal information" that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention. Subsection 7(3), or more specifically subparagraphs (c.1), (d) and (e), allow an organization to voluntarily disclose "personal information" without disclosing the fact of that disclosure to their customer.

288. Subsection 7(3) (c) of PIPEDA requires organizations to comply with subpoenas or warrants issued as well as any orders made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records. While

35. Section 241 of the *Income Tax Act* creates an offence for any Revenue Canada employee to disclose any income tax information to anyone absent a court order or specific but limited exceptions in the *Income Tax Act.*

PIPEDA was carefully constructed to still permit voluntary disclosures to law enforcement, and clearly does not prohibit same, several regulated private sector persons that met with the FATF assessment team wrongly thought that PIDEDA was at odds with the voluntary disclosure provisions in the Criminal Code, and the mandatory disclosures to FINTRAC that are required by the PCMLTFA. Law enforcement further opined that the enactments of PIPEDA and the PCMLTFA have had a chilling effect on the number of voluntary disclosures to law enforcement under the Criminal Code.

289. *Bona fide third party - immediate relief from seizure*. Subsection 489.1 provides that the seizing peace officer, if satisfied as to ownership of the thing and that its detention is not required for the investigation or other proceeding, may elect to return the thing they seized to the lawful owner or person lawfully entitled to possession of the thing, rather than detaining the thing after obtaining a detention order from the court. In that case the peace officer must obtain a receipt from the person to whom the officer returned the thing and file that receipt with the justice issuing the warrant. A search warrant directed to a public officer (i.e. a person who has been appointed or designated to administer or enforce the applicable federal or provincial laws and who is named in the warrant) is subject to subsection 489.1(2) with the result that anything seized by that public officer may not be returned, but rather the public officer must file a report or bring the thing to the court for the court's determination on detention or return. If the thing is required for a subsequent proceeding, such as a forfeiture application, the officer must, like any public officer, make a section 490 return to the court. This return is for the purpose of either seeking a detention order or allowing the court to determine its return.

290. *Post seizure judicial release*. Section 490 applies to all seized property other than seized or restrained proceeds of crime seized as a result of a special search warrant under section 462.32 of the Criminal Code and restraint order under section 462.33 of the Criminal Code. If an item is seized under the authority of section 14 of the CDSA, then the section 490 Criminal Code's process applies, with the exception of a controlled substance pursuant to sections 13 & 15 of the CDSA. Under Section 490 a person in possession at the time of seizure or the owner has a right to seek the return of the seized thing. In the case of the person in possession they may demonstrate hardship that may be caused by the continued possession of the thing by the state (see subsections 490(7) & (8)). The lawful owner or person lawfully entitled to possession of the seized thing may, at any time, institute an application for the return of the seized thing pursuant to subsection 490(10). The court considering any return application must consider if the seized thing is required for some other purpose, such as a forfeiture application (see subsections 490(9) & (11)). These provisions apply up until the time that the court considers any relevant forfeiture application.

291. *Release of offence related property*. There are special provisions for offence-related property, since that property may be forfeited upon conviction. It is also possible for the person in possession of offence-related property to successfully apply for the return of the seized thing due to a claim of hardship (see subsection 490(8). In that case, a criminal recognizance is an option for the court to consider, pursuant to subsection 490.9 (1), if the thing falls under the Criminal Code's definition of offence-related property. If the property is offence-related property under the CDSA's definition subsection 13 (6) of that Act also contemplates return under the supervision of a criminal recognizance. If the court elects to return seized or restrained offence-related property to the relevant person the court ordered recognizance can require the owner to preserve and retain the thing, making it available for the subsequent forfeiture application. The terms can include a requirement to surrender the thing in advance of the forfeiture application. Any failure to comply with the recognizance can lead to the forfeiture of the amount covered by the recognizance.

292. *Relief from a seizure or restraint of proceeds of crime.* Section 462.34(a) of the Criminal Code provides that any person with an interest in the seized or restrained property may apply to the court to return their seized proceeds of crime or vacate any restraint order against proceeds of crime. These applications must be brought upon notice to the Attorney General under Criminal Code section 462.34(2). The court may order return and the judge may impose a criminal recognizance, under Criminal Code section 462.34(4)(a). Alternatively, the court may simply return the property if it is

satisfied that the original order should not have been issued per section 462.34(6), or the applicant is an innocent owner in a case where the property is not required for any investigation or proceeding per section 462.34(6)(b). Things seized pursuant to a section 462.32 special search warrant may be immediately released to their lawful owner by the seizing agent under section 462.32(4.1) if certain mitigating factors are present.

293. Section 462.34 provides an immediate opportunity to apply to vary or vacate the special search warrant or restraint order. That authority is used in support of the more frequent application under section 462.34 to obtain access to the property for the purposes of the persons business, living and legal expenses under section 462.34(4)(c). The argument that such property, as property obtained from crime, may create an offence when it is placed in the hands of a third-party, such as legal counsel, is addressed by subsection 462.34(7). As a result, it is common to have the court deal with applications, against seized or restrained proceeds of crime, for the purposes of funding a person's business, living and legal expenses. Between 2000 and 2007 Canada seized or restrained CAD572.8 million in assets, while in the same period court ordered payouts for all business, living and legal expenses was CAD8.3 million. Nonetheless, the forfeiture statistics suggest that a significant proportion of property seized for forfeiture is not actually being forfeited.

294. There are checks and balances in the ability to seek such funding since the property is theoretically dissipated by such orders. Subsection 462.34(4) requires an order unless "… the judge is satisfied that the applicant has no other assets or means available for the purposes set out in this paragraph and that no other person appears to be the lawful owner of or lawfully entitled to possession of the property." This means that if the applicant has other assets or means or if there is a lawful owner of the relevant property the court cannot dissipate that property to fund the applicant's expenses. Of course, it is often difficult for the Attorney General to prove that the applicant has other assets in cases were the accused is particularly adept at hiding his or her criminal proceeds. The authority to seek funded legal expenses out of seized or restrained proceeds of crime is further circumscribed by subsections 462.34(5) to (5.2) of the Criminal Code. If there is a lawful owner (*i.e.* a victim) of the relevant property, the court should not dissipate that property to fund the applicant's expenses. Finally, the court may, but is not required to, consider the applicable legal aid tariff rate in releasing funds to cover legal expenses under Criminal Code Section 462.34(5).

295. *Forfeiture and third party relief.* In addition to the protecting the rights of *bona fide* third-parties in cases where seizure or restraint occurred, the same parties have rights at the time of a forfeiture application of offence-related property or proceeds of crime. Section 490.4 of the Criminal Code and section 19 of the CDSA require third-party protection in the case of forfeiture against offence-related property. Section 462.41 provides a similar protection for third-parties in the case of a forfeiture application against proceeds of crime.

296. All *bona fide* third-parties have a right to notice of the forfeiture application and the right to participate in that application. In addition, section 490.5 of the Criminal Code and Section 20 of the CDSA establish the right of these third parties to also seek relief from forfeiture if they did not appear at the original forfeiture application. In the same fashion section 462.42 of the Criminal Code creates an identical right of third-parties to seek relief from forfeiture of proceeds of crime if they did not appear at the original forfeiture application. Finally, in all cases, the forfeited property may not be sold for thirty (30) days to give all parties an opportunity to institute an appeal (see s. 490.7 of the Criminal Code or s. 22 of the CDSA for offence related property and section 462.45 of the Criminal Code for proceeds of crime).

297. *Victims of crime and forfeiture*. Victims may not have a direct and valid interest in the property that is targeted for forfeiture simply because their property had been laundered long before the seizure and forfeiture issues developed. Those victims have and interest in the criminal but not a specific interest in property targeted for forfeiture. As a result they will not have standing to challenge the forfeiture order. This issue is addressed by sections 738 and 740. It is further ameliorated by subsection 462.49 of the Criminal Code, which continues and gives priority to any Act of Parliament

respecting restitution to or compensation of victims. The Criminal Code does contain restitution to persons affected by crime provisions in sections 738 to 740. As a result, victim restitution and forfeiture effectively coexists in Canada.

298. *Authority to prevent or void actions.* Canada does have the authority, in any appropriate case, to void actions designed to frustrate the forfeiture of property. If the targeted asset is offence-related property, section 490.3 of the Criminal Code or section 18 of the CDSA can be used to set aside a conveyance that occurs after the seizure or restraint. In the case of proceeds of crime section 462.4 provides for the same authority. In addition, if the person receiving the relevant property knew or should have known that the property was proceeds of crime and the transfer occurred before the seizure or restraint that person commits the offence of possession of property derived from an indictable offence under section 354(1) of the Criminal Code. A convicted owner is also subject to a fine in lieu of forfeiture resulting from that owner's dissipation of the property.

Additional elements

299. Membership in a criminal organization is not an offence in Canada. Nor are all the assets of an organization engaged in criminal activity something that can be seized, restrained or forfeited, simply because it is owned by an organization found to be operating for criminal purposes. Those assets would have to be either offence-related property or the proceeds of crime from an offence committed by the organization before they can be subject to forfeiture.

300. Several Canadian provinces have enacted civil forfeiture laws[36]. Other legislation has been passed but not yet in force (Alberta's Victims Restitution and Compensation Act, 2001) or pending before a Legislative Assembly (Quebec's Bill 36 "An Act respecting the forfeiture, administration and appropriation of proceeds and instruments of unlawful activities"). Generally, these provisions allow proceeds of crime to be forfeited in a civil setting under a civil standard. In addition, for indictable offences under the Criminal Code, if an information has been laid against a person, and that person subsequently dies or absconds, a criminal court can issue an *in rem* forfeiture judgment against the proceeds of crime or offence-related property upon a showing beyond a reasonable doubt that the subject property is the proceeds of, or relates to, the offence charged in the information. *See* Criminal Code sections 462.38 and 490.2. Finally, after conviction on any designated offence, a criminal court can order the forfeiture of property that is shown, beyond a reasonable doubt, to be the proceeds any other indictable offence, even if the property is not the proceeds of the offence of conviction. *See* Criminal Code section 462.37(2).

301. On November 25, 2005 a significant revision to the criminal forfeiture provisions, created a reverse onus provision against some proceeds of crime. Subsection 462.37(2.01 to 2.08) of the Criminal Code apply to these cases. The provision covers organized crime offences and drug offences contrary to sections 5, 6 and 7 of the CDSA, including a conspiracy or an attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to an offence under those sections if they were prosecuted by indictment.

Implementation Issues

302. Canadian forfeiture statistics reveal that between 2000 and 2007 Canada's property manager was responsible for the post seizure/restraint of CAD572.8 million in assets. In the same period the realized value of forfeited assets was only CAD203.93 million (roughly 36% of property sought for forfeiture has actually been realised). Canada informed the assessors that the property manager currently has another CAD325.5 million in assets under its management but it is unclear what portion of that amount includes recent seizures or what portion involves assets already captured in the forfeiture statistics. Forfeited funds are often maintained for appeals and other reasons well after they

[36] Remedies for Organized Crime and Other Unlawful Activities 2001, see http://www.e-laws.gov.on.ca/DBLaws/Archives/20050101/Statutes/English/01r28_e.htm; Manitoba The Criminal Property Forfeiture Act, 2004 see http://web2.gov.mb.ca/laws/statutes/ccsm/c306e.php; Saskatchewan, The Seizure of Criminal Property Act 2005, see http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/S46-001.pdf ; British Columbia , The Civil Forfeiture Act 2005.

are on the forfeiture side of the ledger so property under management figures could include large amounts of forfeited property. It appears that in the period 2000-2007, the RCMP's IPOC Units were responsible for approximately for 40% (CAD82.39 million) of Canada's total forfeitures. Thus, the IPOC Unit forfeiture data is the best model for measuring the overall effectiveness of Canada's forfeiture program, particularly as IPOC Units specialize in proceeds of crime investigations and therefore should be getting above-average results.

303. The value of the IPOC Unit seizures appears to be declining over the last 3 years, particularly if the 2004 figures are omitted, and certainly compared to the first three years of data. This is possibly due to the IPOC Unit's relatively recent focus on more labour intensive cases intended to dismantle criminal organizations, which naturally takes away resources from pure proceeds of crime recovery efforts that had been the initial focus of the IPOC Units. A better measure of effectiveness is the IPOC Units overall seizure to forfeiture ratio from 2000 to 2007. Considering that 96% of the IPOC Unit cases from 2000 through 2007 are already closed, it means the lag-time between seizures and forfeitures is not that significant and the cumulative figures are fairly up-to-date. The cumulative IPOC Unit forfeitures over the seven-year period is about 45% the value of the property initially seized or restrained for forfeiture. Over the past seven years Canada is averaging about CAD27 million a year in forfeitures, and over the last 4 years about CAD33 million a year, and has declined slightly over the last two years. If the IPOC units are losing or releasing 55% of restrained assets prior to forfeiture, and the forfeiture numbers are stagnating or declining over time, this suggests that effective is declining. Based on studies, IPOC representatives suggested the 55% seizure-forfeiture gap was potentially due to payment of attorney fees and living expenses of accused persons, and/or. plea bargains. IPOC representatives acknowledged that the seizure/forfeiture gap is still an area of concern. Lack of systemized forfeiture training may be a factor affecting the stagnation of forfeiture numbers.

304. The loss of potentially forfeitable assets, in theory, could be offset by fines in lieu of forfeiture. Section 462.37(3)(d) of the Criminal Code permits a court to substitute a fine for assets no longer available for forfeiture. Even assuming a court would later punish an accused for having successfully petitioned the same court for living or legal expenses under section 462.34(4), in IPOC Unit cases only CAD3.3 million of fines in lieu of forfeiture were "imposed" in the last six years, a small amount when compared to the close to CAD100 million of assets that were seized but not forfeited over that same time period. Further, it is unclear what portion of the CAD3.3 million was actually paid to the Crown. Finally, fines in lieu of forfeiture that are not paid to the Crown may result in higher sentences for the person convicted of the underlying offence. However, the government of Canada has not provided any IPOC Unit data or other law enforcement data indicating how often sentences have been increased for a failure to pay fine in lieu of forfeiture. Thus, it is very difficult to assume that this aspect of the law has been an effective and adequate deterrent to the judicially assisted wasting away of forfeitable assets that IPOC representatives and the statistical data has identified. According to the forfeiture data, it appears a great majority of the assets sought for forfeiture in Canada are not being forfeited.

305. Outside of the IPOC units, there seemed to be less emphasis on confiscation efforts in other law enforcement units or the Crown counsel in general. In an effort to fill some of the deficiencies of the criminal forfeiture regime, certain provinces are experimenting with specialized units and non-conviction based forfeiture regimes, but those programs are still in their infancy and their impact to date has been very limited. Several non-IPOC law enforcement units complained that IPOC units no longer have the resources to assist them with most of their forfeiture needs and feel that they do not have the expertise or resources to handle the forfeiture part of the case. IPOC representatives admitted that they have had to turn down work presented by other agencies and units because the increasing complexity of their cases and their limited resources require them to focus on other aspects of the cases. The IPOC units are hoping to address the assistance shortfall by providing training to other law enforcement agencies so that these entities could handle their own forfeiture matters. IPOC representatives have trained a few hundred law enforcement agents in the last couple of years, but the

scope of the training was limited and Canada has many thousands of agents that did not receive such training.

306. The IPOC Units have been asked to do more complex matters with limited resources. There also seemed to be very little if any coordinated or sophisticated training efforts in the forfeiture area. One legal expert mentioned that he gave at least six lectures to law enforcement groups per annum. It was unclear if he is the only prosecutor giving such lectures. In any event, at most this training is discretionary and not mandatory. Nor does there seem to be any one entity responsible for coordinating Canada's day-to-day forfeiture efforts, forfeiture policy, or forfeiture strategy, or even the collection of forfeiture data, outside of the federal property manager (the federal property manager manages seized assets derived from federal law enforcement cases, *i.e.* RCMP, but also from provincial police forces cases that led to prosecution at the federal level). Since virtually any police officer or prosecutor in Canada can become involved in a criminal case that gives rise to forfeiture, it was surprising there was not a more coordinated national approach to forfeiture efforts or training.

Statistics

307. The confiscation statistics provided by Canada are incomplete (clearly some provincial data was not captured as noted by prosecutors interviewed by the assessment team). Canada has not provided an accurate picture of what all agencies or provinces in Canada seize or forfeit in any given year, but instead has given statistics from various different sources in somewhat incompatible formats and seemingly focused only on "proceeds of crime and money laundering" cases. The scope of Recommendation 3 is slightly broader than that. Under the Vienna and Palermo Conventions possession of criminal proceeds offences relating to covered offences can be characterized as money laundering offences. However, it is highly unlikely that the bulk of Canada's "possession of criminal proceeds" cases resulted from either the organized criminal offences or the drug offences covered by those two treaties. What percentage of Canada's forfeiture involved drug cases, stolen property cases, fraud or organized crime cases can not be determined from the statistics provided by Canada. One thing is certain; Canada has a mostly conviction-based forfeiture system and had only 21 Section 462.31 money laundering convictions in 5 years. In the same five year period the charge and conviction figures show that Canada had 10 150 convictions for the possession of property derived from criminal offence, which could cover a range of different underlying offences.

308. The property manager reports that it managed or supervised the management of CAD572.8 million in seizures between 2000 and 2007. It further reports that it realized CAD203.93 million from forfeitures. Finally it reports that as of September 25, 2007 it currently manages or supervises assets having a value of CAD325.5 million. The amount of property under management by Public Works and Government Services in Table 13 does not help explain what is actually being forfeited in any one year, nor does it explain the actual value of the assets "added" in any one year as it is likely assets are managed for more than one year. Arguably, the steady growth in the amount of property under government management while forfeiture numbers are stabilizing or even decreasing over that time period actually suggests that such property is not being efficiently forfeited, but, instead, is held for long period of times. It would be interesting to see if criminal cases involving substantial amounts of forfeitable assets take longer than similar cases without such forfeitable assets considering the ability to access restrained proceeds of crime for legal fees and other expenses.

RCMP's Integrated Proceeds of Crime Program								
	2000-2001	**2001-2002**	**2002-2003**	**2003-2004**	**2004-2005**	**2005-2006**	**2006-2007**	**Total**
# Cases Opened	239	231	256	226	256	228	204	1 640
Value of Seizures	19 946 000	23 795 000	36 582 000	16 015 000	39 220 000	18 982 000	26 064 321	CAD180 604 321
# Closed Cases	213	198	211	253	289	199	206	1 569
Value of Forfeitures	7 643 504	7 387 364	11 024 119	14 494 264	10 200 981	15 116 644	16 524 728	309. CAD82 391 60 4

Seized Property Management Directorate										
Gross Seizures from RCMP's IPOC Units										
Fiscal Years 2000-01 to 2006-07										
			Asset Count by Type							
Year	Case Count	Total Value (CAD'000)	Cash	Fin. Instr.	Hydro	Aircraft	Vehicle	Vessel	Other	Real Est.
00-01	239	19 946	322	67	26	0	96	6	260	20
01-02	231	23 795	311	45	16	7	176	11	551	53
02-03	256	36 582	374	43	9	1	178	9	219	47
03-04	226	16 015	293	28	8	0	89	2	48	26
04-05	256	39 220	429	136	28	0	162	4	86	82
05-06	228	18 982	265	5	16	0	97	6	65	42
06-07	204	26 064	265	16	24	1	125	8	71	56
Total	**1 640**	**180 604**	**2 259**	**340**	**127**	**9**	**923**	**46**	**1 300**	**326**

Value of the seized property managed by Public Works	
Fiscal Year	**Value of property**
2000-01	CAD152.0 million
2001-02	CAD172.7 million
2002-03	CAD216.3 million
2003-04	CAD235.6 million
2004-05	CAD286.8 million
2005-06	CAD324.5 million

Value of property forfeited in Money Laundering cases		
Fiscal Year	**Value of property forfeited**	**Number of Cases**
2000-01	CAD19.03 million	1 686
2001-02	CAD19.01 million	2 127
2002-03	CAD29.01 million	3 216
2003-04	CAD33.68 million	4 405
2004-05	CAD36.4 million	5 350
2005-06	CAD35.13 million	5 180
2006-07	CAD31.4 million	9 953
Total	CAD203.93 million	

2.3.2 Recommendations and Comments

310. Canada should improve its mechanisms for collecting, maintaining and analyzing confiscation data. It should consider authorizing a study to identify why the IPOC Unit seizures and forfeiture numbers are decreasing, and why there is a large gap between the amount of property seized for forfeiture and the amount of property actually forfeited. Canada should consider ways to combat the dissipation of criminal proceeds and offence-related property to criminals for use as legal, business and living expenses even in non-victim cases. The Criminal Code should provide a specific process to properly obtain income tax information in the investigatory stage that is not limited to investigations of drug, organised crime, terrorist and money laundering offences with a drug, terrorist or organised crime predicate.

311. Canada should consider increasing funding to its IPOC units as they have some difficulties handling both major case responsibilities and every-day forfeiture responsibilities with the current resources allocated. Canada should consider creating mandatory specialized one or two day forfeiture and financial investigation training programs for all new law enforcement personnel and Crown counsel. Canada should create national or provincial entities that sets confiscation policies and standards and can develop and manage any training programs, as well as generally encourage the use of forfeiture in any criminal case in which an economic benefit was obtained by the accused by promoting confiscation.

2.3.3 Compliance with Recommendation 3

Rec.	Rating	Summary of factors underlying ratings

R.3	LC	▪ The fine in lieu forfeiture provision does not fully and effectively meets the requirement for equivalent value provisions and does not apply to property held by third parties. ▪ Based on the limited quantitative and qualitative information available, it does not seem that the confiscation and seizure regime is fully effective, particularly with respect to value based confiscation.

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

General

312. Canada's United Nations Act and its related regulations enable the Canadian government to implement the decisions contained in the resolutions of the United Nations Security Council. The United Nations Al-Qaida and Taliban Regulations (UNAQTR), and the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), were enacted under the authority of Canada's United Nations Act. These regulations allow Canada to list a terrorist individual or entity for the purpose of freezing the funds or assets owned or controlled by that individual or entity or its associates. A third listing mechanism exists under the Criminal Code for threats to Canada's domestic security. The Criminal Code explicitly defines a "terrorist group" and listed individual or entities are determined on the basis of this definition. In combination, these mechanisms allow Canada to list either domestic and foreign terrorist individuals or entities.

313. The decision to list a terrorist entity ultimately lies with the Governor-in-Council, with the exception of those entities listed by the UN 1267 Committee. UNSCR 1267 and successor resolutions are implemented in Canada through the United Nations Al-Qaida and Taliban Regulations (UNAQTR) which automatically incorporate into Canadian law, by direct reference, the list of individuals and entities who are designated by the 1267 Committee. Paragraph 4(b) of UNSCR 1267 is implemented in accordance with s. 4, 4.1, 5 and 5.7 of the UNAQTR. The primary difference between listing an entity pursuant to regulations under the United Nations Act and the Criminal Code is the evidentiary threshold required to support the listing. To list an individual or entity using the UNAQTR, there must be "reasonable grounds to believe" that the individual or entity is involved in terrorist activity. The evidentiary standard is stronger with respect to Criminal Code listings as the Governor-in-Council must have "reasonable grounds to believe that the entity was knowingly" involved in a terrorist activity.

Procedures to freeze terrorist funds or other assets in accordance with S/RES/1267(1999)

314. The United Nations Afghanistan Regulations (1999) gave effect to S/RES/1267(1999). Amendments were made to these regulations on 23 June 2006 and these regulations are now referred to as the United Nation Al-Qaida and Taliban Regulations (UNAQTR).

315. These regulations prohibit persons in Canada and Canadians outside Canada from having financial dealings with the Taliban and Usama Bin Laden and his associates or persons acting on their behalf (Section 4 of the UNAQTR). This includes all funds or assets that are directly or indirectly used, or intended to be used, by these designated individuals or entities. Persons designated by the United Nations 1267 Committee are automatically covered by the regulations.

Procedures to freeze terrorist funds or other assets in accordance with S/RES/1373(2001)

316. The Regulation implementing the United Nations Suppression of Terrorism Regulations (RIUNRST) gives effect to S/RES/1373(2001). The RIUNRST provides a list of individuals or entities for which there are reasonable grounds to believe they are involved in or associated with terrorist activities and prohibits persons in Canada and Canadians outside Canada from having financial dealings with these individuals or entities.

Listing procedures under the Criminal Code

317. The Criminal Code listing mechanism was developed in 2001 as part of the omnibus Anti-terrorism Act. The Anti-terrorism Act was developed to combat terrorism, while ensuring that human rights, such as the right to privacy, are respected. Part II.1 of the Criminal Code has provisions that prohibit the financing of terrorism which are designed to address threats to Canadian security. These provisions include the listing of individuals or entities for which there are reasonable grounds to believe that the individual or entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or the entity is knowingly acting on behalf of, at the direction of or in association with an entity involved in a terrorist activity (Section 83.05 of the Criminal Code).

318. Listing under the Criminal Code allows assets to be frozen and subject to seizure, restraint and forfeiture through the automatic statutory authority in Section 83.08 of the Criminal Code.

Laws and procedures to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions

319. The UNAQTR, the RIUNRST and the Criminal Code listing mechanisms provide Canada with the ability to respond to international listings through the United Nations, undertake joint listings and list both domestic and foreign individuals and entities.

320. In the case where intelligence relating to a proposed listing is received from another country, it is the responsibility of CSIS and/or the RCMP to determine the credibility of the information received. Both CSIS and the RCMP work with their international counterparts when collecting intelligence relating to a potential listing.

321. The process of listing under the Criminal Code begins with criminal and/or security intelligence reports on an entity disclosing the reasonable grounds to believe that the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or the entity is knowingly acting on behalf of, at the direction of or in association with an entity involved in a terrorist activity. The legislation provides for the Governor in Council to establish by regulation a list on which the Governor in Council may place any entity, on the recommendation of the Minister of Public Safety and Emergency Preparedness Canada.

322. The criminal and/or security intelligence reports are submitted to the Minister of Public Safety and Emergency Preparedness Canada for consideration. If the Minister has reasonable grounds to believe that the above test is met, the Minister may make a recommendation to the Governor in Council to place the entity on the list.

323. If the Governor in Council is satisfied that there are reasonable grounds to believe that the above test has been met, the entity may be placed on the list of individuals or entities. The listing of an individual or entity is published in the Canada Gazette and on the Public Safety and Emergency Preparedness Canada website under “Currently listed entities”. As of 31 December 2006, there were 40 entities listed pursuant to section 83.05 of the Criminal Code.

Funds subject to freezing actions

324. The freezing mechanism in place at Section 4 of the RIUNRST prohibits any person in Canada and Canadians outside Canada, to knowingly:

(a) Deal directly or indirectly in any property of a listed person owned or controlled directly or indirectly by that perso.
(b) Enter into or facilitate, directly or indirectly, any transaction related to a dealing referred in (a).
(c) Provide any financial or other related service in respect to the property referred in (a).

(d) Make any property or any financial or other related service available, directly or indirectly, for the benefit of a listed person.

325. Property is defined at Section 1 of the regulations and includes property of every description and documents relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, and includes any funds, financial assets or economic resources. This is in line with the FATF definition of "funds and other assets".

326. Section 4 and 4.1 of the UNAQTR have basically the same provisions for individuals and entities listed by the UN 1267 Committee, specifically the Taliban or a person associated with them, acting on their behalf or at their direction, Usama bin Laden or his associates, or by persons acting on their behalf or at their direction. In addition, a breach of either the UNAQTR or the RIUNRST gives rise to a criminal offence in Section 3 of the United Nations Act, which upon a summary conviction, can lead to fines of up to CAD100 000 and/or imprisonment up to one year. Imprisonment of up to 10 years can result on conviction on indictment.

327. The prohibitions outlined above, combined with the criminal offences of dealing in assets controlled or owned by listed individuals or entities, freezes all that individual or entity's assets within Canada and prevents Canadians outside of Canada from dealing with such property. Although the legal underpinnings are sound, the effectiveness of the freeze mechanisms are impacted by the degree to which information on the listed persons and entities is communicated to Canadians in general and the financial sector and other potential holders of assets of listed persons in particular.The names of listed persons are published in the Canada Gazette and on the Public Safety and Emergency Preparedness Canada website, and a range of financial intermediaries are required to conduct monthly checks for a "listed entity" in section 83.11. This covers a significant amount of assets but is not exhaustive of the persons who can "deal, directly or indirectly, in property." The assessment team believes that the enforcement provisions in the criminal code, the RIUNSRT, the UNAQTR and the United Nations Act are relatively difficult to enforce as they require that the Crown prove "knowledge" of a listing, and this is likely to be even more difficult for entities and persons that are not required to undertake monthly checks .

328. Section 83.08(1) and s. 83.03 of the Criminal Code have basically these same provisions for entities defined as a terrorist group or for terrorist activity. The definition of a terrorist group as it applies to the Criminal Code is defined as: (i) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or (ii) a listed entity, and includes an association of such entities. For the purposes of the Criminal Code provisions property is defined at Section 2 of the Criminal Code and includes real and personal property, funds, financial assets and their substituted property.

329. In addition to the freeze provision, Sections 83.13 through 83.17 permit Canada to seize and forfeit property owned or controlled by Section 83.05 listed entities and property that has been or will be used to facilitate terrorist activity. These provisions can be used cases where assets slip through the section 83.08 freezing net, naturally assuming that the relevant Canadian officials are aware of the forfeitable property and the requisite terrorist nexus. The procedure set forth in Sections 83.13 through 83.17 is a judicial process that very much mirrors the processes set out in forfeiture matters under the Proceeds of Crime provisions located in Part XII.2 of the Criminal Code. This terrorist property seizure and forfeiture regime appears to be in rem and is not conviction-based. The standard of proof in terrorist property forfeitures under Part II.1 is a "balance of the probabilities" test, which is a civil standard. For violations of the RIUNRST and the UNAQTR regulations, the United Nations Act also provides for forfeiture of property dealt with in violation of that Act, and the conviction-based forfeiture scheme set forth in Part XII.2 of the Criminal Code appears to apply to such assets.

Communicating actions taken under the freezing mechanisms and guidance

330. There are several processes that are used to ensure that financial institutions and other individuals and entities are properly notified of a new listing or change to the UNAQTR, the RIUNRST and the Criminal Code. The listing of an individual or entity is published in the Canada Gazette (the official newspaper of the federal government) in conjunction with a press release issued by the Minister of Public Safety and/or the Minister of Foreign Affairs. The Regulations themselves require a continuing monitoring and determination of the existence of property in the possession or control of the institutions. And a failure to undertake the required monitoring is a criminal offence under the regulations and the United Nations Act.

331. To assist financial institutions to search against these listed terrorist names, OSFI, in cooperation with the Department of Public Safety and Emergency Preparedness and the Department of Foreign Affairs and International Trade maintains on its website a database, in various formats, of all terrorist names subject to Canadian laws, including known identifiers for those terrorists. Each time a new terrorist name is listed under Canadian law, or there are changes to existing information, OSFI notifies financial institutions by posting a notification to its website and also notifies all its e-mail subscribers. At the same time OSFI updates the databases with the listing or changes. Since October 1, 2001 OSFI has posted over 90 letters informing financial institutions and the public of updates to the terrorist lists.

332. OSFI also issues a monthly written reminder to federal financial institutions, as well as provincial regulators and SROs that financial institutions are required to file (by the 15th of the following month) a report with OSFI or the appropriate provincial regulator showing, in aggregate, the number of accounts and the dollar value of terrorist property frozen and reported to law enforcement.

333. FINTRAC provides advice and assistance to reporting entities through its website and through the efforts of its Compliance Officers in attending meetings with reporting entities and industry associations. During these outreach sessions and on its website, in particular in its Guideline 5 on Submitting Terrorist Property Reports, FINTRAC refers all reporting entities to OSFI's website, which contains a consolidated list of names.

334. Federally regulated financial institutions, and some other categories of financial institutions[37] are required to determine on a continuous basis whether they are in possession of terrorist property and must report to their regulator on a monthly basis on whether they are in possession of frozen assets. Nil reports are also required. OSFI reminds financial institutions of this obligation every month including their obligations to continuously search their customer names against the OSFI Consolidated List.

335. In addition, federally regulated financial institutions are expected to search their client names against newly listed terrorist names as soon as possible after those new names are posted. If a financial institution discovers terrorist assets it is required to report to the RCMP and CSIS immediately. Reporting entities to FINTRAC must also submit a Terrorist Property Report to FINTRAC if the assets are those of an entity listed under the Criminal Code. It is a criminal offence (section 83.12 of the Criminal Code) to fail to report to RCMP or CSIS.

336. The monitoring systems put in place by financial institutions vary considerably and proper screening against existing lists may take place in some institutions on a monthly basis only. The assessment team believes that this raises some issues of effective implementation of the freezing requirement. In addition, although OSFI provides guidance to federally regulated financial institutions (and forwards its Guidance to provincial regulators and SROs such as IDA in that area, no equivalent measures are in place for other financial institutions, e.g. MSBs, and the DNFBPs (in addition to outreach initiatives and advices and limited guidance provided by FINTRAC). For these entities, the

[37] This does not include MSBs as these entities are not authorised to offer accounts in Canada.

existing communication and guidance is insufficient. This may have an impact on Canada's ability to freeze terrorist funds or other assets without delay.

Publicly-known procedures for considering de-listing requests and for unfreezing the funds of de-listed persons

337. Any Canadian or person in Canada may apply to be delisted. There are clear processes for delisting those entities listed pursuant to the UNAQTR, the RIUNRST and the Criminal Code; (1) on application in writing by a listed individual or entity to the appropriate Minister; and, (2) an applicant may apply to a judge for judicial review of the Ministerial decision.

338. The Minister shall notify the petitioner, within 60 days after receiving the petition, of his or her decision on whether to consider the petition. Within 60 days after the date of receipt of the Minister's decision, the petitioner may apply to a judge for judicial review of the Minister's decision. The regulations or the Criminal Code provide more details of the procedure that has to be followed by the judge when reviewing the Minister's decision.

339. There is a two-year review process for Criminal Code listings by the Minister of PSEPC to ensure accuracy. Delisting procedures for each mechanism are set out in Sections 5.3 and following of the UNAQTR; Sections 2.1 and following of the RIUNRST; and Section 83.05(1) of the Criminal Code. Such procedures are in line with the FATF requirements.

Publicly-known procedures for unfreezing the funds or other assets of persons or entities inadvertently affected by a freezing mechanism

340. Section 5.6 of the UNAQTR, section 10 of the RIUNRST and section 83.07 of the Criminal Code allow for a person or entity to apply for a certificate stating that it is not a listed entity. If it is established that the applicant is not the person or entity referred to under the listing, the Minister has 15 days after receiving the application to issue a certificate.

341. Canadian law enforcement and intelligence agencies have procedures in place to verify identifiers. Verifying identifiers is done through open and classified sources. Full identifiers accompany all domestic listings. Identifiers for individuals may include date of birth, place of birth, country of residence, and address; whereas for entities, a fulsome description is made of the type of activities it engages in and its country of origin. Attempts are made to clarify aliases and alternative spellings of names especially when another country requests that Canada make an addition to its list.

Authorising access to funds or other assets

342. Under the UNAQTR and the RIUNRST, a person whose property has been affected by the freezing, may apply to the Minister for a certificate to exempt property from the freezing procedures if such property is necessary for basic or extraordinary expenses.

343. The Minister shall issue a certificate if the necessity of that property is established with Security Council Resolution 1452 (2002) of December 20, 2002: a) in 15 days after receiving the application if the property is necessary for basic expenses, if the Committee of the Security Council (or the CSC established under Resolution 1267 (19990 OF October 15, 1999, for property frozen pursuant to the UNAQTR) did not refuse the release of the property; and b) in 30 days after receiving the application if the property is necessary for extraordinary expenses, if the release of the property was approved by the Committee of the Security Council. This is set out in Section 5.7 of the UNAQTR and Section 10.1 of the RIUNRST.

344. It is different for property frozen pursuant to the Criminal Code. Pursuant to Section 83.09 of the Criminal Code, the Minister may authorise any person in Canada or any Canadian outside Canada to carry out a specified activity or transaction prohibited by the freezing under the Criminal Code. The authorisation may be subject to any terms and conditions that are required in the opinion of the Minister, including amending, suspending, revoking or reinstating the authorisation. In theory it is

possible to apply to the court to actually seize or restrain the same property. Such an application has never occurred since the provisions amount to an automatic statutory freeze. If the property was seized or restrained pursuant to an order issued under Section 83.13 of the Criminal Code, any person with an interest in the property may apply to have access to it to pay for reasonable living business and legal expenses. However subsection 462.34(6) (b) applies in such cases. The court considering the application must be satisfied that the property is not required for any proceeding. In light of section 83.08 the property is, in fact and law, required for another proceeding, namely the statutory freezing obligation in the criminal law. As a result the section 462.34 process has never been used in a terrorist property case.

Right to challenge freezing measures

345. Sections 5.4 and 5.5 of the UNAQTR, Sections 2.3 and 2.4 of the RIUNRST and provisions in Section 83.05 of the Criminal Code allow for listed entities to apply to a judge for judicial review if the Minister has given it notice that it will remain a listed entity. The judicial review process is stated in these sections and requires that the judge examine the application without delay and provides the applicant with a reasonable opportunity to be heard.

346. If the property was seized or restraint pursuant to an order issued under Section 83.13 of the Criminal Code, any person with an interest in the property may apply to have the property or part of it returned to him/her. In the case of a restraint order, the judge may revoke or vary the order or make the order subject to such reasonable conditions as the judge thinks fit. However no such property has ever been seized or restrained pursuant to a section 83.13 order.

Freezing, Seizing and Confiscation in other circumstances

347. The seizing and confiscation mechanisms as stated in Section 2.3 of the report also apply to cases of FT and terrorist-related funds. In addition to the civil seizure, restraint and forfeiture provisions described above, the normal seizure and restraint provisions for evidence, offence related property and proceeds of crime applies to all terrorist offences established in Part 11.1 of the Criminal Code.

348. For all offences in the Criminal Code, including all terrorism offences in Part 11.1, instrumentalities or, as the concept is described in Canada, “offence related property” provisions apply with the result that all instrumentalities of a terrorist offence are included in the definition. The Criminal Code definition of proceeds of crime, found in section 462.3, also applies to terrorism offences, under either the Criminal Code or as indictable offence in the United Nations Act. Those offences fall within Criminal Code section 462.3’s definition of a designated offence. Finally, it is relevant to consider, for both offence related property and proceeds of crime as they relate to terrorist offences, that the broad definition of “property” in s. 2 of the Criminal Code applies to the search, seizure, restraint and forfeiture provisions.

Rights of bona fide third parties

349. As described above, the UNAQTR, the RIUNRST and the Criminal Code have procedures in place for any person, to make an application to be delisted or to have their property unfrozen.

350. In addition, if the property was seized or restrained pursuant to an order issued under Section 83.13 of the Criminal Code, any person with an interest in the property may apply to have access to it to pay for their reasonable living business and legal expenses, to have the property or part of it returned to him/her. In the case of a restraint order, the judge may revoke or vary the order or make the order subject to such reasonable conditions as the judge thinks fit.

351. Before the forfeiture hearing of property seized or restraint pursuant to the Criminal Code, a judge may require notice to be given to any person who appears to have an interest in the property. Such person shall be entitled to be added as a respondent to the application (par. 83.14(7). If the judge

is satisfied that the person has an interest in the property and has exercised reasonable care to ensure that the property would not be used to facilitate or carry out a terrorist activity and is not a member of a terrorist group, the judge shall order that the interest is not affected by the forfeiture. The order shall declare the nature and extent of the interest in question (par. 83.14(8).

352. There are specific provisions to protect bona fide third party if the property was seized or restraint as proceeds of crime or offence related property.

Monitor compliance with the obligations under SR III and sanctions

353. Federal, provincial and municipal law enforcement authorities are responsible for enforcing the Criminal Code, UNAQTR and RIUNRST. Persons committing offences under these regulations are liable upon conviction to the penalties set out in the United Nations Act.

354. Reporting entities are required to submit Terrorist Property Reports to FINTRAC if they have property in their possession or control that they know is owned or controlled by or on behalf of a terrorist or a terrorist group. FINTRAC refers all reporting entities to the OSFI website, which contains a consolidated list of names. Reporting entities must also put in place policies and procedures that incorporate the verification of lists of terrorists and terrorist entities published in Canada. FINTRAC is responsible to ensure that all reporting entities comply with their AML/CFT obligations under the PCMLTFA and its associated regulations.

355. Section 74 of the PCMLTFA outlines the sanctions that can be imposed on reporting entities on conviction of a summary offence for non-compliance. Reporting entities are subject to fines of up to CAD500 000, imprisonment up to 6 months, or both[38]. Should the same entity be charged with any subsequent summary offence, that entity is liable for a fine up to CAD1 000 000, imprisonment up to 1 year, or both[39]. The PCMLTFA also provides sanctions for a person or entity charged for with an indictable offence for failure to adhere to compliance measures. If a person or entity is charged with an indictable offence for failing to meet compliance obligations, that person or entity is liable for a fine not more than CAD2 000 000, imprisonment for not longer than 5 years, or both[40].

356. Pursuant to section 78 of the PCMLTFA, any officer, director or agent of a reporting entity who directed, authorised, assented to, acquiesced in or participated in the commission of an offence is a party to and guilty of the offence and liable on conviction to the punishment provided for the offence, whether or not the reporting entity has been prosecuted or convicted.

357. Federal and provincial regulators are responsible for ensuring that their regulated financial institutions have procedures in place to continuously monitor and take action against designated entities. Except for OSFI, on-site inspections do not systematically include checks on financial institutions measures to comply with the regulations containing obligations to freeze funds or other assets as well as the prohibition on making funds available to the groups and individuals listed, and the monitoring measures generally are insufficient.

Additional elements

358. Canada has in place some of the measures set out in the Best Practices Paper for SRIII. In particular, there is appropriate communication and co-operation with foreign governments. However, the communication to the private sector, including monitoring of compliance is not sufficient and should be enhanced (with the exception of federally regulated financial institutions supervised by OSFI).

38 PCMLTFA, Section 75 (1)(a)(i).
39 PCMLTFA, Section 75 (1)(a)(ii).
40 PCMLTFA, Section 75 (1)(b).

359. As of December 2006, there has not been a request to free up frozen funds for basic or extraordinary expenses under the RIUNRST or the UNAQTR.

Statistics

360. This table shows the number of Listed Persons and Entities (as of December 2006):

UNAQTR	477
RIUNRST	36
Criminal Code	40

361. This table shows the number of Terrorist Assets Frozen in Accounts:

Date	N° of accounts	Total CAD
November 2001	28	360 000
February 2002	44	460 000
June 2002	16	350 000
September 2002	17	355 000
December 2002	15	335 000
April 2003	17	340 000
September 2003	17	340 000
March 2004	13	181 000
October 2004	14	144 000
April 2005	15	126 000
September 2005	7	68 800
August 2006	10	186 300

2.4.2 Recommendations and Comments

362. There needs to be more communication on listed persons provided to certain categories of financial institutions and other potential asset holders as well more clear and practical guidance to reporting entities (including DNFBPs and MSBs) that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms. This would assist the private sector to understand the process to follow and the action to take in such cases (this does not apply to those types of institutions that already receive specific guidance, as noted above).

363. Canada should enhance the existing measures to monitor the compliance with the legislation governing the obligations under SRIII (except for federally regulated financial institutions supervised by OSFI).

2.4.3 Compliance with Special Recommendation III

Rec.	Rating	Summary of factors underlying ratings
SR.III	LC	▪ The actions taken to communicate the names of listed persons or entities do not cover all types of financial institutions and the lists are not effectively communicated to other types of asset holders. ▪ With the exception of guidance given to federally regulated financial institutions (and copied to provincial regulators/SROs), Canada has issued insufficient guidance to other financial institutions and DNFBPs that may be holding funds of other assets concerning their obligations in taking action under freezing mechanisms. This may have an impact on Canada's ability to freeze terrorist funds or other assets for such entities without delay; ▪ The existing measures to effectively monitor the compliance with the legislation governing the obligations under SRIII are insufficient (except for federally regulated financial institutions supervised by OSFI).

2.5 The Financial Intelligence Unit and its functions (R.26 & 30)

2.5.1 Description and Analysis

Recommendation 26

Functions and responsibilities of the FIU

364. *General.* Canada has established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a national centre for receiving, analyzing and disseminating information concerning suspected money laundering or terrorist financing. The Canada FIU was created in 2000 under the Proceeds of Crime (Money Laundering) Act. FINTRAC's mandate was expanded to include the detection and deterrence of the financing of terrorism and other threats to the security of Canada in 2001 when FINTRAC's enabling legislation was amended and became the PCMLTFA.

365. FINTRAC is an 'administrative' FIU, meaning it does not have investigative powers. FINTRAC is an independent agency that acts at arm's length (it receives no explicit direction) from the recipients of its information and reports its activities to the Parliament of Canada through the Minister of Finance.

366. In addition to its core FIU functions, FINTRAC has a mandate to ensure compliance among financial institutions and other reporting entities with Canada's AML/CFT legislation and regulations (see Section 3.10 of the Report) and promote public awareness of money laundering and terrorist financing issues.

367. *Receiving disclosures of STRs and other types of reports*. FINTRAC receives from reporting parties the following types of reports:

- Suspicious transaction reports related either to money laundering or to terrorist activity financing regardless of dollar value (STRs).
- Terrorist property reports that report the existence of terrorist property in their possession or control, or information about a transaction or proposed transaction in respect of such property (TPRs).
- Large international electronic funds transfer reports involving CAD10 000 or more (EFTRs)[41].
- Large cash transaction reports of CAD10 000 or more (LCTRs).

368. In addition, CBSA provides the following reports to FINTRAC on behalf of individuals, and any entity who is importing or exporting currency or monetary instruments of CAD10 000 or more:

- Cross-border currency or monetary instruments reports (CBCMIRs) involving movements of CAD10 000 or more in currency or monetary instruments.
- Cross-border currency seizure reports (CBCSRs).

[41] Only financial entities, MSBs and casinos are required to report EFTRs.

369. In addition to the reports received from obligated reporting entities, FINTRAC receives information concerning suspicions of money laundering or terrorist financing voluntarily from the general public and various other sources, including law enforcement agencies, CSIS, CBSA, CRA and foreign FIUs. This additional information, referred to as 'voluntary information' or 'VIR', is included in FINTRAC's data holdings and is available to assist in its analytical work. FINTRAC provides acknowledgement of voluntary information received from law enforcement, CBSA, CRA and CSIS within approximately four weeks of its receipt through the delivery of response letters[42]. FINTRAC has received and continues to receive a significant amount of voluntary information from law enforcement and CSIS relating to both money laundering and terrorist activity financing (more than 2,500 voluntary reports since 2001).

370. *Conducting analysis of disclosures of STRs and other types of reports*. To assist in the analytical process, FINTRAC has developed policies and procedures, which identify criteria to be considered in the selection of cases for further analysis and provide guidance in determining that cases have met the legally prescribed disclosure threshold.

371. Once a case has been assigned to an analyst, that person will review and assess the information available to all the analysts (transactions, voluntary information, data from commercial and law enforcement databases, registries of companies, registries of personal property, business profile and open sources[43]) to identify and verify linkages between transactions, people and entities that may be indicative of money laundering and terrorist financing.

372. Once analysis demonstrates that there are reasonable grounds to suspect that the financial activity would be relevant to a money laundering or terrorist activity financing investigation (see below description in "*Disclosing intelligence*"), the analyst prepares the following: (1) an 'analytical report' that provides a description of the case, the analysis that took place, and sets out the rationale for disclosure; (2) a link analysis chart, a visual depiction of the linkages between key transactions, individuals and businesses; (3) a compilation of all relevant publicly available information that the analyst has used in developing the case; and (4) a 'disclosure statement' which sets out the 'designated information' that will be provided to the disclosure recipient. Additional detail on the 'designated information' that FINTRAC is able to disclose is provided below in '*FINTRAC disclosures'*.

373. The analytical report and disclosure statement go through a series of vetting and management approvals before a recommendation is presented to the FINTRAC Disclosure Committee, a FINTRAC Committee consisting of senior management representatives[44] that makes a recommendation to FINTRAC's Director concerning whether cases should be disclosed (*i.e.* whether the case meets the disclosure threshold) and if so, to whom (*i.e.* what is the appropriate police force or other agency in each case). Ultimately, it is the Director that approves disclosures. This review and approval process ensures that, prior to disclosing information, FINTRAC is satisfied that it has met two fundamental criteria. First, that the legislative threshold to disclose has been met and, second, that the information provided is what is allowed under the legislation. This threshold and the list of information that may

---

[42] If FINTRAC's preliminary analysis of the information shows that there is insufficient information to warrant a more comprehensive analysis, FINTRAC issues a letter indicting that FINTRAC is not currently in a position to communicate designated information and provides confirmation that the voluntary information has been incorporated into FINTRAC's database. If the preliminary analysis shows that there is sufficient information to warrant a more comprehensive analysis, FINTRAC will advise the provider, in writing, that FINTRAC is proceeding with the analysis of the information. If FINTRAC meets its threshold for disclosure following a more comprehensive analysis, it will disclose information to the provider of the voluntary information. If the threshold is not met, FINTRAC will follow up by sending the information provider a 'negative response' letter.

[43] 'Open source' refers to information that is available from sources that can be accessed by everyone such as the Internet, media articles etc.

[44] Currently, FINTRAC's Disclosure Committee consists of: the Director, all Deputy Directors, Assistant Directors (some on a rotational basis), Legal Counsel (in an advisory role) and any other persons appointed by the Director.

be provided are set out in sub-Sections 55(3), and 55(7), 55.1(1), 55.1(3), 56.1(1) and 56.1(5) of the PCMLTFA. However given the variety of circumstances seen in money laundering and terrorist financing schemes, FINTRAC makes its decision to disclose on a case-by-case basis.

374. All cases that culminate in a disclosure are coded and entered into a disclosure database. This also allows for the maintenance of a running tally of disclosures made to disclosure recipients. In addition, analysts entering case information check the original disclosure information for any inconsistencies or errors in logging or detailing case information. The assessment team was told that this database is also queried on every case opened by an analyst, which allows FINTRAC to link new cases to previous disclosures and potentially provide secondary or "follow-up" disclosures to law enforcement.

375. The time required to complete a disclosure will vary based on the complexity of the case. For complex disclosures that include thousands of transaction reports, more time is obviously necessary for FINTRAC to complete analysis of such cases. The assessors were told that FINTRAC has disclosed urgent cases in less than 48 hours (see further comments on effectiveness).

376. FINTRAC's case analysis can have a variety of starting points. In most cases, the initiator for a case to be developed is one particular information source. The majority of FINTRAC cases disclosed have been built with information contained in voluntary information provided by law enforcement, CSIS, or the public. In 2005/2006, queries submitted by foreign FIUs (FIUQs) were also frequent case originators. It is cross-referenced against all financial transaction and other data held by FINTRAC to identify transactions or patterns of transactions that may be indicative of money laundering or terrorist financing. Cases also originate from other sources such as STRs or open source information. However, the number of these types of cases has declined as the number of voluntary information reports from law enforcement have increased (see comments below on effectiveness).

377. *Disclosing intelligence*. Under the PCMLTFA, FINTRAC is authorised to disseminate financial information to domestic authorities for further action when it has reasonable ground to suspect that the information would be relevant and useful to the investigation or prosecution of a money laundering or terrorist activity offence. The following summarizes the various agencies that FINTRAC discloses to, and under what circumstances:

- Where FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating a money laundering or a terrorist activity financing offence, FINTRAC must disclose this information to the appropriate police force[45].
- Where there are reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada[46], FINTRAC must disclose designated information to CSIS.
- FINTRAC also discloses to the CRA or the CBSA under certain circumstances. For these disclosures, FINTRAC must meet a dual test. First, FINTRAC must suspect that the designated information will be relevant to investigating or prosecuting money laundering or terrorist activity financing offence and then, for example, if FINTRAC also determines that the information is relevant to tax evasion, FINTRAC must disclose to CRA. Similarly, once the first test is met, and FINTRAC also determines that the information is relevant to determining if a person is inadmissible or relevant to certain offences under the *Immigration and Refugee Protection Act* or to the evasion of customs taxes or duties, FINTRAC must disclose to the CBSA.
- When FINTRAC has reasonable grounds to suspect that designated information would be relevant to the investigation or prosecution of a money laundering or terrorist financing

[45] PCMLTFA, 55(3).

[46] 'Threats to the security of Canada' is defined in the *Canadian Security Intelligence Service Act*, Section 2.

offence or a substantially similar offence, FINTRAC also has the authority to disclose information to foreign financial intelligence units with which it has entered into a Memorandum of Understanding (MOU) to govern such exchanges (see additional information about FINTRAC's international cooperation in Section 6.5 of the report).

378. FINTRAC analysts use a variety of indicators from a number of sources to determine whether a transaction is related to money laundering or terrorist financing (including indicators developed by the reporting entities themselves). FINTRAC has developed a reference guide of indicators with input from law enforcement units. However, the assessment team was told that these indicators are solely based on typologies and indicators issued by the FATF; the Egmont Group as well as AML guidelines issued by a number of FIUs to their reporting entities. They are not based on ML/TF trends developed by FINTRAC itself. Furthermore, a list of 13 of these indicators has been disclosed to the assessment team. In the assessment team's views, this list spots relatively basic and unsophisticated indicators.

379. During the on-site visit, the assessors were told by a law enforcement agency that FINTRAC may occasionally disclose ML/CF cases to the wrong police authority, which may delay the course of the investigation though FINTRAC indicated that it had never heard of such a case.

FINTRAC Disclosures

380. As stated previously and as set out in sub-Sections 55(7), 55.1(3) and 56.1(5) of the PCMLTFA, the information that FINTRAC can provide to a disclosure recipient is referred to as "designated information". The designated information includes key details that identify individuals or entities and their financial transactions. Designated information provided in FINTRAC's case disclosures includes any or all of the following:

- Name and address of company(ies) involved in the transaction(s).
- Name, address and type of business where the transaction(s) occurred.
- Location, date and time of the transaction(s).
- Type and value of the transaction(s) including the amount and type of currency or monetary instruments involved.
- Transaction, transit and account number(s).
- Name of importer or exporter, in the case of importation or exportation of currency or monetary instruments.
- Name and alias of person(s) involved in the transaction(s).
- Address of person(s) involved in the transaction(s).
- Date of birth.
- Citizenship.
- Passport, record of landing or permanent resident card number.

381. Disclosures may also contain publicly available information about transactions, persons or entities contained in the report as well as a visual display highlighting relevant linkages and money flows.

382. The decision to provide police and other recipients with designated information only when FINTRAC reaches its threshold, rather than to provide unrestricted access to FINTRAC's data holdings, reflects the fact that FINTRAC receives a large amount of varied financial information on persons and entities, the vast majority of which is legitimate and not relevant to any investigation or prosecution. By having FINTRAC disclose designated information, under specific circumstances (reaching the disclosure threshold), the assessors were told that lawmakers have struck a balance between the needs of police and other recipients to pursue ongoing and new investigations, and the privacy rights of Canadians guaranteed under the Canadian Charter of Rights and Freedoms. Instead of providing direct access to its data holdings, FINTRAC discloses cases that provide new leads to law enforcement authorities and other partners, either in support of ongoing investigations or in support of other intelligence related to new investigative targets.

383. Although delineating designated information assists in protecting the privacy of Canadians, the 2004 Report of the Auditor General of Canada and the Year Five Evaluation of the National Initiatives to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing, stated that the effectiveness of FINTRAC disclosures was limited by legislative restrictions that constrain the information that can be disclosed. This was seen to have a direct impact on law enforcement ability to effectively investigate ML and TF cases.

384. The two above-mentioned reports encouraged the government to re-examine the list of designated information and identify potential additions to the list with the objective of expanding the information available in FINTRAC disclosures while continuing to respect the privacy and Charter rights of Canadians. Designated information was enhanced as a result of amendments to the PCMLTFA which came into force on June 30, 2007. Since that date, FINTRAC may disclose the following, in addition to the original list of designated information identified above:

- The existence of pending criminal charges or of criminal records of the parties involved in or related to any transaction.
- The relationship or association of any person or entity to a corporations or any other entity referred to in the disclosure, if the transaction was/were made on behalf of a corporations or other entity.
- The name, address and telephone number of each partner, corporate director or officer of a corporation or other entity, its business number and its place of business, or principal location of activities.
- Whether the parties referred to in the disclosure have any beneficial or financial interest in the partnership, corporation or other entity.
- In disclosures where more then one person is involved in, associated with, or related in any manner to the money laundering and/or terrorist financing activity, the principal or controlling entity or individual involved in or related to the money laundering and/or terrorist financing activity.
- The number and type of reports or types of information a disclosure is based on.
- The number and type of reporting entities who filed the reports.
- A summary of indicators (*e.g.* rapid movement of funds and transactions inconsistent with customer profile).
- The reporting entity's reason for submitting a suspicious transaction report to FINTRAC.

385. *Production Orders*. When law enforcement or CSIS want additional information from FINTRAC that is not included in a case disclosure of designated information, they may seek a court order, which requires FINTRAC to provide them with additional information. In most cases, a production order will be served on FINTRAC after an initial disclosure has been made; however, under the Act, a disclosure of designated information is not a precondition to a production order.

386. A production order may include the transaction reports (STRs, LCTRs, etc,) and the case analysis report, which contains the facts on which the analysis is based, the detailed reasons for suspecting money laundering or terrorist financing (the rationale for disclosure), and any other information named in the order. These facts are gathered from the financial transaction reports received and publicly available information, among other sources. To get a production order, the police must satisfy a judge that there are reasonable grounds to believe that a money laundering or terrorist-activity financing offence has been committed by the person in respect of whom the police are seeking information or that that person has benefited from such an offence. In addition, the police must satisfy the judge that the information that they are seeking is likely to be of substantial value to the investigation of the offence. The judge may then issue a production order requiring FINTRAC to permit the police officer named in the order to examine, or be provided certified copies of, all information and documents described in the court order, subject to conditions the judge considers advisable in the public interest.

387. To date, FINTRAC has been served with only 14 production orders from law enforcement. Law enforcement authorities cite two basic reasons for the reluctance to apply for production orders. One is that the legislative threshold is high, the same as for a search warrant: the applicant must satisfy the court that there are "reasonable grounds to believe" an offence has been committed. A search warrant is preferable because it provides direct access to target information that could be used as evidence. Second, the information contained in FINTRAC disclosure is generally considered below the legislative threshold that a production orders requires.

Guidance on reporting

388. FINTRAC provides comprehensive guidance to reporting entities regarding the manner of reporting and the procedures that should be followed when reporting. FINTRAC has defined very structured reporting forms for STRs, LCTRs, EFTRs and CBCMIRs.

389. In order to ensure that FINTRAC is able to receive and process large volumes of reports quickly and efficiently, a mandatory requirement was established in the PCMLTFA Regulations, requiring reporting entities to submit reports electronically to FINTRAC when the sender 'has the capacity to do so'[47]. Today, approximately 99.9% of all reports are submitted electronically.

390. Given the IT requirements for submitting reports, FINTRAC works very closely with reporting entities, particularly the larger ones, with respect to the development and implementation of technical specifications. To assist with this, FINTRAC has created and hosts regular meetings of a technical support group for technology specialists within some of the major reporting sectors, to act both as a consultative body and to ensure that technical questions and issues on reporting to FINTRAC are addressed and communicated within the group. FINTRAC also developed and provided the software to reporting entities to allow them to encrypt and transmit batch files to FINTRAC.

391. In February 2006, FINTRAC launched an updated secure online report capture system, F2R, that provides reporting entities with a reliable mechanism to file reports through the Internet. This tool further facilitates the reporting of financial transactions for the many individuals and businesses that are obliged to do so under the PCMLTFA. This newly implemented reporting system has also been designed to increase data quality through new functions which return LCTRs and EFTRs to reporting entities for revision (*RRFA: Reports Return for Further Action*) when the required information is not included in the report. The new reporting system also has built in controls to ensure that more complete reports are provided to FINTRAC through the implementation of automatic, immediate error messages that go to reporting entities concerning any errors made in specific fields of their submitted transaction reports. The system does not accept the reports if certain key fields are not completed.

392. The assessment team believes that such IT tools can generate positive outcomes. However, during the on-site visit, the assessors were told on several occasions by reporting entities that the format of reporting forms is somewhat too rigid and reduces the capacity to communicate a maximum level of information. FINTRAC indicated to the assessment team that reporting entities were consulted during the development of the new reporting system in order to offer a product that meets reporting entities expectations and needs as well as FINTRAC's requirements. FINTRAC has also worked closely with reporting entities to explain the importance of including a clear and complete description of events and reasons for suspicion in the narrative portion of the form (section G), which has no space limitation.

[47] A reporting entity needs only have basic information technology infrastructure, such as a PC and connection to the Internet in order to be able to report electronically to FINTRAC.

Access to information

393. FINTRAC now has over 45 million reports in its data holdings, and data holdings continue to grow at the rate of approximately 15 million reports each year. All of the data on these reports is available for analysis within FINTRAC.

394. FINTRAC analysts have ongoing, direct access to many different commercially and publicly available databases (*e.g.* Registries of companies, Registries of Personal Property, and Business Profiles), as well as the Internet.

395. Under the PCMLTFA, FINTRAC has authority to collect information from databases maintained for law enforcement or national security purposes and in respect of which an agreement is entered into. FINTRAC currently has access to two major national police databases.

396. The first database is a computerized system that provides tactical information about crimes and criminals. It is an integral part of the RCMP's National Police Services (NPS) as it is the only national information-sharing system that links criminal justice and law enforcement partners across Canada and internationally. This database is responsible for the storage, retrieval and communication of shared operational police information to all accredited criminal justice and other agencies involved with the detection, investigation and prevention of crime. This database has been operational since 1972, and is located in the RCMP Headquarters complex in Ottawa, Ontario. It allows for over 80 000 law enforcement officers to connect to the central computer system within 3 185 police departments, RCMP detachments, and federal and provincial agencies across the country. This system has four data banks, Investigative, Identification, Intelligence and Ancillary (containing information not found in the other categories), which includes files and information such as: vehicles, persons and property.

397. The second database is the RCMP's automated information management system used to store, update and retrieve information on operational case records/occurrences being, or having been, investigated. This electronic indexing system is used by the RCMP operational units, some municipal police agencies, by Firearms Officers (FO) across Canada, and by other federal partners. The database captures data on individuals who have been involved in investigations under the Criminal Code, federal and provincial statutes, municipal by-laws and territorial ordinances. According to the RCMP, in addition to details of an event in a brief synopsis, the database contains limited information relating to investigations and criminal histories. Unlike the first database, which essentially contains factual information (*e.g.* charges and convictions), this database may also contain information provided by witnesses, victims and other associated subjects that can be highly subjective, as well as the names of the witnesses, victims, and acquaintances of the accused individual. It also contains information on occurrences and incidents that never resulted in charges.

398. FINTRAC continues to work with law enforcement and national security partners to identify databases, assess FINTRAC's interest in their content and if appropriate develop agreements for access.

399. FINTRAC has dedicated staff (Law Enforcement Liaison Officers) that are responsible for liaising and maintaining a relationship with FINTRAC's law enforcement partners. These liaison officers are responsible for delivering FINTRAC's disclosures to and obtaining feedback about these disclosures from law enforcement. They also facilitate law enforcement's provision of voluntary information to FINTRAC.

400. FINTRAC does not have access to information on the income of suspects of money laundering or terrorism financing activities. FINTRAC has no authority under the PCMLTFA to collect information from the CRA. FINTRAC has no direct or indirect access (i.e. cannot query) to databases maintained by the CSIS, which can provide information on suspects of terrorism financing activities, nor to databases maintained by the Canadian Customs Agency. However the assessment team was told that CSIS provides FINTRAC with general analysis of threats to the security of Canada that can help FINTRAC to analyze the reports it receives.

401. FINTRAC must rely on voluntarily information provided by the law enforcement authorities to carry out the analysis of the reports it receives. When receiving and analysing such reports, FINTRAC does not ask information directly or via its liaison officers to specific or local law enforcement agencies but limits itself to collect information from the two available law enforcement databases that are not fully integrated and not entirely complete.

Additional information from reporting parties

402. FINTRAC is not allowed by the PCMLTFA to ask additional financial information from reporting entities at the analytical stage. FINTRAC can return STRs to reporting entities because of missing information or other errors (*e.g.* some fields in the electronic form are not completed. Since the adoption of the secure online report capture system (F2R), this process has become more formalized and systematic under the "Reports Returned for Further Action" or RRFA. RRFAs are returned by FINTRAC to reporting entities that must complete insufficient data. Once the reporting entity has made the corrections required (*i.e.* has completed the missing field(s)), the STR is forwarded back to FINTRAC. However, at this stage, no substantive analysis of the report has been made yet. Therefore FINTRAC can only ask reporting parties to supplement an incomplete report but cannot obtain from the reporting entities additional information during the analytical process (for instance, FINTRAC cannot ask the reporting entity about other financial operations carried out in that institution by the same person which are not covered by the report but knowledge of which could help in fully understanding the ML mechanisms they might be using). Canada has advised that Section 8 of the Charter that sets out that "everyone has the right to be secure against unreasonable search and seizure" would not allow FINTRAC to request additional financial information to the reporting entities.

403. The assessment team was told that the legislated reporting requirements were developed in such a way as to ensure that FINTRAC has a broad and detailed amount of transaction information to link suspect transactions and develop intelligence products for the police forces and others. FINTRAC also relies on additional information from reporting entities it can get through other types of reports than STRs (*i.e.* its compliance work as well as from commercial databases and publicly available information).

404. The Suspicious Transaction Report includes a wide range of fields to be complete by the reporting entities (certain fields are mandatory – for all other fields the reporting entity has to make reasonable efforts to get the information). The report has been built by FINTRAC to oblige the reporting entities to provide FINTRAC with as many information as possible on the suspicious financial transactions (multiple suspicious transactions can be reported simultaneously) and the suspects of money laundering or terrorist financing activities. Amongst other things, mandatory fields on how the transaction was initiated (where the money came from) and on the disposition of the funds (where the money went) are included in the report. With respect to STRs, special attention is given to the section of the report dealing with the description of the suspicious activity regarding a transaction (Section G). The ideal response clearly and completely describes the factors or unusual circumstances which led the reporting entity to a suspicion of money laundering or terrorist financing, and provides as many relevant details as possible.

405. However, the assessment team does not consider such mechanisms sufficient to meet the FATF requirement. The current legal framework does not permit FINTRAC to go back at reporting entities to ask for additional potentially relevant information available within the financial sector. As FINTRAC has no authority to obtain additional financial information from the reporting entities, law enforcement authorities may be provided with incomplete pictures of the suspicious ML/TF cases, *i.e.* a partial description of the financial information.

Operational independence and autonomy

406. The PCMLTFA established FINTRAC as an independent agency and, as such, FINTRAC has a high level of operational independence and does not take direction concerning day-to-day operations from any external parties. The Director is appointed for a 5-year term, has supervision over, and direction of, FINTRAC's work and employees, and may exercise any power and may perform any duty or function of FINTRAC.

407. The Minister of Finance is responsible for FINTRAC and may direct FINTRAC on its strategic direction or matters that affect public policy. Similarly, the Director is required to keep the Minister informed of any matter that could materially affect public policy or the strategic direction of FINTRAC. The PCMLTFA prohibits the Director from disclosing any information to the Minister that would directly identify an individual who provided a report or information to FINTRAC, or a person or entity about whom a disclosure was provided by FINTRAC under the PCMLTFA.

408. In addition, FINTRAC is mandated to operate at arm's length from those to whom it discloses information and FINTRAC cannot take direction from police forces or other agencies that it discloses to.

Protection of the information

409. Information held by FINTRAC is securely protected and is disseminated only in accordance with the PCMLTFA. FINTRAC has a legislated mandate to ensure that personal financial information in its possession is protected and remains confidential. This piece of its mandate guides every aspect of FINTRAC's operations.

410. The PCMLTFA upholds the principles outlined in the Canadian Charter of Rights and Freedoms and the Privacy Act, and contains significant provisions specifically designed to protect the privacy of individuals.

411. FINTRAC employs a robust integrated security program that incorporates state of the art technology including both smart cards and biometric technology to control physical and computer access. Continuous improvement and vigilance of physical and electronic security systems ensure that FINTRAC maintains a high standard of information protection[48].

412. When delivering domestic disclosures, all information is handled in a highly secure manner. A FINTRAC Law Enforcement Liaison Officer hand delivers all outgoing disclosures to the appropriate law enforcement or intelligence agency recipient. The disclosure package is presented in both paper and electronic format to facilitate use by the receiving agency. All disclosure activity is logged, whereby the recipient signs for receipt of disclosures and both parties retain a receipt for their records. This process is practiced on a consistent basis and adheres to the Government of Canada's "Security Policy".

413. The protection of information is a paramount consideration in the decision to enter into an agreement with a foreign FIU for the exchange of information. As required by the PCMLTFA, these agreements contain specific provisions that commit those organizations to protect the information, to use it only for purposes related to the investigation or prosecution of money laundering or terrorist activity financing offences (or substantially similar offence), and to treat the information in a confidential manner. Further disclosure of the information to a third party is done only with FINTRAC's explicit consent. Disclosures to foreign FIU are made via the Egmont Secure Web (a

[48] For instance, all employees must obtain 'Top Secret' security clearance as a condition of employment. Staff operate under the 'need to know' principle, meaning that staff has access only to information they require in order to perform their specific duties. Measures to control physical access to FINTRAC offices include security staff, high security locks, electronic access control, closed circuit monitoring, electronic intrusion detection and monitoring.

secure communications channel used by most Egmont-member FIUs) or more secure means, if necessary.

Periodic reports

414. Part of FINTRAC's mandate is to enhance public awareness and understanding of matters related to money laundering and terrorist financing activity. Subsection 72(1) of the PCMLTFA requires the Director to prepare and submit on or before 30 September of each year an annual report on the operations of FINTRAC for the preceding year to the Minister of Finance. Subsequently, the Minister tables the report in Parliament.

415. FINTRAC's Annual Report contains a range of information regarding financial transaction reporting statistics, agency highlights, staffing matters, future priorities and performance summaries. FINTRAC has released Annual Reports since 2002. FINTRAC's Annual Report has evolved over its five publications. In the 2005 Annual Report, FINTRAC provided a sanitized money laundering case in an effort to further enhance the public's understanding of money laundering and FINTRAC's role in detecting it. In 2006, before Parliament, FINTRAC provided detailed televised testimony, on FINTRAC's business flow and how it produces financial intelligence. This material has subsequently been published on FINTRAC's website and replicated in the 2006 Annual Report, in order to reach a wider audience.

416. The Annual Report 2006 provides the following statistical tables: reports received by fiscal year and type; suspicious transaction reports by sector; disclosures and value of transactions; number of reporting entities represented in disclosures; percentage of case disclosures supported by each type of report; regional distribution of money laundering case disclosures; and agreements with foreign FIUs. With regard to ML/TF trends, it describes trends that FINTRAC has observed with respect to drug and fraud-related cases. One complex sanitized case is also presented that includes: description of the facts; a brief summary of the result of the case (such as number of arrests); where appropriate, a description of the inquiries made by the FIU; and, lessons learned. However, the assessment team believes that the FINTRAC Annual Reports could provide more statistical information (such as for instance the number of STRs sent to law enforcement authorities), typologies and ML/TF trends related information considering the number of ML/FT cases FINTRAC annually deals with and the amount of information FINTRAC at its disposal (out of 45 pages of the annual report 2006, only 12 pages are dedicated to statistical information, typologies and ML/TF trends). This is to be linked to the need for FINTRAC to improve its capacity to produce typologies works and studies on ML/TF trends in Canada.

Egmont Group membership

417. FINTRAC became a member of the Egmont Group in June 2002. Since that time it has participated actively in many of its activities, committees and working groups. Currently, FINTRAC's Director holds a seat on the Egmont Committee as Vice-Chair and is Chair of the Information Technology Working Group.

Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases

418. FINTRAC takes into account both the Egmont Group Statement of Purpose and its Principles for information Exchange between Financial Intelligence Units[49].

[49] The Egmont principles stipulate that FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party.

Recommendation 30 (Resources)

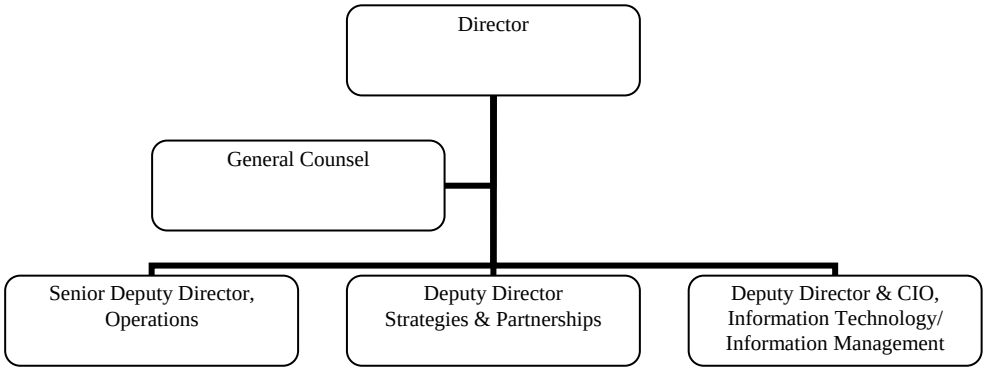
General

419. In 2000, FINTRAC was established as Canada's FIU with an initial annual budget of approximately CAD18 million and 70 employees. In 2001, FINTRAC was given additional responsibilities for combating terrorist financing as part of the Anti-terrorism Act, and the budget was increased to CAD42 million. In the 2006 Budget, the Government announced its priority to bolster existing capacity to combat money laundering and terrorist financing by providing incremental resources to the AML/CFT regime, including an additional CAD16.2 million and 102 employees to FINTRAC. The following table outlines FINTRAC's past, current and planned annual budget.

	2000-01	**2001-02**	**2002-03**	**2003-04**	**2004-05**	**2005-06**	**2006-07**	**2007-08**
Full-Time Employee (FTE)	70	135	150	189	184	180	265.4	271
Total Funding FINTRAC (CAD '000)	17 985	36 093	42 158	33 255	32 003	33 973	51 081	49 839

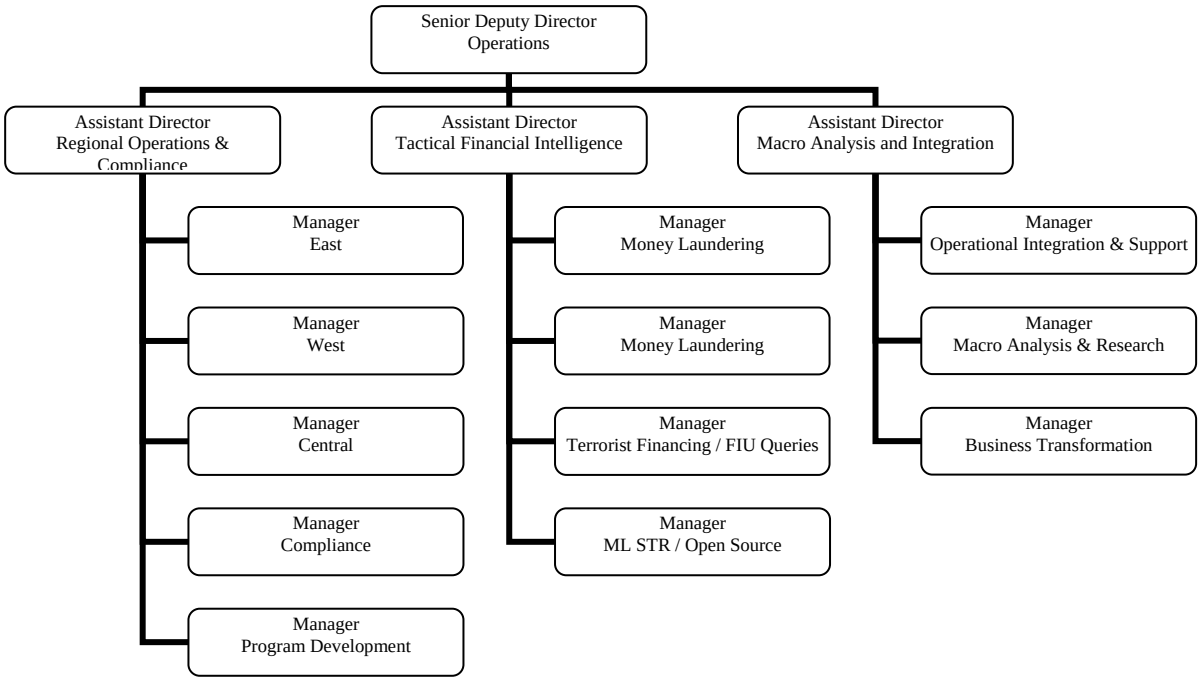
420. FINTRAC has three regional offices (Western, Central, and Eastern)[50] of approximately ten staff each with responsibilities for the various aspects of the national compliance program (policy interpretation, reporting entity assistance, risk assessment and examinations, data quality, timing and volume, reporting entity feedback and disclosures of non-compliance to law enforcement) as well as for liaison with law enforcement agencies (delivery of disclosures, receipt of voluntary information, and relationship management).

FINTRAC's Organizational Chart



421. *Operations Sector*. The Operations Sector (117 employees) is responsible for detection and deterrence activities with the support of the following three functions: Regional Operations and Compliance (ROC), Tactical Financial Intelligence (TFI) and Macro Research and Integration (MAI).

[50] Western – located in Vancouver, covers British Columbia, Alberta, Saskatchewan, and the Yukon; Central – located in Toronto, covers Ontario Manitoba, the Northwest Territories and Nunavut; Eastern – located in Montreal, covers Quebec, New Brunswick, Nova Scotia, Prince Edward Island and Newfoundland and Labrador.

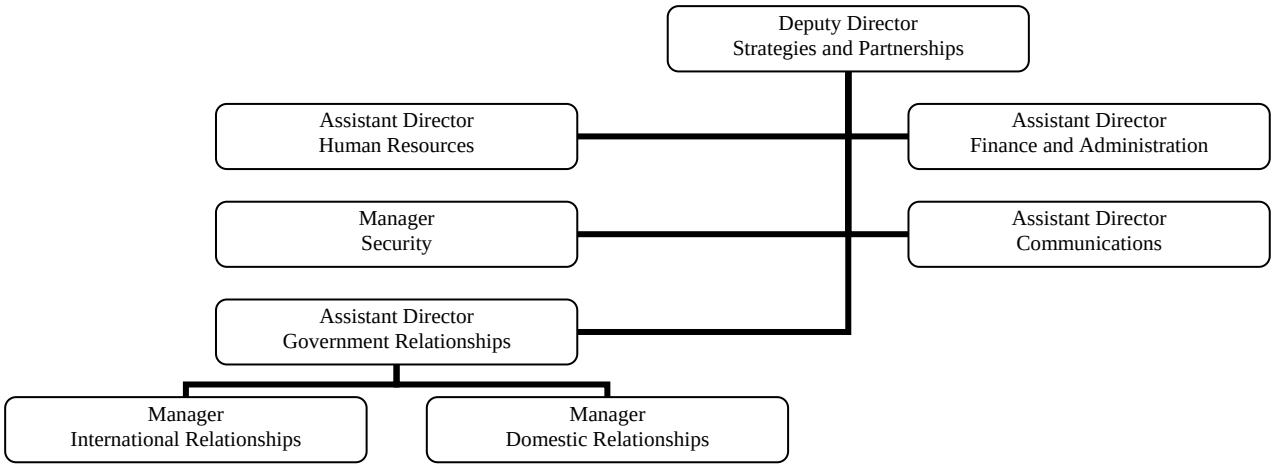


422. Regional Operations and Compliance (49 employees) is responsible for interpreting policy and regulations, providing advice and assistance to reporting entities; conducting risk assessment and examinations; monitoring data quality and volume; providing feedback to reporting entities; making disclosures of non-compliance to law enforcement; conducting regional liaison with disclosure recipients; and developing and implementing new programs.

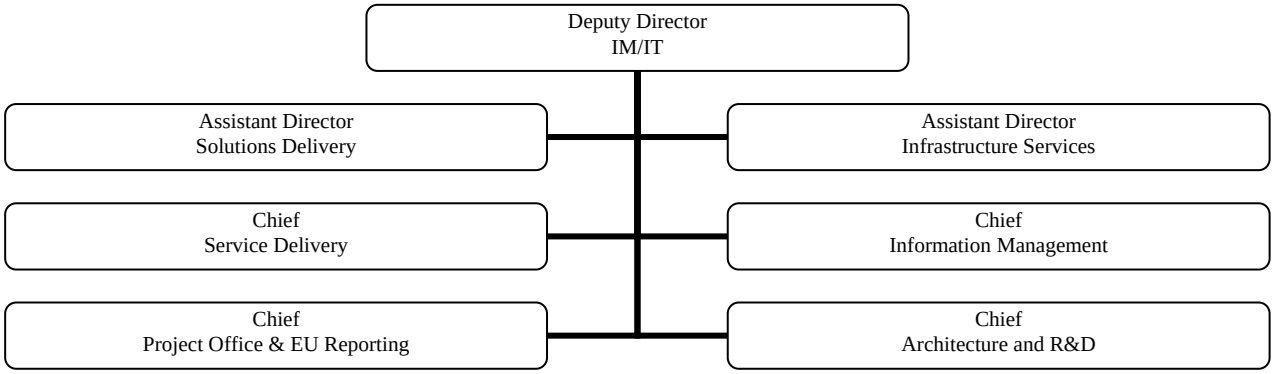
423. Tactical Financial Intelligence (36 employees) is responsible for developing cases and FINTRAC's disclosures. The Tactical Financial Intelligence Unit comprises four units. Three units are dedicated to the analysis of ML cases and the fourth unit deals with terrorist activity financing cases as well as FIU queries. The three ML units are structured to ensure FINTRAC's disclosures are provided in a most timely fashion. For example, one ML unit is set up to deal with the less complex cases. These cases often have fewer transactions and can be analysed within a short time frame and disclosed quickly. The second ML unit deals with more complex cases. This allows analysts to spend the necessary time on the preparation and analysis of these cases to ensure they are worked on immediately and disclosed in a timely manner. The third unit is set up to deal with cases generated by STRs and open source or media articles. The TF unit deals entirely with terrorist activity financing and threats to the security of Canada cases as well as with any queries FINTRAC receives from other FIUs. There is a manager in charge of each unit and a total of 36 analysts handle the workload.

424. Macro Analysis and Integration (29 employees) is responsible for operational integration and support (including handling of Voluntary Information and disclosures, and support on production orders), macro analysis and research (statistics and reports to support FINTRAC's operations, research and exploit available macro level information sources) and business transformation (i.e. development and review of business processes within Operations Sector and the development of user requirements in support of new systems development).

425. *Strategies and Partnerships Sector*. The Strategies and Partnerships Sector (63 employees) manages the key relationships that FINTRAC has with domestic and international partners, and is the primary conduit for ensuring that FINTRAC's views are put forward in the development of public policy and international standards and is responsible for establishing, maintaining and nurturing positive and productive relationships with critical partners such as law enforcement, other government departments and foreign FIUs relationships. This sector also supports corporate needs, including human resources, finance and administration, facilities management, and security. The Communications group is responsible for internal and external communications and public awareness.



426. *Information Management/Information Technology Sector*. The Information Management and Information Technology Sector (75 employees) provides support to FINTRAC's operations in five key areas: the receipt and processing of financial transaction reports, the provision of high quality financial intelligence products, the production of insightful strategic intelligence, compliance and the protection of personal information. This sector develops and applies information management and information technology methodologies that support and advance all of FINTRAC's objectives. It designs, maintains, implements, secures and supports IT infrastructure and system solutions to meet internal and external end user requirements.



427. *Legal Services*. FINTRAC's Legal Services unit is staffed by Department of Justice Canada lawyers who provide advice to FINTRAC on legal questions pertaining to FINTRAC's mandate and operations.

428. *Conclusion*. Canada decided to establish an FIU that would make maximum use of advanced technologies in its analytical and compliance work, allowing FINTRAC to effectively manage a very important and growing database and to analyse incoming reports within a short time frame. FINTRAC's analysts certainly benefit from support from advanced technologies as well as from many experts in the agency. As such, FINTRAC's analysts are significantly focussed on conducting analysis and developing cases for disclosure recipients. Much of the work done outside of the Tactical Financial Intelligence (TFI) unit directly supports this analytical work.

429. Taken into account the above-mentioned considerations and while the total number of staff seems more than adequate, the assessment team has concerns with regard to the number of staff dedicated to the analysis of potential ML/FT cases. Only 36 analysts out of 271 employees (13%) are responsible for developing cases and elaborating FINTRAC disclosures. It seems very challenging for these staff to deal with the amount of reports coming in (15 million reports in 2005-2006, including

nearly 30 000 STRs). Having regard to total resources, FINTRAC should review its internal resource allocation and use, and consider the best and most effective results are being achieved.

Professional standards

430. FINTRAC staff is a diverse group with relevant experiences and skills from both the public (41.7%) and private sectors (58.3%) such as the financial industry, accounting, law enforcement, customs, justice, and public safety. Also, FINTRAC relies upon, and leverages a multidisciplinary team of analysts with backgrounds in various reporting entity sectors, other government departments and international organizations.

431. Employees in the Operations sector bring a varied background of education, including undergraduate and graduate degrees as well as affiliations with professional associations such as Chartered Accountants, Certified Fraud Examiners, International Association of Crime Analysts, and International Association of Law Enforcement Intelligence Analysts.

432. More specifically for the Tactical Financial Intelligence sector, FINTRAC seeks analysts that have sound knowledge and understanding of complex financial manipulations, and a degree from a recognized university. FINTRAC analysts also have experience in using software to analyse data and previous experience in the Canadian or international sector in banking, securities, intelligence analysis, law enforcement, or law.

Standards concerning confidentiality

433. FINTRAC has implemented enhanced security measures and employees participate in security awareness sessions. A robust and effective security program, and a full suite of policies and procedures to protect privacy, and prevent unauthorised disclosures of information, are in place and are vigorously upheld. As mentioned above, FINTRAC employees must obtain a ‘Top Secret’ security clearance as condition of employment.

Training

434. Employees are able to undergo training and attend conferences on ML/TF issues. FINTRAC provides ongoing internal and external training opportunities to enhance analysts’ skills and development. New analysts complete a two-day Operations Orientation Session that covers the operational working and structure of FINTRAC including its legal framework and domestic and international relationships. Entry level analysts also take part in pertinent courses offered regularly, such as courses relating to tactical and strategic intelligence analysis, international AML/CFT standards, effective use of the Internet, and report writing.

Statistics

435. FINTRAC keeps a broad set of statistics, including statistics relating to the number and type of reports received by sector and other relevant information. FINTRAC also maintains statistics on disclosures, in order to track the amount, type, recipient, and foundational information such as the types of financial transaction reports that supported disclosures and the number of reporting entities represented in disclosures.

Effectiveness

436. The following table shows, by report types, the total reports submitted to FINTRAC, by fiscal year, since beginning to receive reports in November 2001:

Report Type	2001-2002[1]	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[2]	Total
CBCSRs/CBCMIRs	--	650	29 369	75 821	54 506	19 914	**180 260**
LCTRs	--	226 918	2 792 910	3 658 462	6 003 493	3 119 156	**15 800 939**
EFTRs	--	1 859 237	6 689 626	7 077 675	8 887 097	4 814 423	**29 328 058**
STRs	3 772	17 358	14 794	19 113	29 367	18 431	**102 835**
Terrorist Property Reports	--	19	6	6	1	--	32
Total	3 772	2 104 182	9 526 705	10 831 077	14 974 464	7 971 924	45 412 124

[1] For the period of November 2001 to March 2002 (FINTRAC became operational in November 2001 and fully operational in March 2003).
[2] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

437. The number of FINTRAC disclosures since 2001 is as follows:

	2001/2003	2003/2004	2004/2005	2005/2006	2006/2007*	**Total**
Number of disclosures	104	197	142	168	92	**703**

* Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

438. The following table breaks down FINTRAC disclosures, by recipient and fiscal year. The RCMP has received the largest number of FINTRAC disclosures. FINTRAC discloses to the RCMP both as the national police force, but also as the provincial police service for all Canadian provinces except Ontario and Quebec. Foreign financial intelligence units, CSIS, and other police forces, (including provincial services for Ontario and Quebec, and municipal services) all receive FINTRAC disclosures.

Disclosure Recipient	2001-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]	Total	%
Royal Canadian Mounted Police	88	163	97	111	63	522	56%
Canadian Security Intelligence Service	23	38	22	21	9	113	12%
Foreign Financial Intelligence Unit	10	22	22	28	17	99	11%
Other Government Agency	3	1	2	4	3	13	1%
Other Law Enforcement Agency	28	66	34	38	27	192	20%
Total	**152**	**290**	**177**	**202**	**119**	**939**	**100%**

[1] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

439. The number of disclosures to 'Other Government Agency' (CRA, CBSA) is reflective of the dual test that must be satisfied in order to disclose to these agencies. As a recipient of information from multiple law enforcement agencies, international counterparts and reporting entities, FINTRAC often identifies links between reports and other information, and this means that disclosures are sometimes made to more than one recipient (*i.e.* multiple police forces in one province, different levels of domestic law enforcement, domestic and international agencies at the same time).

440. The following table shows the number of STRs used in disclosures since 2001:

	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]
Disclosures including STRs	89	117	78	108	62
Total disclosures made	104	197	142	168	92
Number of STRs in these disclosures	5 814	3 080	1 040	1 368	787
Total STRs received	**17 358**	**14 794**	**19 113**	**29 367**	**18 431**

[1] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

441. The total number of STRs used in the cases disclosed has strongly decreased from 5 814 in 2002/2003 (33.5%) to 1 368 (4.6%) in 2005/2006.

442. The following table provides an overview of disclosures by fiscal year, in terms of numbers of disclosures made, the relative dollar amount and the number of transactions contained in the disclosure.

Fiscal Year	Number	CAD Amount	Transactions
2001-2003[1]	104	471 359 543	12 571
2003-2004	197	696 434 493	12 235
2004-2005	142	2 048 445 054	19 263
2005-2006	168	5 004 349 860	43 771
2006-2007[2]	92	2 265 046 135	25 706

[1] Too few disclosures were made in 2001-2002 to present separately. FINTRAC became operational (November 2001).

[2] Fiscal year 06-07 statistics include only the first two Quarters (up to September 30, 2006).

443. The above-mentioned tables indicate a very low number of disclosures in comparison with the total number of reports that FINTRAC receives. In 2005/2006, out of 14 974 464 reports received and out of 29 367 STRs, only 168 disclosures were sent to law enforcement authorities for further investigations (out of these 168 disclosures, 108 included STRs and these disclosures related to more than 43 000 transactions and contained 1 368 STRs). FINTRAC believes that the large number of transactions being disclosed is a positive indicator of the amount of financial data that FINTRAC delivers to law enforcement authorities.

444. FINTRAC disclosures are essentially based on cases generated by law enforcement authorities. The assessors were told that 80% of the cases disclosed by FINTRAC resulted from voluntary information from law enforcement or another recipient[51]. The remaining 20% of the disclosed cases concern new cases that are not already under investigation by law enforcement. This raises serious concerns with respect to the capability of FINTRAC to generate new ML/TF cases (as opposed to positively contributing to existing investigations) on the basis of the STRs it receives (*i.e.* the financial information provided by the private sector).

445. FINTRAC initiated a case disclosure feedback framework in November 2005, which was developed in cooperation with law enforcement agencies throughout Canada. The objective was (1) to enhance FINTRAC's understanding of how law enforcement uses its intelligence product; (2) to initiate steps to strengthen FINTRAC's disclosure process and product; and (3) to be able to report publicly, as a performance measure, the results of FINTRAC's disclosures to law enforcement.

446. Of the feedback forms received as of the end of September 2006, 85% of the responses indicate that the FINTRAC disclosure related to persons, businesses or entities of interest to their current investigation and 60% indicate that the FINTRAC disclosure provided leads on previously unknown persons, businesses or entities of interest. Overall, close to half of the responses indicate that the FINTRAC disclosure provided a major contribution to an ongoing investigation, while about 15% indicate that a FINTRAC disclosure triggered a new investigation. Approximately 15% of the responses also indicated that a FINTRAC disclosure had contributed to an investigation that is expected to be prosecuted.

[51] More than 2 500 voluntary reports were sent to FINTRAC since 2001 (the RCMP provides the majority of these reports).

447. The general view of some organizations that receive FINTRAC disclosures and that were met by the assessment team during the on-site visit is that the balance has been so far too strongly in favour of privacy concerns. The approach that prevailed until the amendment of the PCMLTFA in June 2007 – characterized as too "conservative" or "risk-averse" by some –led to insufficient information in disclosures, which reduced the usefulness for investigations (in particular, for new cases), and difficulty in obtaining production orders for more information.

448. In addition, law enforcement partners have expressed a need for more details (*i.e.* a narrative) on the analysis and rationale underlying FINTRAC disclosures in addition to the factual information that must be provided under the PCMLTFA (as revised). They argue that if more details were provided, this would reduce unnecessary duplication of intelligence effort (*i.e.* there would be no need to redo the analysis already conducted by FINTRAC), enhance availability of timely information, improve the usefulness of disclosures for investigations, and ultimately enhance the effectiveness of the AML/CFT regime.

449. A number of recipients initially indicated that the timeliness of disclosures should be improved to increase relevance to ongoing investigations. The assessors were told that FINTRAC has worked to decrease the time it takes to build a case and make a disclosure, and feedback since April 2006 has indicated an increasing satisfaction with timeliness of disclosures.

450. FINTRAC has an obligation to disseminate financial information to domestic authorities for further action when it has reasonable ground to suspect that the information would be relevant to the investigation or prosecution of a money laundering (Section 462.31) or terrorist activity offence seems to be too strictly implemented using a higher threshold that the one required by law. The assessors have concerns about the interpretation that is made by FINTRAC of the "threshold to disclose" level that might be reached to disclose. Assessors understood during the on site visit that certain financial transactions are not disclosed because they considered as not important enough to be investigated, even if law enforcement information is available. FINTRAC indicated however that all relevant transactions are transmitted to law enforcement as soon as the legal threshold is reached.

451. Based on all of these factors, the assessment team has serious concerns with regard to the added value of the information generated by FINTRAC on ML/TF cases. Importantly, during the on-site visit, the assessors were advised that since the creation of FINTRAC, no conviction for ML or TF has resulted from a FINTRAC disclosure[52]. Although FINTRAC has no role in investigation, prosecution or conviction of ML, TF and the predicate offences, the assessment team believes that this is an additional factor to consider when looking at FINTRAC's ability to produce intelligence that is able to be used in criminal investigations and prosecutions.

2.5.2 Recommendations and Comments

452. FINTRAC should be authorised to develop a more proactive approach for collecting data on suspicious cases of money laundering or terrorist financing and should consider more actively employ its liaison officers to interact with the law enforcement authorities. FINTRAC should be authorised to have access to more intelligence data from CSIS, CRA and the Canadian Customs Agency to reinforce its analytical work. FINTRAC should envisage employing liaison officers from these agencies.

453. FINTRAC should be able to obtain additional financial information from the reporting entities, especially during the analytical process.

[52] On 23 January 2008, Canada informed the assessors that one investigation resulted in a conviction for money laundering and was initiated as a result of a STR-driven FINTRAC disclosure case. In addition, FINTRAC indicated that in 22 cases, its disclosures supported investigations that resulted in convictions for ML, proceeds of crime, fraud and other offences.

454. While it will always take a certain level of judgment to decide what constitutes "reasonable grounds" for suspicion, an explicit framework helps produce consistent decisions among analysts and over time. Such indicators should be developed based on ML/TF trends elaborated by FINTRAC. FINTRAC should improve its capacity to produce typologies works and studies on ML/TF trends in Canada.

455. Canada should ensure that the format of reporting forms developed by FINTRAC provides some flexibility and allows the reporting parties to enter all the information in their possession (including annexes such as banking records) that could be relevant for further investigation.

456. Canada should clarify on what basis and criteria FINTRAC decides to which law enforcement authority disclose ML/TF cases. FINTRAC should timely provide law enforcement authorities with more comprehensive and clearer narratives of the cases it discloses.

457. So far, the number of disclosures made by FINTRAC to the CRA has been rather low. It is important that FINTRAC provide information to the CRA because often where cases do not meet the threshold for criminal prosecution, civil liability for unpaid taxes may be possible. FINTRAC and CRA seem to work on developing indicators that would allow FINTRAC to more readily determine whether the information it has in its possession would meet the test of being relevant to an offence of evading or attempting to evade taxes.

458. Canada should ensure that FINTRAC has sufficient analysts that are in charge of developing ML/TF cases and processing disclosures to law enforcement authorities for further investigations.

459. Canada should examine FINTRAC effectiveness in disclosing ML/TF cases to law enforcement authorities including whether all relevant information in FINTRAC possession is disclosed within the restrictions imposed by law, whether this information positively and timely participates in prosecuting ML and TF and whether FINTRAC discloses cases strictly in the circumstances imposed by law. Canada should also consider the use made of STRs and other forms of reports when disclosing cases and consider the current disproportionate reliance on voluntary information reports.

2.5.3 Compliance with Recommendation 26

Rec.	Rating	Summary of factors underlying ratings
R.26	PC	▪ FINTRAC has insufficient access to intelligence information from administrative and other authorities (especially from CRA , CSIS and Customs). ▪ FINTRAC is not allowed by the PCMLTFA to gather additional financial information from reporting entities. ▪ Effectiveness: (1) the number of staff dedicated to the analysis of potential ML/FT cases is low especially in comparison with the amount of reports coming in, which may have an impact on the number of cases that FINTRAC generate; (2) feedback from law enforcement authorities outlines the relatively limited added value of FINTRAC disclosures in law enforcement investigations; (3) the timeliness of FINTRAC disclosures to law enforcement authorities was raised as an issue at the time of the on-site visit; (4) 80% of the disclosures made by FINTRAC result from voluntary information from law enforcement; only 20% result from STRs which raises serious concerns with respect to the capability of FINTRAC to generate ML/TF cases on the basis of STRs or other reports it receives from the private sector; (5) so far, very few if any convictions for ML or TF have resulted from a FINTRAC disclosure which is an additional factor to consider when looking at FINTRAC's ability to produce intelligence to be used in criminal investigations and prosecutions.

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27, 28 & 30)

2.6.1 Description and Analysis

Recommendation 27

Law Enforcement authorities

460. Canadian efforts to combat organized crime and terrorism are shared by law enforcement agencies throughout the country. As such, Canadian law enforcement authorities are tasked with enforcing federal, provincial, territorial and municipals laws. Statistics indicate that in 2005, there were 229 police forces in Canada, with a total of 61 050 peace officers to enforce various statutes throughout the country. Canada has one national police force (RCMP), two provincial police forces in Ontario and Quebec (Newfoundland's provincial police force is focused largely in St. John's), 169 municipal, and 56 First Nations police forces.

461. While all Canadian police forces can investigate money laundering and terrorist financing offences, the Royal Canadian Mounted Police (RCMP) and, to a lesser extent, the provincial law enforcement authorities in Ontario (the Ontario Provincial Police) and Québec (Sûreté du Québec) undertake virtually all money laundering and terrorist financing investigations. While all police services in Canada are potential recipients of FINTRAC disclosures, the majority of disclosures are made to the RCMP, then CSIS and the Ontario Provincial Police (see table in Section 2.5).

RCMP

462. The RCMP is unique as it is a national, federal, provincial and municipal policing body. The RCMP is organized under the authority of the RCMP Act and is headed by a Commissioner. The RCMP is an agency of the PSEPC. It is divided into four regions and 15 Divisions plus the headquarters located in Ottawa.

463. The Royal Canadian Mounted Police enforces throughout Canada laws made by, or under the authority of the Canadian Parliament. Administration of justice within the provinces, including enforcement of the Criminal Code, is part of the power and duty delegated to the provincial governments. The RCMP provides police services under the terms of policing agreements to all provinces (except Ontario and Quebec), Yukon, the Northwest Territories and Nunavut, and under separate municipal policing agreements to 197 municipalities.

464. *Money Laundering and Proceeds of Crime*

465. The RCMP Proceeds of Crime Program falls under the Federal Policing Services program, which coordinates the RCMP's components in combating money laundering in relation to two federal government initiatives targeting money laundering and criminal proceeds of crime: the Integrated Proceeds of Crime Initiative (IPOC) and the AML/CFT regime.

466. The goal of the IPOC initiative is to contribute to the disruption and dismantling of targeted organized criminals and crime groups (see Section 1.2 of the report for more information on the IPOC Units). The IPOC initiative is currently comprised of 14 units located across Canada and has a total of 257 regular member police officers, 19 civilian members, 59 public servants and approximately 30 seconded provincial and regional police officers.

467. The AML/ CFT regime is led by the Department of Finance. The RCMP coordinates its activities through its Money Laundering Program and currently operates 12 money laundering units, located across Canada and within either Integrated or non-Integrated Proceeds of Crime Sections. The Money Laundering Program has a current workforce of 28 regular member police officers and four civilians.

468. The assessment team believes that the Integrated Proceeds of Crime Units (IPOCs) have demonstrated an ability to enforce proceeds of crime and ML offences and are effective at investigating proceeds of crime and ML offences despite insufficient resources (see also comments in relation to Recommendation 30).

National Security/Terrorist Financing

469. The RCMP has an integrated model for responding to National Security Investigations (NSI), which forms part of the overall Public Safety Anti-Terrorism (PSAT) initiative. The NSI centrally coordinates and directs all national security investigations, intelligence and policy. At the operational level in each province of Canada, NSI serves as the policy centre for the Integrated National Security Enforcement Teams (INSETs) and the National Security Investigation Sections (NSIS).

470. The NSI includes a unit in Ottawa called the Anti-Terrorist Financing Team which consists of the RCMP and CRA. The team is responsible for (1) monitoring and coordinating major ongoing investigational projects related to terrorist organizations focusing primarily on their financial and procurement infrastructures and (2) liaising on a routine basis with partner agencies such as FINTRAC, CSIS and CRA Charities Directorate. The unit has also hosted terrorist financing courses in 2005 and 2006.

471. National Security Operations Branch (NSOB) supports and coordinates all national security field operations by reviewing, analyzing and disseminating information from all sources, including international partners, the CSIS, third parties and RCMP field investigations. NSOB also prepares subject profiles, case briefs and briefing notes for senior management, ensures compliance with RCMP policy, and tasks RCMP liaison officers in support of RCMP National Security investigations.

472. The Anti-Terrorist Financing Team (ATFT) supports counter-terrorism strategies with respect to financial intelligence investigations, enforcement, and the listing process in respect to Terrorist Entities.

473. Using existing resources from NSIS, and complemented by PSAT funding, the RCMP created new Integrated National Security Enforcement Teams (INSETs). INSETs have two mandates: to increase the capacity for the collection, sharing and analysis of criminal intelligence among partners; and to enhance enforcement capacity with respect to criminal activities relating to national security.

474. Supplemented by several other agencies (*e.g.* Canada Border Services Agency, CSIS and Transport Canada), partners work closely in the collection and sharing of intelligence relating to the activities of terrorist groups or individuals. INSET units are located in Vancouver, Toronto, Ottawa and Montreal and total approximately 300 staff. In 2005/2006, the INSET Units concluded approximately 2 900 files.

Provincial Police Forces

475. *Ontario Provincial Police (OPP).* The OPP is comprised of over 5 500 uniformed members, 2 000 civilian employees and 850 Auxiliary members.

476. The OPP established the Ontario Provincial Police Asset Forfeiture Unit (AFU) as the group responsible for the application of all asset forfeiture legislation and the coordination of asset forfeiture initiatives within Ontario. The main activities of the AFU include the identification, investigation, and seizing of offence-related property and proceeds of crime, including the investigation of money-laundering activities resulting from the commission of designated offences found in Part XII.2 of the Criminal Code. The AFU also identifies assets as proceeds of crime, instruments, or conspiracies as defined under the Civil Remedies for Illicit Activities Act (Ontario). The AFU supports local investigative units with their investigation of the substantive criminal offence(s) by providing investigative expertise, training, case management, asset management, expert witness, and external agency liaison.

477. The AFU has developed a core of specialized investigators who investigate asset forfeiture to carry out these activities. To assist in the investigations, the AFU has a full-time forensic accountant. Also, the AFU uses a Currency Reading and Tracing System (CRATS) for searching and tracing seized Canadian or U.S. currency to determine its involvement in criminal offences.

478. With the expanding and changing criminal activity in Ontario, there is a parallel need for substantive investigations and related asset forfeiture investigations. The AFU reviews new trends in crime and law enforcement and adapts their specialized investigative resources accordingly.

479. *Sûreté du Québec*. The Sûreté du Québec (usually translated as "Quebec Provincial Police") is the provincial police force of Quebec, employing approximately 5,200 officers. The primary function of the Sûreté du Québec is to enforce provincial laws, some municipal bylaws, the criminal code, and many other laws throughout Quebec and to assist municipal police forces when needed. The Sûreté du Québec created the first team of investigators specialized in proceeds of crime in 1996. Until 2003, some 12 investigators were specifically assigned to proceeds of crime investigations. Since then, the Sûreté has adopted an integrated approach to organized crime investigations by incorporating a proceeds of crime focus in each major investigation.

480. In the last five years, the Sûreté has initiated or completed approximately 20 major investigations that had a significant proceeds of crime component. Overall in these five years, over CAD20 million dollars have been forfeited as a result of the work of the Sûreté du Québec and a number of criminal organizations have been dismantled.

Prosecution

481. The attorney general of Canada is the chief litigator for the Government of Canada. The Criminal Code establishes jurisdiction to undertake criminal prosecutions in Canada. Criminal prosecution responsibility is divided, by tradition and the law of criminal procedure, between the attorney general of Canada and provincial attorneys general. Generally the attorney general of Canada is responsible for undertaking money laundering prosecutions whenever the offences giving rise to the property being laundered are derived directly or indirectly from offences under criminal law other than the Criminal Code. The provincial attorneys general have the jurisdictional responsibility for money laundering prosecutions for offences found in the Criminal Code. The attorney general of Canada and the provincial attorneys general have concurrent jurisdiction over all terrorist financing prosecutions.

482. The attorneys general prosecute through public prosecution offices established under the authority of their federal or provincial departments. Public prosecutors, known as Crown counsel, are distributed throughout Canada and prosecute on the basis of the jurisdiction to prosecute set out in the Criminal Code. Each province and the attorney general of Canada has a delegated head of criminal prosecutions. Those heads of prosecution meet regularly to coordinate prosecution issues and help each other develop prosecution policies. Money laundering is a regular topic of discussion within the heads of prosecution group. The group has established a subcommittee, the National Liaison Committee on Proceeds of Crime, to coordinate prosecutions issues on money laundering.

483. Counsel for attorneys general have the authority to take over private prosecutions, issue stays of prosecution and generally manage the prosecution function in the Criminal Code. That function includes authority to approve charges. Under the money laundering prosecution authority, only the attorneys general – through their prosecution counsel – may apply for special search warrants, restraint orders, forfeiture orders and wiretap authorisations. Additional responsibilities associated with the PCMLTFA include attorney general applications for production orders and prosecutions related to new offences created within that Act, such as failure to report suspicious transactions.

484. There are 2 349 prosecutors, known as Crown Counsel, working for the ten provincial Attorneys General departments or in a provincial Director of Public Prosecutions office in the province. These prosecutors work in cities or towns throughout their provinces and they are assisted by other legal counsel, acting as standing agents, as the prosecution volume requires. Each of the provincial prosecution services has their own crown counsel prosecution manual and the distribution of money laundering or organized crime cases is managed within the operational structures of the provincial Attorneys General departments of Director of Public Prosecution office.

485. In addition, there are 411 federal prosecutors, now under the supervision of the Director of Public Prosecution in the Public Prosecution Service of Canada (PPSC). These prosecutors work in 13 regional prosecution offices and sub-offices, strategically distributed across Canada. There are also 800 standing agents working for the PPSC who are widely scattered across Canada and operating under the local supervision of the thirteen regional prosecution offices.

486. The federal prosecutor complement includes 70 prosecutors working on proceeds of crime and money laundering litigation in Canada. These include the federal prosecutors assigned to the 12 IPOC units in the RCMP as well as counsel who prosecute the cases generated by the IPOC units. The 70 PPSC prosecutors are dedicated to POC prosecution. They do not prosecute cases generated by NSIS or IBETS. In the larger provinces (Ontario, Quebec, British Columbia and Alberta, as well as in New Brunswick) special teams of crown counsel work with provincial investigative units that are assigned to undertake money laundering investigations.

487. *Measures to postpone or waive the arrest of suspected persons*

488. There is no specific legislative measure in place that allows a law enforcement official to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purposes of identifying persons involved in such activities or for evidence gathering. Rather, the competent authorities have discretionary powers to determine when such enforcement action will be taken. It is important to note, that this power brings with it the responsibility to ensure that the discretion complies with the internal policies of the authority and is in the best interest of Canadians.

Additional elements

489. In Canadian law, there is no separate legislative framework that applies to special investigative techniques (SITs). Law enforcement is covered under the general legal framework of criminal law, as well as under legislation governing the establishment and conduct of police forces and other enforcement agencies. Within this framework, specific kinds of SITs are subject to specific legal requirements. It should be emphasized, as well, that laws providing for SITs, and law enforcement activity in using SITs, are subject to review by the courts under the Canadian Charter of Rights and Freedoms and in respect of compliance with other general requirements, such as those that govern abuse of process.

490. Some SITs, such as general undercover police operations, non-intrusive police observation techniques, and use of informants are not subject to specific provisions of statutory law addressing when and how they can be used. Nevertheless, general legal standards and common law requirements apply. Common law standards, such as the abuse of process doctrine, also come into play: police conduct which is unacceptable as an abuse of process is that which violates a community's sense of decency and fair play and police use of such techniques may lead to a judicial staying of proceedings against the accused. It should be noted that the use of SITs such as undercover operations are also governed by internal police policy and procedures. Comprehensive administration and accountability provisions addressing law enforcement activity is provided by laws addressing the establishment and organization of police forces, codes of conduct, and internal discipline (deontology), and public complaints.

491. Certain other SITs do have detailed provisions in law requiring prior judicial authorisation. These include, for example, interception of private communications and searches. Judicial authorisation requirements also apply to additional special procedures such as the taking of DNA samples, installation of tracking devices and installation of devices recording telephone numbers dialled (and the numbers from which calls are received).

492. In respect of SITs in which police would engage in illegal conduct, the Supreme Court of Canada has ruled that police have no inherent immunity from liability for unlawful conduct committed in good faith during the course of an investigation. The Supreme Court further noted that if immunity

were necessary, it was for Parliament to provide for it. On its face, this restrictive principle could apply, depending on the circumstances, to certain SITs. Parliament has, however, adopted provisions allowing law enforcement officers to engage in conduct that would otherwise be illegal for the purpose of investigations and enforcement, subject to controls and limitations. For example, measures under the Criminal Code provide a limited justification for designated law enforcement officers – and others acting at their direction – for acts and omissions that would otherwise be offences. The justification includes a fundamental requirement of "reasonable and proportional" conduct. Three factors are set out as relevant to determining reasonableness and proportionality: the nature of the act or omission, the nature of the investigation, and the reasonable availability of other means for carrying out enforcement duties. Certain conduct that would otherwise be an offence is justified only if a public officer has the prior written authorisation of a senior official responsible for law enforcement or in exigent circumstances. Certain other conducts, such as the intentional causing of death or bodily harm, obstruction of justice, or conduct that would violate the sexual integrity of an individual, are not justified.

493. Certain other exemptions and exceptions for specific law enforcement SITs that would otherwise be illegal are provided by separate legal provisions. For example, the Controlled Drugs and Substances Act (Police Enforcement) Regulations governs the use of controlled deliveries and reverse stings in drug investigations.

494. In the proceeds of crime context, provisions of the Criminal Code provide exceptions, respectively, for possession of property obtained by crime and for money laundering where this is done by a law enforcement officer – or a person acting under the direction of a law enforcement officer – for the purpose of an investigation or otherwise in the execution of the law enforcement officer's duties.

495. Canadian law enforcement undertakes co-operative investigations with appropriate authorities in other countries, especially with the US. Canadian authorities actively participate with foreign jurisdictions in both money laundering and criminal proceeds investigations. During these co-operative investigations, compliance with Canadian legislation is ensured. The participation of Canadian authorities is limited to its domestic legislative parameters, most notably with respect to the use of special investigative techniques.

Recommendation 28

496. Through authority in criminal law, law enforcement has the ability to compel production, to search persons or premises and seize or obtain documents, information or data while conducting ML, TF and underlying predicate offence investigations. The accessible information includes bank account records, customer identification records, and other records maintained by financial institutions and other persons through lawful process, as necessary, to conduct investigations of money laundering, terrorist financing and predicate offences.

497. Most of the procedures allowing law enforcement to compel production of, to search persons or premises and seize or obtain documents, information or data are found in the Criminal Code. The following list is describes several of the procedures frequently used by the police:

- Search warrant under s. 487 of the *Criminal Code* – search and seizure of evidence.
- Special search warrant seizures under s. 462.32 of the *Criminal Code* – search and seizure of proceeds of crime.
- Search warrant under s. 11 of the *CDSA* – search and seizure of evidence for a drug offence.
- Production order under s. 487.012 of the *Criminal Code* – production of documents or copies or preparation of a document.
- Production order under 487.013 of the *Criminal Code* – for financial and commercial information.
- General warrant under s. 487.015 of the Criminal Code.

- Order for gathering evidence under s. 83.28 of the *Criminal Code* (for terrorist offence only) – order the examination on oath or not of a person, order the person to bring any thing in their possession or control.
- Order for disclosure of information in respect of FINTRAC – for money laundering or terrorist activity financing offences only – for information or documents obtained by or on behalf of the Director of FINTRAC.
- Order for disclosure of income tax information under 462.48 of the *Criminal Code* – for a money laundering or possession of proceeds of crime offence, for a designated drug offence or a terrorism offence – tax information from Canada Revenue Agency.

498. Pursuant to paragraph 34(2) of the Interpretation Act, these procedures can be used while investigating suspected money laundering, terrorist financing, and all other offences of federal legislation, except if the legislation otherwise provides.

499. These procedures are issued by either a judge of the peace, a Provincial Court judge or a Superior Court judge. Before making an order, the justice or judge must be satisfied, on the basis of an ex parte application containing information on oath in writing, that there are reasonable grounds to believe that (a) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed; (b) the documents or data will afford evidence respecting the commission of the offence; and (c) the person who is subject to the order has possession or control of the documents or data.

500. During the on-site visit, the assessment team was told that such threshold is difficult to reach in practice, especially under Article 487.013 of the Criminal Code for collecting financial and commercial information. The law enforcement authorities met were also unanimous with regard to the difficulty to get valuable information from FINTRAC (limited data contained in “designated information” (although new PCMLTFA requirements in force since June 30, 2007 address this issue), lack of narrative information, delays in responding - see conclusions in relation to Recommendation 26 in Section 2.5 of the report). The law enforcement authorities met during the on-site visit also identified other types of impediments to the conduct of ML/TF investigation including access to information in possession of lawyers and access to ownership information on legal persons.

501. The RCMP has demonstrated an advanced capability in terms of using special investigative techniques for money laundering and proceeds of crime investigations. An example is the 'store front' operation referred to as Project Eldon, which involved establishing and operating an import / export business that provided money laundering services to organized crime. This investigation was conducted over several years, including the time that it took to establish the business and technical infrastructure, and to infiltrate and dismantle an international organised crime group with extensive involvement in money laundering offences. The investigation relied primarily on undercover policing techniques and was supported, among other things, by electronic surveillance and computer crime investigation capability. The RCMP has indicated that further covert money laundering investigations will be conducted based on the experiences learned from Project Eldon.

502. Law enforcement agencies in Canada have a wide range of investigative powers and capabilities for use against organized and serious crime, including for the investigation of ML, TF and predicate offences. The evaluation team noted that while the Canadian undercover policing programme was used for the investigation of money laundering, to attack the upper most levels of organised crime, there is no provision for protecting the true identity of the undercover police officer - instead, the true identity of the officer must be revealed to the accused person. This situation arises due to there being no dedicated legislative regime for conducting undercover policing operations. When compared with internationally equivalent jurisdictions, this was considered to be a weakness for special investigative techniques that may be used for money laundering investigations.

503. Competent authorities have the powers to take witness statements for use in investigations and prosecutions of ML, TF, and other underlying predicate offences and related actions.

504. In money laundering and terrorist financing cases, witness statements are taken voluntarily in accordance with the Charter of Rights and Freedoms and the Canada Evidence Act. However, in terrorist financing investigations, witnesses are bound to provide a statement. There are legislative provisions outlined under Part II.1 of the Criminal Code (Terrorism) whereby an investigative hearing can take place for the purposes of gathering evidence, including the questioning of persons, in respect to a terrorism offence. Those offences are outlined under Section 2 of the Criminal Code and include the financing of terrorism offences (Sections 83.02, 83.03 and 83.04 of the Criminal Code).

Recommendation 30 – structure, staff and resources

Law Enforcement

505. The RCMP provides federal policing services in all provinces and territories and provincial/municipal policing services in three territories, eight provinces (except Ontario and Quebec), more than 200 municipalities, 165 Aboriginal communities, three international airports and numerous smaller airports. In total, the RCMP employs approx. 23 466 employees, of which 16 327 are peace officers.

506. One of the RCMP's division or directorate that is particularly relevant for combating criminal activity and money laundering is the Federal and International Operations (FIO) group. This group works to ensure the safety and security of Canadians and their institutions, domestically and globally, through intelligence-based prevention, detection, investigation, and law enforcement measures taken against terrorists, organized criminals, and other criminal activity. The strategic priorities are: (1) effective support of international operations; (2) reducing the threat and impact of organized crime and (3) effective delivery of federal programs.

507. FIO works closely with other activities for the national delivery of federal programs. The assistance of Criminal Intelligence Directorate is crucial to timely, effective and efficient service delivery. Technical Operations provides specialized investigative supports services which encompass and enhance research and development on techniques and tools to ensure FIO's ability to conduct high level investigations. Under the FIO umbrella is Drugs and Organized Crime, Border Integrity, International Policing and Financial Crime.

508. *Drugs and Organized Crime* focuses on combating Organized Crime as well as drug related social and economic harm to Canadians. It works to reduce supply of and demand for illicit drugs using an integrated approach involving measures for prevention, education, enforcement, counseling, treatment and rehabilitation.

509. *Border Integrity* is responsible for enforcement issues related to Canada's borders, and enforcement of more than 250 federal statutes in a variety of areas. It also builds partnerships with stakeholders throughout all segments of Canadian society to provide the best response(s) to policing concerns, whether by investigating criminal offences, assisting federal government departments, informing and seeking input from general community and implementing problem oriented policing.

510. *International Policing* enhances international cooperation at strategic and tactical levels between RCMP and foreign police and law enforcement agencies. It provides support and assistance, through the liaison officers, to Canadian law enforcement agencies in the prevention and detection of offences to Canadian federal laws, liaises with foreign criminal police agencies and related institutions, and coordinates activities related to Interpol. In accordance with Canada's foreign policy, it selects, trains and deploys Canadian police personnel on UN civilian police missions and provides logistical support to them and their families.

511. *Financial Crime* contributes to the security of the Canadian economy and seeks to protect Canadians and their governments from financial crimes perpetrated by organized crime and others. It reduces, controls and prevents business-related or white-collar crime, including fraud, false pretenses, and offences against the Government of Canada, corruption of public officials, insolvency process,

counterfeiting and others. It also oversees RCMP's contribution to the Integrated Proceeds of Crime (IPOC) partnerships against money laundering.

Proceeds of Crime Program

512. The Proceeds of Crime Program coordinates the RCMP's components in combating money laundering and terrorist financing in relation to 2 federal government initiatives targeting Money Laundering and Criminal Proceeds of Crime, being the IPOC and the AML/CFT regime (see comments above under Recommendation 27). The following table provides the funding available for the RCMP's Proceeds of Crime Program as a result of the IPOC and AML/CFT regime.

Funding arrangements for the RCMP Proceeds of Crime Program			
Year	**IPOC**	**AML/CFT regime**	**TOTAL**
2005-2006	CAD40 796 662	CAD4 900 000	CAD45 696 662
2004-2005	CAD38 838 869	CAD4 900 000	CAD43 738 869
2003-2004	CAD38 693 000	CAD4 900 000	CAD43 593 000
2002-2003	CAD36 848 960	CAD4 900 000	CAD41 748 960

513. In addition to the resources identified above that are directly linked to the Proceeds of Crime Program, the program has access to other technical investigational support from within the RCMP. These resources include police undercover operations, source/agent operations and support, electronic and physical surveillance, and forensic science support to name a few.

514. Further statistics in relation to the resources available to the RCMP were provided to the assessment team. The first table identifies resources available to the RCMP in the context of the National Initiative to Combat ML (NICML) established in 2000. In that context, the RCMP got 12 extra staff in December 2006. The second table makes inventory of the resources of IPOC Units in 2007.

RCMP Resources in the context of the National Initiative to Combat ML (NICML)					
YEAR	FUNDING	REGULAR MEMBERS	PUBLIC SERVICE	Civilian Member	TOTAL POSITIONS
2002-2003	CAD4 900 000	30	1	4	35
2003-2004	CAD4 900 000	30	1	4	35
2004-2005	CAD4 900 000	30	1	4	35
2005-2006	CAD4 900 000	30	1	4	35
2006-2007	CAD4 900 000	30	1	4	35
2007-2008	CAD6 962 000	42	1	4	47

IPOC Units Resources				
Proceeds of Crime RCMP DIVISIONS 2007	Regular Member	Civilian Member	Public Service	**Total**
A Division (Ottawa)	10	1	3	**14**
B Division (Newfoundland)	5	0	3	**8**
C Division (Quebec)	62	5	16	**83**
D Division (Manitoba)	10	1	2	**13**
E Division (British Columbia)	39	3	12	**54**
F Division (Saskatchewan)	10	2	2	**14**
G Division (Northwest Territories)	1	0	0	**1**
H Division (Nova Scotia)	9	0	2	**11**
J Division (New Brunswick)	11	1	2	**14**
K Division (Alberta)	27	2	6	**35**
L Division (Prince Edward Island	0	0	0	**0**
N Division (HQ Ottawa)	11	1	3	**15**
O Division (Ontario)	56	2	12	**70**
TOTAL	251	18	63	**332**

515. As far as IPOC Units are concerned, RCMP has the same level of resources as of 1996 when the Units were set up. RCMP representatives insist on the fact that the type of investigations they carry out are more complex and require more time and resources than it was the case in the 1990's. In addition, the increase allowed in December 2006 (plus 12 staff) brings the resources to their level before the budget cuts that took place in the late 1990's. The evaluation team was informed that the RCMP received funding for an additional 1 000 positions to restore staffing in several programs where gaps had been identified: commercial crime; drug enforcement; federal enforcement services; customs and excise; immigration and passport, criminal intelligence; and technical operations. Initiatives, such as IPOC, were not identified for additional funding and positions could not be reallocated outside of the programs targeted.

516. Following September 11, 2001, the Government of Canada enhanced its terrorism response capabilities and improved the legislative framework for terrorist threats. The RCMP received funding to enhance analytical, intelligence sharing and operational technology; support protective operations; enhance security activities at airports, ports and borders; and focus on human resourcing for activities targeting cross-border criminal activities. The following enforcement units and funding were put in place to address National Security enforcement:

- Integrated National Security Enforcement Teams (INSETs) – CAD64M over 5 years.
- Integrated Border Enforcement Teams (IBETs) – CAD125M over 5 years.
- Financial Intelligence – CAD1M.
- Investigative Operations Support – CAD25M.
- Police Reporting and Occurrence System – CAD10M.
- Marine Security – CAD115M.
- National Ports Enforcement Teams – CAD11.5M over five years.
- Integrated Immigration Enforcement Teams –CAD18.7M over five years.

517. Despite the increase of budget, the RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations. The RCMP acknowledges that, due to resources constraints, it is essentially dedicates its resources to large and complex ML investigations related to organised crime groups.

Marine Security

518. The marine sector supports a vital trade gateway, connecting Canada to the world. In 2000, Canadian international marine trade, including traffic between Canada and the US, was valued at more than CAD100B, equalling one-eighth of the country's total trade, and employing more than 30 000 people.

519. The role of Canada's marine security includes the investigation of occurrences dealing with national security, organized crime and other federal statutes, such as those involving smuggling, illegal drugs and immigration. They also work with various Government departments as part of its integrated response to marine security, to help deter and detect any illicit and/or terrorist activity, cargo or people within Canadian waters. Budget 2004 included CAD115M for marine security issues and improvements to Canada's marine security.

National Ports Strategy

520. Through its National Ports Strategy, the RCMP strategically and tactically addresses criminal activities and terrorism at Canada's major marine ports. The objective is to take an intelligence-led, multi-disciplinary and integrated approach to prevent, deter and detect any illicit and/or terrorist activity, cargo or people at major marine ports that may pose a threat to national, US and global safety and security. The RCMP enforce federal statutes dealing with issues such as migrant smuggling, illegal drugs, illegal firearms.

National Ports Enforcement Teams (NPETs)

521. NPETs were established in 2003 to conduct investigations of federal offences relating to Canadian seaports. Comprised of partners from federal, provincial and municipal law enforcement agencies, NPETs are complemented by local management teams to resolve conflicts and identify roles and responsibilities. There are currently 24 RCMP members dedicated to NPETs, centered at Canada's three major ports. Commencing in 2003/04, CAD11.5M in funding over five years will be used to position investigators in major ports; increase training for marine intervention (*i.e.* ASB); and, conduct records checks of port employees for Transport Canada.

Airports

522. Airport Federal Enforcement Sections (AFES) are mandated to combat organized crime and terrorism by providing enforcement of numerous federal statutes, as well as assistance to various federal programs and departments. Since the inception of the AEFS system in 1999 the Airport Federal Enforcement Sections have seized over CAD460M worth of contraband, including drugs and weapons. A funding strategy is under development to expand the program at the Toronto site, as well as include other airports (*i.e.* Calgary and Ottawa).

Smuggling and Trafficking of Persons

523. Canada's long border, with high volumes of people and goods passing across, provides opportunity for the smuggling of contraband and prohibited goods. Challenges are also posed by expanding global migration by land, sea and air. In June 2002, Canada introduced the Immigration and Refugee Protection Act, creating new offences that directly address trafficking in human beings. In addition, as of November 2005, three new *Criminal Code* offences came into effect relating to trafficking in persons.

524. The Immigration and Passport Program (IPP) is being regionalized to meet evolving expectations and demands. The roll-out of the program continues, with the reallocation of funded positions to six locations – Vancouver, Calgary, the Greater Toronto Area, Ottawa, Montreal and Halifax. The focus of these teams will be to combat and disrupt organized migrant smuggling and the trafficking of persons, with more recent emphasis on those individuals and/or organizations posing a threat to the security of Canada. As of June 2006, the CBSA gained responsibility for criminal investigations related to migrant smuggling.

525. In addition to these regional teams, a new trafficking unit will be co-located with the Ottawa Immigration and Passport Section, focusing on the coordination of domestic and international trafficking investigations; interacting with foreign law enforcement agencies in support of Immigration and Passport teams; and, advocating education, prevention and awareness of these global problems[53].

526. A federal interdepartmental working group, consisting of 16 departments and agencies, is developing Canada's position on the UN Trafficking Protocol. The working group is responsible for co-ordinating federal activities to address trafficking including the development, promotion and implementation of a comprehensive anti-trafficking strategy, in keeping with Canada's international commitments.

527. Specialists from the RCMP have developed training material for the recognition of fraudulent travel documents. A collaborative effort is underway between BCDE and Interpol forensic analysts to improve Interpol's central databank for lost and stolen passports – Canada was selected as one of the countries to participate in this important pilot project.

---

[53] This unit has been formed and is fully functional. Information about the Human Trafficking National Coordination Centre (HTNCC) can be found at http://www.rcmp-grc.gc.ca/imm_pass/htncc_e.htm.

Prosecution

528. Until December 12, 2006 the Federal Prosecution Service of Canada was an integral branch of the Attorney General of Canada's function as part of the Canadian Department of Justice. On December 12, 2006 the Director of Public Prosecution Act came into force, resulting in the seamless transition of the Federal Prosecution Service into an independent public prosecutions office that reports to the Parliament of Canada through the Attorney General of Canada. The new Public Prosecution Service of Canada (PPSC) assumes carriage and control of all prosecution functions previously undertaken by the Federal Prosecution Services and the PPSC is tasked with all of the consultation and coordination responsibilities previously undertaken by the Federal Prosecution Service. The federal prosecutor complement includes 70 prosecutors working on proceeds of crime and money laundering litigation in Canada. These include the federal prosecutors assigned to the 12 IPOC units in the RCMP as well as counsel who prosecute the cases generated by the IPOC units. The 70 PPSC prosecutors are dedicated to POC prosecution

529. The provincial heads of prosecution manage and supervise all provincial crown prosecutors. As a result, this group of prosecution heads regularly meets to discuss and coordinate common prosecution issues. In the area of money laundering and proceeds of crime, there are two committees that have been created. The National Liaison Committee comprised of money laundering prosecutors, selected by and reporting to the heads of prosecution, meets yearly or more frequently to coordinate common issues relevant to money laundering prosecutions. The second committee is the Coordinating Committee of Senior Officials (CCSO) on Proceeds of Crime. It is also comprised of money laundering prosecutors and criminal law policy lawyers and reports to the Justice Deputy Ministers Committee (Federal, Provincial and Territorial).

530. The PPSC is also a partner in a national memorandum of understanding with the RCMP for the Integrated Proceeds of Crime Program. This integrated program includes a significant number of full time prosecutors, who are PPSC prosecutors, assigned to be members of the 12 IPOC investigative units. In addition, the program also funds PPSC prosecutors to actually prosecute the money laundering cases investigated by the IPOC units and general law enforcement. There is a regular series of meetings between the RCMP's national Proceeds of Crime program and the PPSC on money laundering and proceeds of crime. In addition, the PPSC has quarterly meetings with RCMP Federal Police Service to discuss and plan for investigative and prosecution issues, both in the proceeds of crime and general prosecution area.

531. There are also regional IPOC unit and PPSC regional office meetings, as mandated in the existing Memorandum of Understanding with the RCMP. These meetings resolve local problems and concerns that may develop in the proceeds of crime program. In addition, the PPSC will carry on the Federal Prosecutions Service's Cross Border Crime Forum meeting with law enforcement and the United States Attorneys Office. The Forum works on common prosecution issues, including proceeds of crime, with counterparts in the United States. The PPSC is a member of the International Association of Prosecutors and it attends that organization's annual meetings. Finally, the PPSC has counsel in its headquarters assigned to coordinate all proceeds of crime issues. That counsel conducts a quarterly video conference with all counsel in the IPOC units and the IPOC unit counsel have an IPOC common electronic mail room that is used daily to discuss money laundering and proceeds of crime issues between counsel.

Recommendation 30 – staff professional standards

Law Enforcement

532. Municipal, regional, and federal policing agencies conduct activities in accordance with the laws of Canada. To ensure enforcement and adherence to the laws and values of Canadian society, policing agencies have established professional and ethical codes of conduct. These matters are monitored through both internal and external processes, and may result in criminal judicial proceedings and/or internal disciplinary action.

533. The RCMP employs both regular (peace officers) and civilian members, who are subject to the provisions of the RCMP Act. The RCMP Act is a Federal statute, which governs the structure, operations, and ethical conduct of the membership. Members must pledge an Oath of Allegiance and an Oath of Secrecy pursuant to their engagement with the RCMP. The RCMP also employs public servants who take oaths of office and secrecy pursuant to the Public Service Act.

534. The Proceeds of Crime/Money Laundering investigative sections are integrated units tasked with conducting complex financial investigations. Professionals from the legal, accounting, asset management and taxation fields work with police investigators, from the RCMP and Regional/Municipal police services to conduct proceeds of crime/money laundering investigations. Each person assigned to the investigative unit is bound by the professional and ethical standards established by their respective organizations.

535. The Security of Information Act permanently binds all RCMP employees, which includes those assigned to the Proceeds of Crime/Money Laundering units and the National Security, who have access to special operational information to secrecy. Sensitive information obtained through the day-to-day operations of the Proceeds of Crime/ Money Laundering Units is classified using the RCMP security classification system. Access to this information is limited to those persons with the appropriate security clearance and who have an operational requirement to access the said information. Breaches with respect to classified, sensitive and or private information can be dealt with through criminal or internal disciplinary proceedings.

Prosecution

536. Prosecutors, as opposed to standing agents, are all full time appointment positions within the public service of Canada or a province. Each prosecutor must sign an oath of office and maintain their legal duty relative to solicitor client privilege. Just as full time prosecutors maintain privileged communications the same professional obligation applies to every standing agent. There are strong conflict of interest obligations and prohibitions against accepting outside work as legal counsel.

537. Every prosecutor, whether they work for a provincial Attorney General, director of public prosecutions or the federal Director of Public Prosecution, must be a full member of a provincial or territorial law society who is in good standing with that professional society. In addition they all operate independently of law enforcement and separate from the judiciary. Every prosecutor fully appreciates their responsibility as a quasi minister as described by Supreme Court of Canada and courts of appeal decisions. This role is best seen in the following excerpts from two cases: R. v. 1353837 Ontario Inc. and R.. v. Boucher[54].

Recommendation 30 – training

Law Enforcement

538. Since the inception of the Proceeds of Crime Program, the RCMP has taken the lead role in training investigators who specialize in these investigations.

---

[54] *The tradition of Crown counsel in this country in carrying out their role as "ministers of justice" and not as adversaries has generally been very high (R. v. 1353837 Ontario Inc., et al, February 24, 2005, C42378, at par. 34, per Laskin J.A. (Ont. C.A.)).* It cannot be over-emphasized that the purpose of a criminal prosecution is not to obtain a conviction; it is to lay before a jury what the Crown considers to be credible evidence relevant to what is alleged to be a crime. Counsel have a duty to see that all available legal proof of the facts is presented; it should be done firmly and pressed to its legitimate strength, but it also must be done fairly. The role of prosecutor excludes any notion of winning or losing; his function is a matter of public duty than which in civil life there can be none charged with greater personal responsibility. It is to be efficiently performed with an ingrained sense of the dignity, the seriousness and the justness of judicial proceedings. (R.. v. Boucher [1955] S.C.R. 16, at pp. 23-24; 100 C.C.C. 263, at p. 270.).

539. Specific eligibility requirements have been established in an effort to ensure that qualified and motivated personnel are hired by the RCMP. These requirements include specific language, education, physical and age restrictions. Upon completion of an extensive recruitment process which includes medical, physical and psychological testing the successful candidate attends the RCMP Training Academy situated in Regina, Saskatchewan for a five month training program. This training program is comprised of a number of courses including: Criminal Law, Firearms training, Driver training, Police Incident Reporting procedures, and witness/suspect interviewing techniques. This training provides the foundation for all aspects of policing within the RCMP.

540. Subsequent to the successful completion of this basic training, the candidate is given the legal authority to enforce the criminal laws of Canada. Human Resources Department will assess the needs of the RCMP and assign the new police officers to detachments throughout Canada. These police officers will further develop their policing skills through work experience and additional work related training. The "Proceeds of Crime" units seek experienced investigators who have developed their skills from both front line uniform and plain-clothes aspects of policing. To further enhance the skills of these investigators, the RCMP developed two training courses specific to "money laundering".

541. The RCMP currently offers a "Basic" and "Advanced" proceeds of crime investigators course. These courses, based at the RCMP's Centralized Training Facilities in Regina, Saskatchewan, follow the adult based learning model. Training is targeted primarily around RCMP proceeds of crime/money laundering personnel as well as employees of the initiatives partner agencies. Positions on these courses are based on the operational requirements of units and whenever possible, training is also given to non-program related investigators in order to increase both awareness and understanding of the program, while developing expertise for potential future proceeds of crime/money laundering investigators.

542. The Basic Proceeds of Crime course is offered to members of the RCMP assigned to the Proceeds of Crime program as well as employees of partner agencies. This course is seven days in length and concentrates primarily on the basic structure and methods used to investigate money laundering offences. A combination of experienced facilitators and a "problem base" method of instruction, allows participants to share their work experiences and explore different strategies in conducting these complex investigations.

543. In addition, municipal and provincial police partner agencies representatives have participated in these courses. The RCMP has also made efforts to educate other agencies, at both the federal and provincial levels. Federal agencies such as FINTRAC and the Competition Bureau have received training, while provincial agencies such as Revenue Quebec, have also been given the opportunity to partake in these courses. Internationally, the RCMP has trained six international law enforcement officers and continues to field requests from countries for this training.

544. The Advanced Proceeds of Crime Course is offered primarily to investigators, with approximately three years of proceeds of crime/money laundering experience and who have received the Basic Proceeds of Crime Course. Candidates are primarily from within the Proceeds of Crime/ Money Laundering Program and partner agencies. In addition, this training is also offered to seconded policing partners, both provincial and municipal, who have developed their expertise within their respective units. The course is also offered to other RCMP investigators. From January, 2001 to December, 2005, the RCMP has presented 20 Basic Proceeds of Crime courses and 8 Advanced Proceeds of Crime courses to close to 775 candidates.

545. To further meet the needs of the more complex investigations within the mandate of the RCMP, the RCMP has developed training programs which concentrated primarily on complex investigative techniques including wiretaps, search warrants, human source development and undercover police operations. The instructors for these training courses include police investigators and lawyers who are specialists in these areas. These techniques are used traditionally in drug investigations. With the

evolution of money laundering investigations, the RCMP has modified this training to demonstrate the application of these techniques within these types of investigations.

546. Within the money laundering/proceeds of crime investigators program, there are approximately 30 investigators who form an "Expert Witness Program" and provide "expert testimony" in criminal court pertaining to money laundering offences. To further supplement their experience, the RCMP provides a bi-annual expert and senior investigator's training workshop where these investigators share their knowledge on money laundering investigative techniques, trends and typologies.

Prosecution

547. All prosecutors must maintain their status as members of their relevant provincial or territorial law society. Every law society has a continuing legal education obligation for its members. In addition every Attorneys General department, including the federal Attorney General of Canada, and the Office of the Director of Public Prosecutions has a continuing legal education policy and extensive training courses in their manuals and procedures. In the case of federal prosecutors working for the Office of the Director of Public Prosecutions each must have an annual performance review report, which includes a specific component on continuing legal education.

548. Every year, the Director of Public Prosecution organizes the School for Prosecutors and the Advanced School for Prosecutors. Each school is an intensive seven-day training course on substantive law, policies and practice. Every year, approximately 30 prosecutors attend each school. Each provincial prosecution service has similar training obligations and programs.

549. The federal Department of Justice and the Office of the director of Public prosecutions has a formal Continuing Legal Education Policy, which requires each of its lawyers to take a minimum of 12 hours of training, or to teach for at least four hours, every year. The policy is based on a number of principles, one of them being that "Crown counsel are expected to maintain a high level of expertise by keeping abreast of developments in the law." The policy may be found on the Department's intranet site, under the heading Continuing Legal Education. Finally, every prosecutor's mandatory annual performance review includes a detailed consideration of the prosecutor's successful completion of their training obligations and their training plans for the next year.

550. Training initiatives dedicated to combat ML and TF seem limited in practice.

Additional elements

551. The National Justice Institute is dedicated to the development and delivery of educational programs for all federal, provincial and territorial judges.

552. The Institute has conducted a Criminal Law Seminar in March 2007 that has focused on financial Crimes. One of the agenda items dealt specifically with money laundering issues.

553. In addition, an RCMP senior investigator and a Department of Justice prosecutor traveled to Ottawa in 2004 and 2005 to provide training on money laundering investigations and prosecutions to the CBSA's Adjudications Division. Also, a senior investigator of the RCMP made a money laundering presentation to the Osgoode Hall Law School continuing development program on February 11, 2006.

Statistics

554. The following table provides an overview of the investigative work at the IPOC units in recent years.

Trends in All Files Opened, by Year and Predicate Offence								
	2002		2003		2004		2005	
Predicate Offence	#	%	#	%	#	%	#	%
Drug related	643	39.7%	606	35.7%	1288	42.1%	1511	45.3%
Proceeds of crime /Money laundering	476	29.4%	552	32.5%	1329	43.5%	1481	44.4%
Customs related	54	3.3%	51	3.0%	87	2.9%	101	3.0%
National security	17	1.0%	5	0.3%	7	0.2%	1	0.1%
Other Criminal Code offences	68	4.2%	54	3.2%	155	5.1%	240	7.2%
International requests	178	11.0%	161	9.5%	54	1.7%	0	0.0%
Predicate undetermined	185	11.4%	267	15.7%	137	4.5%	0	0.0%
TOTAL	**1621**	**100%**	**1696**	**100%**	**3057**	**100%**	**3334**	**100%**

2.6.2 Recommendations and Comments

555. Canada should ensure that additional resources are allocated to law enforcement authorities to allow them to carry out a larger number of ML/TF investigations (including at provincial level) in addition to the biggest ML cases they can actually tackle.

556. Canada should also collect more data on current ML investigations (especially in Ontario and Quebec).

557. Canada should consider reviewing the possible existing impediments to ML/TF investigations (including access to information in possession of lawyers and access to ownership information on legal persons). Access to tax information, while provided for, could also be enhanced.

558. Canada should improve the educational and training programmes provided for judges and courts concerning ML and TF offences.

2.6.3 Compliance with Recommendations 27 & 28

Rec.	Rating	Summary of factors underlying ratings
R.27	LC	▪ The RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations.
R.28	C	▪ The Recommendation is fully met.

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

Declaration system

559. Canada's mandatory cross-border currency reporting regime came into force in January 2003. Under Part II of the PCMLTFA, any person or entity is required to report to Canada Border Services Agency (CBSA) officers the importation or exportation of currency and monetary instruments of an amount of CAD10 000 or more. The requirements apply whether the currency or monetary instruments are brought across the border by the importer or exporter themselves, (*e.g.* carried in baggage) or imported or exported by mail, courier, rail or by any other means. This reporting requirement applies to the physical movement of money, not to funds transferred electronically.

560. Section 12 of the PCMLTFA establishes the requirement to report the cross-border movement of currency or monetary instruments over a set amount. The Cross-Border Currency and Monetary Instrument Reporting Regulations set out the reporting threshold and other modalities of the reporting obligations.

561. The regulations define the term "monetary instruments" as including, among other things, stocks, bonds, bank drafts, traveller's cheques or any other financial instruments in bearer form or in such form as title to them passes on delivery, and set the reporting threshold at CAD10 000 or its

equivalent in a foreign currency. The report must be made in writing using the forms designed by the CBSA – the Cross-Border Currency or Monetary Instrument Report (CBCMIR). Limited provisions exist to allow for reporting from remote locations. If there is no CBSA office in the vicinity, reporting may be done by telephone. The CBSA officer could request that the importer or exporter present themselves at a specified place for examination of the currency or monetary instruments.

562. The regulations also provide for certain exceptions from reporting, such as when currency or monetary instruments are brought into Canada aboard a commercial passenger conveyance (airplane, charter bus, cruise ships or ferry), and where Canada is a transit point rather than the final destination. It does not apply where the passenger disembarks and reports to CBSA. Also exempt are movements of currency by or on behalf of the Bank of Canada that the Bank is manufacturing for other jurisdictions, as well as stocks, bonds and debentures imported into Canada by courier or as mail, if the importer is a financial institution or a securities dealer as defined in section 1(2) of the PCMLTFA.

563. In practical terms, the system used to detect the physical cross-border transportation of currency varies among the modes of transportation as well as whether individuals are coming to or leaving Canada. For example, in the case of incoming flights to Canada, all passengers must complete a CBSA Declaration Card where they declare if they are in possession of currencies and monetary instruments of a value equal or greater than CAD10 000 and hand over this declaration to a CBSA officer who may ask additional questions. For outgoing flights, CBSA will use a mix of intelligence information and random searches to target flights where passengers will be asked whether they are transporting CAD10 000 or more.

Failure to declare

564. Subsection 12(4) of the PCMLTFA imposes an obligation to any person arriving or leaving Canada to answer truthfully any questions from CBSA officers in respect of the reporting of currency or monetary instruments. The PCMLTFA provides for a maximum fine of CAD500 000 and a maximum jail term of five years for failure to report or for failure to cooperate with the border services officer when a report is submitted. This would include refusing to answer questions posed by the border services officer or failing to open packages or containers.

565. The CBCMIR form requires individuals to report the value of currency and monetary instruments being exported or imported, the country from which the funds are being exported or imported and key identifying information. If an individual fails to report the currency or monetary instruments whose value is equal to or greater than the CAD10 000 threshold CBCMIR, the CBSA officer may seize the currency. The individual CBCMIR can recover the currency or monetary instruments on payment of a monetary penalty ranging from CAD250 to CAD5 000. If the CBSA officer believes there are reasonable grounds to suspect that the funds are the proceeds of crime or linked to terrorist activities, the funds cannot be recovered.

Stop or restrain currency or bearer negotiable instruments

566. When an individual fully complies with the requirement to report on currency above the threshold, a CBSA officer who has reasonable grounds to suspect that information contained in the report or any other information may be relevant to the investigation or prosecution of a money laundering or terrorist financing offence is permitted to immediately disclose this information to law enforcement authorities. The CBSA officer may also provide information to FINTRAC where the information could be useful in the detection, prevention or deterrence of money laundering or terrorist financing.

567. Section 18 of the PCMLTFA grants authority to CBSA to seize unreported currency or monetary instruments. All seizures are reported to FINTRAC. If the border services officer suspects the seized money to be proceeds of crime or funds for use in financing a terrorist activity, it is forfeited to the Crown. Otherwise the CBSA will release the funds upon payment of a penalty ranging from

CAD250 to CAD5 000. The PCMLTFA allows the person from whom the funds were seized, or their owner, to appeal the seizure.

568. Under section 14 of the PCMLTFA, when an individual or entity does not have all the information needed to complete a report, the CBSA can temporarily retain the money until a border services officer is satisfied that they have been reported or the importer/exporter has decided not to proceed with the importation/exportation. If CBSA is not provided further information for seven days (30 days for mailed or items sent by courier), the money is forfeited to the Crown.

Retention of information

569. Every person or entity is obliged to complete a CBCMIR on the importation or exportation of currency or monetary instruments of a value equal to or greater than CAD10,000 in Canadian dollars or its equivalent in foreign currency. CBSA sends the reports to FINTRAC, which incorporates them into its database for analysis. The schedules to the Cross-Border Currency and Monetary Instrument Reporting Regulations set out the information that must be provided in the mandatory reports, including identifying information on the person transporting, mailing or shipping the currency or monetary instruments, as well as information on the person or entity on behalf of which the importation or exportation is made. Information on the amount and type of currency or monetary instruments must also be provided.

570. When unreported currency or monetary instruments are seized, a seizure report is prepared by CBSA officials and forwarded to FINTRAC. The seizure report includes, among other things, identifying information on the importer or exporter, the funds seized and the circumstances of the seizure.

Information accessible to the FIU

571. CBSA forwards all Cross-border Reports submitted by importers or exporters as well as seizure reports to FINTRAC electronically. FINTRAC analyzes this information in conjunction with other reports in order to identify potential money laundering and terrorist financing activities. The border services officer will report through the Occurrence Reporting System (ORS) an explicative summary of the circumstances and detailed information on the occurrence, the individual or any other information that the officers evaluate to be of importance for the intelligence community. This report is submitted to the Intelligence Directorate by the Regional Intelligence Officer for analysis. The relevant information is then disclosed to FINTRAC.

Co-ordination among customs, immigration and other related authorities

572. Domestic authorities co-ordinate their activities to stop and restrain the illegal cross-border transportation of currency and other monetary instruments through a variety of different mechanisms: the IPOC Units, Integrated Border Enforcement Teams (IBETs), and the sharing of cross-border reporting information by CBSA.

573. Within IPOC units, CBSA Regional Intelligence Officers provide expertise and intelligence on CBSA matters linked to the border concerning proceeds of crime investigations. CBSA Regional Intelligence Officers also provide a service to border services officers by responding at the ports of entry to incidents related to forfeitures of currency that may be associated to organised criminal groups. In return, CBSA receives expert advice and intelligence information from the IPOC partners to assist in CBSA matters.

574. Integrated Border Enforcement Teams (IBETs) are a Canada/U.S. initiative set out in the Smart Border Accord. These Teams combine the intelligence and law enforcement expertise of various agencies (Canada Border Services Agency, Royal Canadian Mounted Police, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement and U.S. Coast Guard) and use a coordinated approach to identify and stop the high-risk movement of people and goods between the

ports of entry on the Canada - United States border. The CBSA and RCMP jointly operate IBETs. They share the responsibility for collecting critical information to develop criminal intelligence to assist in investigations relating to national security or criminality such as organized crime and human smuggling.

575. In addition, the CBSA sends Cross-border Reports and Seizure Reports to FINTRAC for analysis (see description above).

International co-operation and assistance amongst customs, immigration and other related authorities

576. Section 38 of the PCMLTFA allows the CBSA to enter into information sharing agreements with other countries that impose similar requirements in respect of reporting the importation or exportation of currency or monetary instruments. The CBSA is currently negotiating with the United States to enter into such an agreement.

577. Canada has a partnership agreement with the United States under the Shared Border Accord, allowing the governments of both countries to better manage the flow of refugee claimants at their shared border. This agreement allows for exchange of information between the two countries on:

- Advance Passenger Information and agreed-to Passenger Name Records on flights between Canada and the United States, including in-transit flights in order to identify risks posed by passengers on international flights arriving in each other's territory.
- Data related to Customs fraud, and agreed upon customs data pursuant to NAFTA, as well as any additional commercial and trade data, for national security purposes.
- Advance information on designated individuals and organizations for the purpose of freezing of terrorist assets.
- Refugee and asylum claimants in order to ensure that applicants are thoroughly screened for security risks.
- Marine in transit containers arriving in Canada and the United States.
- Anti-terrorism efforts through the Cross-Border Crime Forum and Project Northstar.

578. Canada entered into a trilateral agreement with the U.S and Mexico called the Security and Prosperity Partnership (SPP) in June 2005. The Partnership is a trilateral effort to increase security and enhance prosperity among the three countries through greater cooperation and information sharing. It includes efforts to develop and implement a comprehensive North American strategy for combating transnational threats to the three countries, including terrorism, organized crime, illegal drugs, migrant and contraband smuggling, and human trafficking.

Sanctions

579. Section 74 of the PCMLTFA provides for a maximum criminal fine of CAD500 000 and a maximum jail term of five years for failure to report or to cooperate with the border services officer when a report is submitted, such as falsely or not answering questions posed by border services officers or failing to open packages or containers as requested.

580. Part II of the PCMLTFA also provides that non-reported currency or monetary instruments is seized. Where there is no suspicion that the funds are linked to money laundering or terrorist financing, the owner may retrieve the forfeited funds after payment of penalties from CAD250 to CAD5 000 set out in the regulations. The funds cannot be retrieved when such a suspicion exists. Under section 18 of the PCMLTFA, unreported currency or monetary instruments in respect of which a border services officer has reasonable grounds to suspect are related to money laundering or the financing of terrorist activities are seized and forfeited and cannot be retrieved by the importer or exporter, subject to the appeals provisions.

581. In instances where a CBSA officer intercepts a foreign national or non-Canadian citizen suspected of involvement in money laundering or terrorist financing activities, they are instructed to

forward the file to CBSA's Organized Crime Section (OCS) at National Headquarters. OCS then analyzes the file based on in-house databases and research tools, and will request, if necessary, support from the appropriate units of partner agencies in law enforcement and intelligence, as well as FINTRAC. Once a portfolio-wide analysis has been completed, OCS contacts the originating officer with an assessment to assist that officer in deciding upon the proper course of enforcement action, possibly in concert with law enforcement partners, depending on the specific details of the case.

Confiscation, freezing and seizing measures

582. Generally, the provisions in Canada in respect of the confiscation, freezing and seizing of proceeds of crime or funds for terrorist activities also apply to the cross-border movements of currency or monetary instruments. When there is suspicion that the funds may be related to money laundering or terrorist financing, the various provision described in Section 2.3 of this report apply, in respect of the restraining of funds through criminal or civil procedures. Provisions under the PCMLTFA, the Criminal Code and other criminal or civil procedures for the confiscation, freezing and seizing of terrorist funds also apply to the cross-border movements of currency or monetary instruments. The measures are described in detail in Section 2.4.

Unusual cross-border movement of gold, precious metals or precious stones

583. Section 110 of the *Customs Act* gives CBSA officers the authority to seize goods where he or she has reasonable grounds to believe that the *Customs Act* or regulations have been contravened with respect to those goods. Gold, precious metals and stones are goods that are required to be declared upon importation. In cases where they are not properly declared, the CBSA can seize them with terms of release. In addition, section 101 of the *Customs Act* gives officers the authority to detain goods until he or she is satisfied that they have been dealt with in accordance with the *Customs Act* or any act of Parliament that prohibits, controls or regulates the importation or exportation of goods. This provision would apply to rough diamonds that are dealt with under the *Export and Import of Rough Diamonds Act*. CBSA officers also have authority under s.489(2) of the *Criminal Code* to seize goods where he or she has reasonable grounds to believe that the goods have been: obtained through the commission of an offence; used in the commission of an offence; or, will afford evidence of an offence under the *Criminal Code* or any other Act of Parliament.

Data protection

584. Section 36 of the PCMLTFA prohibits the unauthorised disclosure by a customs officer of information contained in a Cross-border currency and monetary instrument report or other information obtained in the course of enforcing the reporting requirement. Information forwarded to FINTRAC is subject to the privacy safeguards applicable to other information received by FINTRAC under the PCMLTFA. The CBSA sends the completed reports electronically, in a secure manner, to FINTRAC (see also comments in relation to FINTRAC detention of information in Section 2.5 of the report).

Additional elements

585. Canada has implemented the measures outlined in the Best Practices Paper. A number of these measures have been described earlier. In addition, the following measures are also in place:

- The threshold that triggers the reporting requirement is less than the threshold suggested by the FATF (CAD10 000 is roughly equal USD10 000 or EUR6 600).
- CBSA uses canine units, scanners and other sophisticated equipment to detect currency.
- The Bank of Canada stopped issuing the CAD1 000 bank notes in 2000. The largest note in active circulation is the CAD100 note.
- CBSA performs risk assessments and uses intelligence information to target all modes of transportation and travellers.
- CBSA officers are trained to detect suspicious behaviour by identifying indicators that are taught in various training courses.
- CBSA regularly performs examinations of passengers, vehicles, cargos, etc.

586. The Canada Border Services Agency (CBSA) uses a variety of technological tools to help stop the entry of contraband and dangerous goods into Canada. The use of detection technology tools enables CBSA officers to conduct effective, non-intrusive inspections, allowing them to focus on high-risk individuals and goods.

587. In the past, the CBSA's detection tools were developed primarily for the identification of contraband commodities (*i.e.* narcotics, weapons, child pornography, etc.). Recently, new legislation, policies, and programs initiated in support of fighting terrorism placed greater focus on border security. An integral part of Canada's plans in the fight against terrorism includes providing the necessary resources to purchase detection equipment. The CBSA has spent over CAD70 million in the last few years on new technology to improve border security.

588. Some of key interdiction technologies are: Gamma-ray Imaging Program (VACIS – Vehicle and Cargo Inspection System); the Remote Operating Vehicle (ROV), X-Ray Program and Ion Mobility Spectrometry (IMS) Technology. The CBSA also utilizes many smaller handheld tools. For example, the Snake Eye Camera is a self-contained, lightweight video inspection system. The Merlin Density Meter is a hand-held non-intrusive detection device that can indicate the presence of hidden contraband by measuring the density of a surface or an object. Videoprobes are used to inspect narrow spaces for hidden contraband in the air and land modes. The CBSA utilizes Contraband Outfitted Mobile Examination Truck, Chemical Biological Radiological Nuclear (CBRN) Detection Teams as well as Detector Dog Service.

Resources

589. The CBSA is part of the Public Safety and Emergency Preparedness (PSEPC) portfolio and is an integral component of Canada's national security approach along with other portfolio partners such as the RCMP, CSIS, etc. The CBSA integrates complementary business lines to protect public security and facilitate and control the movement of people and goods. Employing approximately 10 000 public servants, for which 7 500 are border services officers, the CBSA operates at 1 369 service points across Canada and nearly 40 locations abroad.

590. The 7 500 border services officers located at Canada's point of entry, among many other duties, are responsible to enforce the reporting requirement of Part II of the PCMLTFA. CBSA Intelligence officers located either in the regions or at Headquarters provide information or intelligence concerning individuals and organizations suspected of involvement in money laundering or terrorist financing activities to the officers. Then, senior program officers located at Headquarters coordinate and provide functional guidance on the program policies and procedures and address any issues relevant to the program's enforcement or administration.

591. The CBSA's current budget for the Cross-Border Currency Reporting Program is CAD2.43M yearly. CBSA will receive an additional CAD3.5M yearly in order to expand its intelligence mandate, cross border currency reporting, currency dog teams and deal with the seizure appeals. This will bring the CBSA's allocation to CAD5.93M yearly.

592. CBSA employees have relevant experiences and skills in sectors such as the law enforcement, customs, immigration, justice, and public safety as well as backgrounds in other government departments and international organizations.

593. The CBSA has implemented enhanced security measures and employees participate in security awareness sessions. A security program, and a range of policies and procedures to protect privacy, and prevent unauthorised disclosures of information, are in place and are upheld. They include the application of the need-to-know principle, guiding principles for the handling of sensitive and classified information and application of measures surrounding the analysis and disclosure processes. In addition, the clearance level required for CBSA employees involved in these issues demonstrates

the importance attached to the confidentiality of sensitive financial and personal information that is obtained and analyzed by its employees.

594. New CBSA officers graduate from the Port of Entry Recruit Training program at the CBSA training facility in Rigaud, Québec. Among other things, they are taught how to recognize and investigate based on key indicators, intelligence information, and suspicious activities and are provided with a web-based training for cross border currency related infractions as well as information related to money laundering and terrorist financing. Adjudicators working on behalf of the Public Safety Minister receive a half-day training course from the RCMP and Crown Prosecutor on money laundering and terrorist financing activities. A handout of the RCMP indicators as well as a booklet prepared by the RCMP on Money Laundering is provided at the training session.

Statistics

595. Statistics are available on the number of CBCMIRs involving movements of CAD10 000 or more in currency or monetary instruments.

Effectiveness

596. The number of CBCMIRs and seizure reports since 2002/2003 is as follows:

Report Type	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]	Total
Cross Border Currency Report	631	28 289	74 103	52 626	19 289	174 938
Seizure Report	19	1 080	1 718	1 880	625	5 322
Total	650	29 369	75 821	54 506	19 914	180 260

[1] Fiscal year 06-07 statistics include only what was received from CBSA up to September 30, 2006. CBSA receives CBCMIRs, captures the information electronically and transfers it to FINTRAC.

597. In 2005-06, 18% of FINTRAC's case disclosures were supported by cross-border currency and seizure reports.

598. Since the program implementation in January 2003, there have been over 5 000 currency seizures totalling more than CAD132 million. Approximately CAD34 million has been forfeited to the Crown, and penalties have been assessed in excess of CAD2 million. Over 500 seizures have resulted in forfeiture as suspected proceeds of crime or funds for the use of terrorist activities. Border services officers have collected over 100 000 cross-border currency reports.

599. Seizures related to cross-border currency transportation are classified into four levels based on the degree of concealment, previous seizures and the source of currency or monetary instruments. In levels one to three, a fine must be paid prior to release of the seizure. When seizures are made based on the suspicion it stems from proceeds of crime or terrorist financing (the fourth level), there are no terms of release. The following table describes the four levels of seizure related to cross-border currency interdictions and the fines that must be paid prior to the release of the seizure.

Level	APPLICATION	FINE
I	Applied when an individual or entity • has not concealed the currency or monetary instruments, • has made a full disclosure of the facts concerning the currency or monetary instruments on their discovery, and • has no previous seizures under the Act;	CAD250
II	Applied when an individual or entity • has concealed the currency or monetary instruments, other than by means of using a false compartment in a conveyance, or who has made a false statement with respect to the currency or monetary instruments, or • has a previous seizure under the Act, other than in respect of any type of concealment or for making false statements with respect to the currency or monetary instruments; and	CAD2500
III	Applied when an individual or entity • has concealed the currency or monetary instruments by using a false compartment in a conveyance, or • has a previous seizure under the Act for any type of concealment or for making a false statement with respect to the currency or monetary instruments.	CAD5000
IV	Applied when • CBSA Officers, who suspect on reasonable grounds that non-reported currency or monetary instruments are proceeds of crime or terrorist finances.	No terms of release

600. Since 2003, the RCMP has been asked to provide investigational assistance in 147 Level IV seizures conducted by CBSA officials. The following table provides a yearly breakdown of requests from CBSA to the RCMP's Money Laundering Program for assistance in these seizures.

Reports of Canada Border Services Agency (CBSA) Callouts				
	2003	2004	2005	Total
Number of Callouts	72	53	22	**147**

601. Since 2003, the Adjudications Division has seen numerous challenges of these enforcement actions. Level IV forfeiture enforcement actions tend to be highly litigious. Since 2003, of the 6 007 enforcement actions taken by the CBSA (at September 30, 2006), 666 of those actions have been appealed to the Recourse Directorate. Of those 666 appealed actions, only 55 have been cancelled and all funds have been returned. There are currently 45 active cases before the courts.

602. In 2004, the largest number of currency and proceeds of crime seizures (732) were made at customs points of entry located in the Pacific region, representing 45% of all seizures made. Customs officers in the Greater Toronto Area made 367 seizures, while officers in the Québec region made 338, officers at Niagara Falls/Fort Erie made 85, those in Windsor/St. Clair made 39, Prairie region made 27, Northern Ontario made 24 seizures and the Atlantic region made 4 interceptions. Combined, the Pacific, Quebec and the three regions of southern Ontario intercepted the bulk of all unreported currency and proceeds of crime totalling CAD42 301 608 million, accounting for 96% of the national total. In most cases, currency and proceeds of crime interceptions involved citizens of Canada, China and the United States. Canadians were involved in 10% (165) of the seizures totalling CAD4.1 million; citizens of China accounted for 21% (345) of the seizures totalling CAD7.6 million, and citizens of the United States were involved in 25% (401) of the interceptions yielding CAD18.1 million.

603. The following table shows the number and value of seizures made by type of currency for the year 2004.

Currency Type Seized	Number of Seizures	Value of Currency
Banker's drafts	26	CAD919,046
Bonds	3	CAD141,456
Cheques	54	CAD2,503,720
Currency	1450	CAD39,062,887
Money orders	20	CAD350,494
Other instr. in bearer form	1	CAD1,360
Stocks	1	CAD12,300
Traveller's cheques	60	CAD998,874
Treasury bills	1	CAD24,180
TOTAL	**1,616**	**CAD44,014,317**

Source: Cross-Border Currency and Proceeds of Crime Report 2004, Canada Border Services Agency.

604. This table shows the interceptions made in 2004, by referral type. The final two columns indicate the value and percentage (relative to the total) of seizures that were related to proceeds of crime.

Referral Type	Number of Seizures	Total Value of Currency Seized CAD	Value of which are Level IV – Proceeds of Crime CAD	Percent of Total
Selective referrals	1 382	**34 635 545**	7 412 250	21.4%
Lookouts	75	**5 284 884**	4 343 478	82.2%
Random referrals	38	**956 416**	374 202	39.1%
Targeting	17	**292 124**	29 787	10.2%
Canine indicators (DDS)	29	**753 210**	224 538	29.8%
Export examinations	56	**1 589 496**	633 796	39.9%
U.S. Customs referrals	5	**197 818**	44 284	22.4%
Other	14	**304 825**	0	0.0%
TOTAL	**1 616**	**44 014 318**	**13 062 335**	29.7%

Source: Cross-Border Currency and Proceeds of Crime Report 2004, Canada Border Services Agency.

2.7.2 Recommendations and Comments

605. Canada has a comprehensive system to protect the physical cross border transportation of currency and monetary instruments of a value of CAD10 000 or more and the law enforcement authorities have a clear understanding of the procedures that are in place in Canada for implementing SRIX. A range of methods and technologies are employed at the border to enhance capability relating to cross border currency enforcement. The legal authority for this is supported by a strategic and operational response that demonstrates close cooperation between agencies, especially enforcement agencies from the United States.

606. The effectiveness of Canada's cross border currency enforcement is demonstrated in the significant volume and value of currency seizures – 5 130 currency seizures totalling more than CAD132 million since January 2003. Seizures have been result of a broad range of enforcement methods, across a broad range of monetary instruments and currency, at various entry points into Canada - all of which indicates a broad enforcement response by Canadian authorities.

607. The assessment team however believes that competent authorities should further invest in the detection and investigation of out-going cross-border transportations of cash or any negotiable bearer instrument.

2.7.3 Compliance with Special Recommendation IX

Rec.	Rating	Summary of factors underlying ratings
SR.IX	C	▪ The Recommendation is fully met.

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

Overview of legal and regulatory framework

PCMLTFA and its Regulations

608. To combat money laundering, the Canadian federal government enacted the Proceeds of Crime (Money Laundering) Act which received Royal Assent on June 29, 2000. To help fight terrorism, it enacted the Anti-Terrorism Act (Bill C-36) which came into force on December 24, 2001 and amended the Proceeds of Crime (Money Laundering) Act, which became the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

609. The basis for the AML/CFT preventive legislation in Canada is the PCMLTFA that consists of five parts:

- Part I sets out record keeping requirements and requires the reporting of suspicious and prescribed financial transactions.
- Part II creates the obligation to report to Customs the importing or exporting of currency or monetary instruments of a value equal to or greater than CAD10 000 or its equivalent.
- Part III establishes FINTRAC as an independent agency to collect, analyze, assess and disclose designated information on financial transactions to assist in the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while protecting Canadian's privacy.
- Part IV authorises the Governor in Council to make regulations.
- Part V creates offences, including the failure to report suspicious financial transactions and the prohibited use of information under the control of FINTRAC.

610. The PCMLTF Regulations implement a portion of Part I of the Act by requiring the financial institutions and financial intermediaries that are subject to the Act to identify their customers, keep certain records, report large cash transactions and international electronic funds transfers of CAD10 000 or more to FINTRAC and develop an internal compliance regime.

611. The PCMLTF Suspicious Transaction Reporting Regulations implement the remainder of Part I of the Act by requiring financial institutions and financial intermediaries to report financial transactions where there are reasonable grounds to suspect that they are related to money laundering or terrorist financing activities.

Recent amendment of the PCMLTFA and its Regulations

612. The Department of Finance issued a consultation paper in June 2005 outlining policy proposals to enhance the AML/CFT regime. These proposals included a series of new requirement such as the obligation to identify beneficial owners of client entities and to conduct enhanced due diligence for correspondent banking relationships and politically exposed persons. The adoption of a new registration scheme for money services businesses and of an administrative monetary penalties scheme was also proposed.

613. In October 2006, the Minister of Finance tabled Bill C-25, which proposed amendments to the PCMLTFA to expand the customer due diligence and transaction reporting requirements for financial institutions and financial intermediaries, set out a framework for the registration of money services businesses and extend the list of information that FINTRAC may disclose to law enforcement and

intelligence agencies. This Bill received Royal Assent in December 2006. However, a series of successive regulations is due to be adopted for the PCMLTFA to be fully effective.

614. Some new provisions of the PCMLTFA came into force on February 10, 2007 including technical amendments and information sharing in respect of cross border reporting regimes, FINTRAC record retention time limits, information sharing on charities and terrorist financing and a review of the Act by Parliament and the Office of the Privacy Commissioner. A "carve out" for suspicious transaction reporting by legal counsel also took effect.

615. On March 10, 2007, in the format of a pre-publication in the Government Gazette, the Canadian Department of Finance opened two proposed regulations (*Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* and *Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*) to consultation[55]. The consultation period ended on April 9, 2007. Quite a large number of financial institutions, financial sector associations and professional associations sent representations regarding the feasibility of the proposed amendments and possible coming-into-force dates for the new provisions. Overall, the assessors were told that stakeholders were supportive of the proposed enhancements to Canada's regime. However, with regard to the proposed registration system, some of them have suggested modifications to the proposed amendments to reduce the compliance burden[56].

616. On June 27, 2007, the *Regulations Amending Certain Regulations Made Under the PCMLTFA* were enacted and published in the Canada Gazette (Part II). A second package of regulatory amendments, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* was published, which sets out a framework for the registration of MSBs.

617. Additional amendments are necessary for the regulations to implement fully the legislation. For instance, amendments to the PCMLTF Regulations and PCMLTF Suspicious Transaction Reporting Regulations were pre-published on June 30, 2007 to address some of the measures that still need to be adopted. The proposed amendments extend coverage of the PCMLTFA to three non-financial professions (see Section 4.1 of the report). A proposed PCMLTF Administrative Monetary Penalties Regulations also set out specific measures for an administrative monetary penalties scheme. These proposed amendments were open to consultation until August 2007[57].

---

[55] Draft regulations in Canada must be pre-published in Part I of the Canada Gazette, before they can be made. Pre-publication in Part I of the Canada Gazette gives various interested groups and individuals, as well as Canadians in general, a final opportunity to review and comment on a proposed regulation at the last stages of the regulation-making process, before it is enacted and published in Part II of the Canada Gazette. Pre-publication also gives interested parties, and those stakeholders previously consulted at the beginning of the regulatory process, the opportunity to see whether the final draft proposal is in keeping with previous consultation drafts and to comment on the implementation timeline.

[56] The regulatory impact analysis of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations* of 7 June 2007 states the following: "for example, as requested by a group of money services businesses, amendments to the Regulations exempt the sector from customer due diligence requirements when they enter into a service agreement with a publicly traded company or public body. Other exemptions to the client identification and record-keeping requirements have been added to alleviate the compliance burden for securities dealers and other sectors. As proposed by banks and credit unions, the definition of politically exposed foreign persons has been limited to fewer family members and the timeframe for the identification of such persons has been extended. Following discussions with banks, the record-keeping requirements applicable to financial entities for funds transfers of CAD 1 000 or more have been limited to international electronic funds transfers and domestic SWIFT MT103 transfers. Likewise, the obligation to keep a record of the address of the beneficiary for such transfers has been removed from the amendments to the Regulations. Many sectors have expressed their concerns regarding the amount of information that would have to be collected on partnerships and other entities if the published amendments were to come into force. To reduce this compliance burden, the amendments to the Regulations no longer require persons and entities to obtain information on the partners or directors of an entity other than a corporation".

[57] The amendments were enacted on 26 December 2007 and come into force in December 2008, see http://www.fin.gc.ca/news07/07-105e.html.

618. The present report takes into account (for analysis and rating purposes) the amended version of the PCMLTFA dated February 10, 2007. The report also takes into account (for analysis and rating purposes) the provisions of the PCMLTF Regulations that have been in force since June 30, 2007 (*i.e.* in relation to correspondent banking relationships, shell banks and a broader set of information released in FINTRAC disclosures). However, the provisions of the PCMLTF Regulations and the PCMLTF Suspicious Transaction Reporting Regulations also published on June 27, 2007 that will enter into force on June 23, 2008 (such as information to collect on beneficiaries and the politically exposed foreign person's related requirements) have not been analysed by the assessors. However, the existence of such provisions has been taken into account when drafting the recommendations given to Canada to improve its AML/CFT regime. Annex 1 of the report provides an inventory of the changes brought to the Canadian AML/CFT regime since December 2006.

Enforceability of AML provisions issued by competent authorities

619. There are 14 legislative bodies in Canada: the Parliament of Canada, and the legislatures of 10 provinces and three territories. Statutes enacted by these legislative bodies are primary legislation. Regulations are made under a statute or an Act by the government department or ministry administering that Act (see Part IV of the PCMLTFA) and are another form of law. This is the generally-recognized hierarchy of authority: the Constitution, human rights legislation, other legislation, regulations, case law from higher courts, other case law, treaties/international law and doctrine.

620. FINTRAC (for all reporting parties), OSFI (for Federally Regulated Financial Institutions) and IDA (for securities dealers) have developed guidelines to assist reporting entities understanding their obligations under the Act and associated regulations. During consultations on the proposed Regulations, stakeholder groups have identified the need for guidelines to assist persons and entities understanding their obligations under upcoming regulatory changes.

621. Repeated reference is made in this section of the report to various types of guidance issued by regulatory agencies with respect to the financial sector's AML/CFT obligations and the regulators' approach to compliance. The extent to which such guidance can be deemed to be "other enforceable means" is central to the evaluation of the financial sector preventive measures and the following summary reflects the view taken by assessors on the main forms of guidance.

622. Within the FATF, "other enforceable means" refers to guidelines, instructions or other documents or mechanisms that set out enforceable requirements with sanctions for non-compliance, and which are issued by a competent authority (*e.g.* a financial supervisory authority) or an SRO. The sanctions for non-compliance should be "effective, proportionate and dissuasive".

OSFI guidance

623. In relation to AML/CFT issues, OSFI has issued two pieces of guidance. Firstly, there is the Guideline E-13 entitled "Legislative Compliance Management", dated March 2003, which is a general guideline on managing regulatory risk that "*conveys OSFI's expectations of federally regulated financial institutions regarding controls through which they manage regulatory risk inherent in their activities worldwide"*. Second, there is Guideline B-8 entitled "Deterring and Detecting Money Laundering and Terrorist Financing", published originally in April 2003 and amended in November 2004 after publication of the Basel Committee paper "Consolidated KYC Risk Management". B-8 is applicable to domestic and foreign banks, trust & loan companies and life insurance companies, referred to collectively as federally-regulated financial institutions (FRFIs) although the text focuses more on banking related matters. OSFI advised the assessors that B-8 is scheduled for update and amendment after the introduction of the new regulations.

624. Based on the definition of "other enforceable means", the assessors have given consideration to a number of basic requirements when considering whether OSFI Guideline B-8 can be considered as "other enforceable means". These requirements are as follows:

1) *A document or mechanism that sets out enforceable requirements addressing the issues in the FATF Recommendations.* Guideline B-8 only addresses a very limited range of AML/CFT issues (essentially Recommendation 15 and to a lesser extent Recommendations 5, 6, 9, 22, 18 and 29). In relation to customer identification for instance, the Guidance essentially addresses some enhanced due diligence situations and suggests that beneficial ownership identification is particularly important. The most comprehensive part of the guideline deals with internal control procedures to prevent ML and TF (role and position of the CAMLO, oversight by the Board, compliance reporting processes, self-assessment program, independent procedures testing, etc.) in relation to Recommendation 15. Finally, the Guideline refers FRFIs to the website of FATF, FINTRAC and BIS and encourages them to familiarise themselves with the various standards contained therein. Looking at whether OSFI Guideline B-8 sets out enforceable means, the assessment team has considered:

   - *The nature of the document*: OSFI itself defines the guidelines it publishes (see OSFI website) as "*essentially best or prudent practices that it expects financial institutions to follow. Guidelines are used to set standards to govern industry activities and behaviour*". OSFI has indicated that its guidelines aim at *promoting* the adoption of policies and procedures designed to control and manage risk. Based on these clarifications and looking at the current form of such guidelines, they appear to be more similar to general advice than mandatory obligations and there is no contrary indication that the guidelines place mandatory obligations on FRFIs.
   - *The language of the document*: OSFI has intentionally opted for a gradation of the language in the B-8 Guidance (from FRFIs "must" to FRFIs "should consider" or FRFIs "are encouraged". Except on four occasions where the wording of the guidance is assertive (using a "must"[58]) the guidelines are generally worded in a permissive manner (FRFIs "should" do or "should consider"; OSFI "encourages", OSFI "recommends", OSFI "suggests") which do not adequately substantiate OSFI's expectations of FRFIs and leaves a great deal of discretion in the hands of the FRFIs. So, even if OSFI addresses the FRFIs' compliance with the Guideline in its regular on-site assessments, it is not clear which provisions of these guidelines could be considered as "requirements", most of them being "recommendations" or "best practice".

2) *The document/mechanism must be issued by a competent authority (e.g. a financial supervisory authority) or an SRO.* OSFI regulates and supervises federally regulated financial institutions and administers financial institution governing statutes. As a financial supervisory body, it is a competent authority.

3) *There are sanctions for non-compliance, which should be effective, proportionate and dissuasive and there is evidence that effective and dissuasive sanctions have been applied in practice.* When reviewing the compliance of FRFIs with the AML/CFT regime, OSFI explicitly includes in its scope and objectives the assessment of compliance with OSFI Guideline B-8. Sanctions are available to OSFI based on a failure of the financial institution to conduct its business in a safe and sound manner in relation to AML/CFT failings and OSFI Guidelines are enforceable to ensure "safety and soundness" within a financial institution. To encourage financial institutions to implement the AML/CFT provisions (including OSFI Guidance), OSFI's related supervisory powers are very much focused on early intervention

[58] 1. "*To identify their level of exposure to potential MLTFA and the associated risks, FRFIs must understand the nature of the risks associated with the different parts of their operations*"; 2. "*With respect to introduced business, FRFIs must obtain the necessary customer information for their records prior to, at, or at a reasonable time after, the time that the business is accepted*"; 3. "*The board of directors and senior management must be strongly committed to ensuring that measures designed to address risks associated with these activities (that are risky) are implemented*" and 4. "*Front-line staff plays an essential role in implementing anti- MLTFA measures and, therefore, must receive appropriate training to understand problems associated with MLTFA, the financial institution's anti- MLTFA policies, and the proper application of procedures*".

and OSFI strongly relies on a remedial program through the normal supervisory process to address compliance failures.

- *Applicable sanctions*. OSFI has a range of supervisory tools and sanctions at its disposal, including written interventions, staging, directions of compliance, placing terms and conditions in the FRFI's Order To Commence And Carry On Business (operating licence) and imposing an Administrative Monetary Penalties (AMP) under the OSFI Act.

- *Sanctions that have been applied*:

  (a) OSFI issues supervisory letters after each AML/CFT assessment. The letters contain "required actions" on compliance issues or "recommendations". In most cases, interventions in the form of "recommended action" (vs. "required action") have been applied for failing to implement OSFI Guidance B-8 as a result of OSFI inspections. OSFI issues "Recommended actions" to address deficiencies in risk management controls or *other supervisory requirement not directly related to a legal requirement*. However, when OSFI feels it necessary to deliver a stronger signal to the financial institution, they may use the term "require" as more prescriptive language when dealing with deficiencies under B-8. This may be because the lack of compliance with the B-8 provision resulted in a markedly weaker AML program overall. So, for example, OSFI will sometimes say they "require" a self-assessment and at other times "recommend" it. OSFI claims that there is indeed no procedural difference applied to the terms "requirement" and "recommendation" and that FRFIs work to quickly implement the necessary changes, whether required or recommended.

  (b) Beyond the supervisory letters, OSFI has a range of supervisory tools (including sanctions) at its disposal. Staging is a supervisory measure implemented by the Supervisory Sector of OSFI based on its overall view of the level of risk in the FRFI balanced against the effectiveness of the risk controls. It results in progressively more and more intense oversight and detailed intervention by OSFI on the issues that led to the Staging. It also results indirectly in a financial charge to the staged deposit-taking financial institutions as it attracts a higher OSFI assessment fee and may attract a higher deposit premium by CDIC. Cumulatively, in the period 2004-2006 inclusive, OSFI staged 4 financial institutions for AML/CFT control deficiencies (2 of them on this sole basis). The AML/CFT deficiencies giving rise to the staging were a mixture of regulatory non-compliance and non-compliance with B-8 requirements. The amount of OSFI and CDIC surcharges ranged from CAD 45 000 up to CAD 500 000.

  (c) Supervisory tools such as direction of compliance or prudential agreements (see Section 3.10 for further details) are available but have never been used for a failure to implement OSFI Guidance or even for any AML deficiencies. OSFI considers that such actions have never been necessary, as weaknesses have always been adequately addressed with measures taken under (a) and (b) above.

  (d) OSFI can issue Administrative Monetary Penalties (AMPs) but these penalties only apply in case of a contravention of a provision of a financial institutions Act (such as the Bank Act) or of a direction of compliance, terms and conditions or a prudential agreement (see OSFI ACT, art. 25). They cannot be administered directly in case of non-compliance with the PCMLTFA, its regulations or a fortiori OSFI Guidance.

625. In conclusion, sanctions for non-application of OSFI Guideline B-8 do not appear to be sufficiently effective, proportionate and dissuasive. OSFI essentially use written recommendations as a main supervisory tool and in some limited occasions, closer monitoring (only staging (to stage 1) was used in a limited number of cases although very serious deficiencies were identified in a number of assessments). These supervisory tools have been the only ones that OSFI has used so far for failure to implement Guideline B-8. Looking at the language of the guidelines and the sanctions that have been applied by OSFI, the assessors' believe that OSFI Guidelines cannot be considered as "other enforceable means".

IDA guidance

626. The IDA is the national self-regulatory organisation of the securities industry in Canada and regulates the activities of investment dealers in terms of both their capital adequacy and conduct of business. The IDA is the front-line regulator of full securities dealers. A number of provisions in provincial securities regulations recognize IDA rules as an alternative to provincial regulations, generally by explicitly granting or allowing the granting of exemptions from the provincial rules to members who abide by IDA rules.

627. The IDA regularly publishes By-laws, Regulations and Policies that set out detailed requirements to be implemented by its members in carrying out their business (such as opening account rules, recordkeeping requirements, etc. that are applicable in the AML/CFT context). IDA By-laws, Regulations and Policies use prescriptive language (securities dealers "must" do). Penalties for breaches of the By-laws, Policies and Regulations include a wide range of sanctions for registered employees and member firms and have been used by IDA in the past (see section 3.10 of the report). The assessors took the view that IDA By-laws, Policies and Regulations are legally enforceable and can be considered as "other enforceable means".

628. In the AML area more specifically, the IDA published "*Deterring ML activity, A Guide for Investment Dealers*" in October 2002. This Guide is intended to highlight the key elements for a Canadian investment dealer to consider in developing an effective AML program. The language of the document clearly states that securities dealers are encouraged to take certain AML/CFT measures. There is no sanction directly applicable for a failure to comply with an AML/CFT measures contained in the Guide. For the purpose of this report, this Guide is considered as non-binding guidance which is neither law, regulation nor other enforceable means as defined by the FATF.

FINTRAC guidance

629. Under the PCMLTFA (Section 40(e)), FINTRAC has responsibility for ensuring compliance, reporting, record-keeping and client identification requirements of the reporting parties. FINTRAC has therefore developed a series of guidelines defined by FINTRAC as "'helpful hints"[59] that do not remove the responsibility for reporting entities to be familiar with or comply with the PCMLTFA and related Regulations. Such guidelines have therefore been developed by a competent authority that deals with AML/CFT issues. The language of the FINTRAC Guidance is direct, forceful and explicit with clear direction and requirements and points out how criminal sanctions exist to tackle breaches on record-keeping requirements set out by the PCMLTFA and the PCMLTF Regulations. However, FINTRAC Guidelines in themselves do not impose any mandatory requirements with sanctions for non-compliance, and indeed state in the preamble to each guidance note that "*it is provided as general*

[59] The list of FINTRAC Guidance is as follows (as of June 2007): 2 – Suspicious transactions; 3A – Submitting Suspicious transactions Reports to FINTRAC Electronically; 3B - Submitting Suspicious transactions Reports to FINTRAC By Paper; 4 - Implementation of a Compliance regime; 5 -Submitting Terrorist property Reports; 6-Record keeping and Client Identification; 7A – Submitting Large Cash Transaction Reports to FINTRAC Electronically; 7B - Submitting Large Cash Transaction Reports to FINTRAC By Paper; 8A – Submitting Non-SWIFT Electronic Funds Transfers Reports to FINTRAC Electronically; 8B - Submitting SWIFT Electronic Funds Transfers Reports to FINTRAC Electronically; 8C - Submitting Non-SWIFT Electronic Funds Transfers Reports to FINTRAC By Paper and 9 – Alternative to Large Cash Transaction Reports to FINTRAC.

information only. It is not legal advice and is not intended to replace the Act and Regulations". Furthermore, under the PCMLTFA, FINTRAC cannot impose penalties or sanctions but only has the option of referring cases to law enforcement (see Section 3.10). For the purposes of this report, the requirements of such Guidelines cannot be considered as "other enforceable means".

3.1 Risk of money laundering or terrorist financing (R.5 – 8)

Application of AML/CFT obligations to certain sectors

630. As described in the FATF Recommendations, a country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is a low or little risk of ML or TF in a given business sector. The country may decide the extent to which certain measures need to be applied on a systemic basis by each general category of financial institution, as well as by various subsets within each industry.

631. In Canada, certain financial institutions that undertake financial activities, as defined by the FATF Recommendations are not currently covered by the AML/CFT regime. These sectors or activities[60] are as follows (excluding entities that are caught because they also engage in financial activities under the regime): financial leasing; factoring; finance companies (*i.e.* entities specialized in consumer lending, credit cards, equipment financing and small business loans that are not loan companies); providers of e-money; Internet payment providers[61]; and cheque cashiers[62] when only cashing cheques issued to denominated persons[63]. Canada considers that these entities pose little or no threat of money laundering/terrorist financing. It is worth noting that these different activities represent a not insignificant part of the financial sector: for instance, the three finance companies that are members of the ACFC (Association of Canadian Financial Corporations) serve 1.74 million customers and have CAD 8 billion in assets. This is still smaller than the banking sector which has 1.5 trillion in assets.

632. Canada's AML/CFT risk-based approach was described to the assessment team as follows[64]: the starting point is that government first looks at ML/FT risks to determine whether particular parts of the financial sector should be covered by AML/CFT legislation. Based on that risk assessment, decisions are then made to regulate or not that sector for AML/CFT purposes. Canada indicated that this general approach has applied with the exception of finance companies which approached the Department of Finance in 2001 to clarify that their risk of AML/CFT was low and they should not be caught by the regime. Based on this, a decision was made not to regulate the sector but subsequent voluntary reporting of suspicious transactions has resulted in that sector remaining under monitoring by competent authorities in order to ensure that emerging risks are addressed if necessary.

633. When considering in more details the process that takes place to assess ML/TF risks, the assessment team was told that risk assessments are presented and discussed at meetings involving relevant departments and agencies, including the RCMP, the Department of Justice and FINTRAC. The assessment team was advised that the Department of Finance looks at the sector structure (types

60 That came to the knowledge of the assessors.

61 Internet payment and e-money providers are only subject to the Act if they also offer funds remittance or transmission services and, as such, would be considered money services businesses.

62 Cheque cashing businesses that also offer money remittance services are included in the definition of MSBs under the PCMLTFA and are therefore subject to the requirements of the PCMLTFA.

63 Credit card issuers are covered by the AML/CFT regime. The assessment team was advised that VISA, Mastercard and American Express are the only general purpose credit cards available in Canada. As a result of VISA and Mastercard internal rules, credit cards are only issued by regulated and supervised financial institutions, both for PCMLTFA and prudential purposes. Finance companies that are not caught under the PCMLTFA can also issue general purpose credit cards (in addition to stored value cards) but do so through subsidiaries that are regulated for AML/CFT and prudential purposes.

64 At the different stages of the evaluation process, the assessment team was provided with varying descriptions of processes in place in Canada to assess ML/TF risks. Some information in that Section was provided in January 2008.

of products and clients involved, etc.) and takes into consideration risk analysis carried out at national and international level. However, no formal minutes or documentation were kept in respect of the decisions to regulate or not a given sector for AML/CFT purposes and consequently the risk assessments underlying the decisions, if any, could not be obtained by the assessment team. Limited documentation was provided for a risk assessment conducted on financial leasing (see below). The following paragraph illustrates how sectors were not included within the coverage of the PCMLTFA.

634. Importantly, Canada subsequently clarified that its risk based approach is centred around the principle that financial sectors will be brought into the AML/CFT regime only if there is a proven risk of ML/TF.

635. Canada's approach to risk is not in line with the FATF approach to risk as defined in the Methodology where a list of activities and operations must be covered by the AML/CFT regime unless there is a proven low risk of ML of TF. Canada has taken the opposite approach to extend coverage of the PCMLTFA only to activities for which there is a proven ML/TF risk. This approach is even more problematic since the risk assessment process carried out by Canada to reach conclusions on the exposure of certain sectors to ML/TF risks is either non-existent or very fragmented and ad-hoc. In the cases where such a process has taken place, the risk assessment has provided clear indicators that certain sectors were at risk (based in particular on studies carried out by the RCMP). Despite this, the decision has been taken not to cover these sectors from the AML/CFT framework (this is the case for financial leasing, stored value cards and white label ABMs – see Section 4.4 of the report). In other scenarios, no proper risk analysis has been carried out or at least there is no evidence that such analysis has taken place. However, based on the general assumption that these sectors present low ML/TF risks or that ML or TF activities can be prevented and detected in these sectors through other entities subject to the PCMLTFA, the decision has been taken not to bring them under the PCMLTFA coverage (this applies to finance companies, factoring, cheque cashiers, Internet payment and e-money providers).

636. A clear example of the approach taken is provided by the financial leasing sector, as a distinct activity, "due to the relatively low money laundering and terrorist risks involved". The assessors were referred to a study undertaken by the Department of Finance ("Financial leasing industry in Canada and ML") but this was only an undated discussion draft. This paper clearly identifies the risks attached to financial leasing activities and suggests some options to regulate the sector to address its vulnerabilities vis-à-vis ML (such as amending the criminal code). The paper concludes that further consultation is necessary before taking a decision to regulate the sector for AML/CFT purposes. However, no further action has been taken by competent authorities to follow-up the conclusions of the report and at the time of the on-site visit, no further steps had been taken to include the financial leasing sector in the scope of the Act despite the demonstrated risk of money laundering (as underlined in the paper) attached to this sector.

637. Finance companies have not been subject to any risk assessment and, as a sector, they remain unregulated. There is the perception that since they do not take deposits, they are not in a position to launder money when in fact, sub-prime lending offers many opportunities through taking out loans and then using illegal funds for repayment. It is worth mentioning that three big finance companies have formed a professional association (ACFC, Association of Canadian Financial Corporations) and decided to implement AML/CFT standards on a voluntary basis; they also regularly send voluntary STRs to FINTRAC.

638. According to another undated document entitled "Risk Assessment Issues" (presented more as a policy paper) received post evaluation in response to assessors' requests for additional information on risk assessments, certain areas such as factoring, stored value cards or e-money, Internet payment providers and financial leasing are either under consideration or have been assessed as low risk. However, the document did not fully address assessors' request to see the risk assessment itself.

639. In general, the assessors believe that the justifications underlying decisions to exclude certain categories of financial institutions or activities from the AML/CFT regime are either insufficient or non-existent and that the approach applied by Canada to do so is the opposite of the agreed approach by the FATF in the 40 Recommendations.

640. Canada should rely on a more comprehensive, thorough and formal risk assessment process. This should typically involve meetings and discussions with any relevant AML/CFT stakeholders (Department of Finance, FINTRAC, OSFI, RCMP, Department of Justice, etc.) as it is already the case but also representatives of different sectors of each industry and with their trade associations; a review of money laundering investigations, prosecutions, and convictions in each industry and consideration of law enforcement views; and consideration of international standards (including those of the FATF). Most importantly, the underlying principle should be that the financial activities referred to in the FATF standards should be covered unless there is a proven low risk of ML/TF.

Risk-based approach taken by financial institutions

641. Canada uses a risk-based approach throughout its financial sector AML/CFT regulations. The regulations identify lower risk sectors, products and customers (in close co-operation with the private sector) and determine the related measures that should be in place. The government has defined a common standard for most situations and allows reduced measures in certain specific lower-risk situations.

Use of a Risk-Based Approach in Supervision of Compliance by Competent Authorities

642. The competent authorities use a risk-based approach when supervising reporting entities for compliance with the legislation. FINTRAC and OSFI have taken a risk-based approach in developing and implementing their supervisory programs.

643. Under the PCMLTFA, FINTRAC is responsible for ensuring compliance with the PCMLTFA and its Regulations. The legislation permits FINTRAC to enter into agreements with regulators that supervise reporting entities. While FINTRAC does not devolve its responsibility for ensuring compliance to these regulators, it assesses the risks related to the regulator's supervisory activities and plans accordingly. For instance, FINTRAC may target relatively fewer compliance resources to a particular sector, such as federally regulated financial institutions, where a MOU with OSFI is in place.

644. When assessing the level of risk for reporting entities, FINTRAC looks at a range of factors, including such elements as open source information, reporting volumes, observations gleaned from outreach activities, voluntary information FINTRAC has received on non-compliance, results of compliance questionnaires completed by reporting entities, other database checks, information from regulators, quality and quantity assurance reviews, and the results of compliance examinations.

645. OSFI's supervisory powers are established through the OSFI Act. These set out the framework and limitations within which federally regulated financial institutions can operate in Canada. Within this framework, OSFI uses a risk-based approach to supervision to effectively allocate staff and resources, as well as to allow for private sector development and innovation. Under its supervisory framework, OSFI applies more supervisory resources when a financial institution's risk profile increases – when, for instance, the institution takes on new types of business or faces risks to its solvency.

646. OSFI uses a number of factors to determine the prioritization of AML/CFT assessments. These factors include: the size of the financial institution; the number of branches in Canada and the number of subsidiaries and branches outside Canada; the product mix and client base of each institution; and OSFI's overall view of the institution's compliance and risk management structure.

Scope of the PCMLTFA

647. Article 5 of the PCMLTFA defines the persons and entities to which the Act applies. The Act lists on the one hand, specific categories of entities regulated by federal or provincial acts and, on the other hand, persons or entities engaged in some specific businesses, professions or activities explicitly referred to in the text or further specified in the regulations. The list of persons or entities is as follows:

- Authorised foreign banks within the meaning of section 2 of the Bank Act in respect of their business in Canada, or banks to which that Act applies.
- Cooperative credit societies, savings and credit unions and *caisses populaires* regulated by a provincial Act and associations regulated by the Cooperative Credit Associations Act.
- Life companies or foreign life companies to which the Insurance Companies Act applies or life insurance companies regulated by a provincial Act.
- Companies to which the Trust and Loan Companies Act applies.
- Trust companies regulated by a provincial Act.
- Loan companies regulated by a provincial Act.
- Persons and entities authorised under provincial legislation to engage in the business of dealing in securities or to provide portfolio management or investment counselling services.
- Persons and entities engaged in the business of foreign exchange dealing.
- Life insurance agents and brokers.
- Persons or entities engaged in the business of "remitting or transmitting funds by any means or through any person, entity or electronic funds transfer network or issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments" (namely money services businesses).
- Departments and agents of Her Majesty in right of Canada or of a province when it accepts deposit liabilities or sells or redeems money orders in the course of providing financial services to the public).

3.2 Customer due diligence, including enhanced or reduced measures (R.5-8)

3.2.1 Description and Analysis

Recommendation 5

648. Customer's identification measures in Canada are currently insufficient to meet the FATF standards[65]. The assessors believe that the current practice, in the bigger financial groups at least, may show better results and be *de facto* closer to the international AML/CFT requirements.

Anonymous and numbered accounts

649. There is no direct prohibition on opening anonymous accounts but basic CDD exists where financial institutions have been required since 1993 to obtain information on and ascertain the identity of all new account holders[66]. The assessment team was told that neither OSFI/FINTRAC nor law enforcement authorities in the course of an investigation have ever found an instance of a financial institution operating an anonymous account.

650. Numbered accounts are permissible. This would be the case for instance for corporate acquisitions where the premature circulation of information could jeopardize the transaction. In this case, the ordinary records of this account may only have a number with no name attached. However, even in those circumstances, Canada has informed the assessors that someone in the financial institution has to ascertain the existence of the corporation that is the account holder, and be able to link this account with the actual account holder. The compliance officer has in principle complete access to the customer's information. However, there are no detailed rules or guidance on how such

[65] The substantial compliance with Recommendation 5 should improve as the new regulations that Canada enacted on June, 27 2007 come into force on June, 23 2008.

[66] Under Section 9.2 of the PCMLTFA, financial institutions cannot open an account when the customer's identity has not been obtained. This provision will come in force in June 2008.

accounts should be managed by the financial institutions. The obligation for compliance officers to have access to CDD information is not clearly stated either.

651. In the securities area, certain firms may permit confidential accounts for appropriate reasons, such as a client's prominence or due to concerns for personal safety. The IDA Guidance on Deterring ML sets out that sufficient documentation identifying the underlying owners should be obtained and on file with the firm and available to appropriate compliance staff.

Account opening and CDD

652. *General*. The PCMLTF Regulations establish the circumstances where customer identification is required. Section 53 requires financial institutions to ascertain the identity of any individual in respect of whom they have to keep a large cash transaction record (for cash transactions of CAD 10 000 or more) at the time of the transaction. FINTRAC has developed guidance in relation to client identification for the following financial sectors: financial entities, MSBs, securities dealers, life insurance companies, brokers and agents and foreign exchange dealers. As far as customer identification requirements are concerned, FINTRAC guidelines expand very little on the provisions set out in the PCMLTFA and related regulations.

653. *Financial entities*[67]. Financial entities, as the backbone of the industry, have additional client identification requirements (Section 54 of the PCMLTF Regulations and FINTRAC Guideline 6G "*Record Keeping and Client Identification for Financial Entities*") in certain circumstances, namely:

- Signature cards[68]: the institution must identify any individual who signs a signature card. In cases where a business account which has more than three individuals authorised for it, the institution must identify at least three of the individuals.
- Where the account holder is an entity, the financial institution must, in addition to identifying the persons authorised to act with respect of the account, confirm the existence of the entity[69] and, in the case of a corporation, ascertain the name and address of the corporation and the names of its directors.
- Foreign currency exchange transactions in which an individual conducts a foreign currency exchange transaction of CAD 3 000 or more at the time of the transaction.
- electronic funds transfers[70] of CAD 3 000 or more.

654. *Trust companies*. Trust companies must identify any person who is the settlor of a personal trust (other than a trust created by a will) or who is authorised to act as a co-trustee of any trust (Section 55 of the PCMLTF Regulations). Trust companies must also confirm the existence of any entity (for corporations the name and address must also be ascertained) that is the settlor of an institutional trust. The existence of an entity that is authorised to act as the co-trustee of any trust and, in the case of a corporation, its name and address must be ascertained as well as all persons (up to three) who are authorised to give instructions with respect to the entity's activities as co-trustee.

655. *Life insurance companies, agents or brokers*. Life insurance companies, agents or brokers who receive CAD 10 000 or more for an annuity or life insurance policy over the duration of the product, must keep a client identification record (Section 56 of the PCMLTF Regulations and FINTRAC

---

67 In the PCMLTF Regulations,: "financial entities" are banks, credit unions, *caisses populaires*, trust and loan companies, agents of the Crown that accept deposit liabilities.

68 Signature card in respect of an account means any record that is signed by a person who is authorised to give instructions in respect of the account.

69 Entity" in the PCMLTFA means a body corporate, a trust, a partnership, a fund or an unincorporated association or organisation.

70 "Electronic funds transfer" means the transmission – through any electronic, magnetic, or optical device, telephone instrument or computer – of instructions for the transfer of funds, other than the transfer of funds within Canada. In the case of SWIFT messages, only SWIFT MT 100 and SWIFT MT 103 messages are included".

Guideline 6A "*Record Keeping and Client Identification for Financial Entities*"). When the transaction referred to above is conducted on behalf of an entity, the insurance company, broker and agent must also confirm the existence of every entity, and if such entity is a corporation ascertain its name and address, and the names of the corporation's directors within 6 months of creating this record[71].

656. *Securities dealers*. Securities dealers have to identify any individual who is authorised to give instructions for any account the dealer has to maintain a record for. In the case of a business account, the securities dealer does not have to identify more than three individuals who are authorised to give instructions for an account (Section 57 of the PCMLTF Regulations and FINTRAC Guideline 6E "*Record Keeping and Client Identification for Financial Entities*"). In addition, where the account is opened in the name of an entity, the securities dealer must confirm its existence and, in the case of a corporation, ascertain the name and address of the account holder and the name of its directors.

657. The identification procedures of securities firms start with the basic KYC requirements mandated by the PCMLTF Regulations. IDA Regulations, Policies and By-Laws add further requirements. IDA Policy 2 ("*Minimum Standards for Retail Account Supervision*") sets out precise requirements for opening new accounts. To comply with the "Know-Your-Client" rule each IDA Member must establish procedures to maintain accurate and complete information on each client. The first step towards compliance with this rule is completing proper documentation when opening new accounts. The IDA has elaborated a "*New Client Application Form*" that sets out the type of information that has to be obtained when opening new accounts. This includes, in particular, client's name, address and date of birth, client's social insurance number, client's occupation, client's employer details and insider information.

658. *MSBs*. In addition to remittance or transmission of CAD 3 000 or more by any means through any person, entity or electronic funds transfers network, MSBs are required to keep client information records if they have an on-going business relationship with a client and for the issuance or redemption of money orders, traveller's cheques or other similar negotiable instruments in excess of CAD 3 000 (Section 59 of the PCMLTF Regulations and FINTRAC Guideline 6C "*Record Keeping and Client Identification for MSBs*"). The money services business must confirm the existence of any entity for which it is required to keep client information record (for the purpose of an ongoing relationship). In the case of a corporation, the MSB must also ascertain the corporation's name and address and the names of its directors within this timeframe (see comments under "*timing of verification*").

659. The current requirements are insufficient to meet the FATF standards that identify the circumstances where financial institutions have to perform customer identification (criterion 5.2 of the Methodology). There is no requirement to carry out CDD measures when there is a suspicion of ML or TF or when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data[72]. Financial entities only identify customers when carrying out occasional transactions that are cross-border wire transfers and above CAD 3 000[73]. This threshold is currently too high. With regard to the identification of domestic wire transfers, the assessors were advised that the competent authorities' interpretation of the provision "the remittance or transmission of CAD 3 000 or more by any means through any person, entity or electronic funds transfers network" is that the list of persons, entities and electronic funds transfers networks are part of a non-exhaustive list of illustrations of what can constitute the "any means" by which a transaction can be carried out and that gives rise to identification obligations. In their view, the expression "any means" would therefore include any type of electronic transfer funds system or network, be it domestic or international. The assessors' view is that the language is ambiguous, that electronic funds transfers is definitionally limited to cross-border

[71] PCMLTF Regulations enacted on 27 June 2007 and coming into force in June 2008 reduce this period from 6 months to 30 days (see 64(2)(d), 65(2)(c) and 66(2)(c) of the amended PCMLTF Regulations).

[72] Regulations enacted in June 2007 and coming into force in June 2008 addresses these deficiencies.

[73] Regulations enacted in June 2007 and coming into force in June 2008 addresses these deficiencies.

wire transfers and that therefore this is not sufficient. There is no direct, clear and unambiguous identification requirement for domestic wire transfers.

660. Financial institutions have to ascertain the identity of any individual for large transactions (CAD 10 000 or more). In FINTRAC Guidance ("*Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically*"), financial institutions have to make transaction report to FINTRAC in the following situations:

- The financial institution receives an amount of CAD 10 000 or more in cash in the course of a single transaction. Or
- The financial institution receives two or more cash amounts of less than CAD 10 000 each that total CAD 10 000 or more. Entities must make a large cash transaction report if their employee or senior officer knows the transactions were made within 24 consecutive hours of each other by or on behalf of the same individual or entity.

661. The assessment team believes that the 24 consecutive hour rule impedes the application of the FATF requirement (see C.5.2b) of the Methodology) since financial institutions should be able to detect smurfing activities with no limit in time between two or more operations that appear to be linked.

662. With regard to the obligation for financial institutions to ascertain the identity of customers for occasional non-cash transactions, requirements in line with the FATF standards are set in Sections 54(1)(b) and (c), 58(1)(b) and 59(a) of the PCMLTF Regulations.

Required CDD measures

663. Sections 64, 65 and 66 of the PCMLTF Regulations describe the measures that financial institutions are required to take for ascertaining the identity of an individual, corporation and entity other than a corporation, respectively.

664. Natural persons. The PCMLTF Regulations state that the identity of a person shall be ascertained when the person is physically present "by referring to the individual's birth certificate, driver's license, provincial health insurance card, passport or other similar document." "Other similar documents" include a record of landing, permanent resident card, an old age security card, a certificate of Indian status or a card with an individual's signature and photograph on it issued by any of the following (see FINTRAC Guideline 6G):

- Insurance Corporation of British Columbia.
- Alberta Registries.
- Saskatchewan Government Insurance.
- Department of Service Nova Scotia and Municipal Relations.
- Department of Transport and Public Works of Prince Edward Island.
- Service New Brunswick.
- Department of Government Services and Lands of Newfoundland and Labrador.
- Department of Transport of North West Territories;
- Department of Community Government and Transportation of Nunavut.

665. For a document to be acceptable for identification purposes, it must be valid and have a unique identifier number. Also, the document must have been issued by a provincial, territorial or federal government in Canada, or the equivalent in a foreign jurisdiction. When a reporting entity refers to a document to identify an individual, it must be an original and not a copy. Valid foreign identification, if equivalent to an acceptable type of Canadian identification document would also be acceptable (FINTRAC Guidance 6G).

666. The extent to which photographic identification is a requirement is not clear but certain identification documents, such as birth certificates and records of landing, would not contain the

bearer's photograph[74] (which may raise potential risk especially when relying on similar documentation for foreign customers).

667. For individuals not physically present, financial institutions, with the current exception of MSBs must ascertain the identity of the individual by confirming that a cheque drawn by that individual on an account at a financial entity has been cleared (Section 64(1) of the PCMLTF Regulations). This means a cheque that was written by the individual, cashed by the payee and cleared through the individual's account. It does not include pre-authorised payments as these are not cheques written by the individual. Life insurance companies, brokers and agents, securities dealers and departments and agents of Her Majesty in right of Canada or of a province can also ascertain the identity of their client by confirming that the individual holds an account in their name with a financial entity.

668. In the PCMLTF Regulations, the two distinct requirements – identification and verification of customer's identity - are covered by the requirement to "ascertain" customer's identity. In practice, this means that financial institutions must obtain certain data to establish the identity of the customer and verify it by referring to an identification document. It is worth noting that the verification requirement is clearly articulated in the PCMLTFA (Section 6.1) since "*reporting entities shall verify the identity of any person or entity*". Canadian financial institutions are not required to necessarily retain copies of the documentation upon which reliance is placed for verification of the customer's identity on the grounds that such a practice may not respect certain provisions governing privacy and customer protection.

669. In the case of non face-to-face business, the assessors were uncomfortable with the third party cleared cheque confirmation process as it was seen as a potential loophole for illegal use. As a sole means to confirm identity in non face-to-face situations, it is unreliable[75].

670. *Corporations*. When the account is opened, the reporting entity must confirm the existence of the corporation as well as the corporation's name and address and the names of its directors (Section 65 of the PCMLTF Regulations) by referring to the following documents (FINTRAC Guidelines 6G):

- The corporation's certificate of corporate status (including the list of the corporation's directors submitted with the application for incorporation).
- A record that has to be filed annually under provincial securities legislation. Or
- Any other record that confirms the corporation's existence. Examples of these include such other records as the corporation's published annual report signed by an independent audit firm, or a letter or a notice of assessment for the corporation from a municipal, provincial, territorial or federal government.

671. The record that is used to confirm a corporation's existence can be a paper or an electronic version. An electronic version of a record has to be from a public source. If the record is in paper format, the reporting entity has to keep the record or a copy of it. If the record is an electronic version, the reporting entity has to keep a record of the corporation's registration number, the type and source of the record (Section 65(2) of the PCMLTF Regulations).

---

[74] The General Guide to Account Opening and Customer Identification issued by the Basel Committee states that natural persons should be identified using "an official personal identification number or other unique identifier contained in an unexpired official document (*e.g.* passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer".

[75] In the case of non face-to-face business, the regulations enacted in June 2007 and coming into force on June 23, 2008 strengthen Canada's non-face-to-face identification methods. In addition to the current third party cleared cheque method various acceptable combinations of identification methods are required for Canadian customers and when the client is a non-resident, face-to-face identification through an agent is required (see 64(1)(b), 64(1.1)(b), 64(1.2), 64(1.3), 64.1 and Schedule 7 of the amended PCMLTF Regulations**)**.

672. There is currently no requirement to identify through personal identification means shareholders of corporations who are beneficial owners (except for IDA supervised entities). Names of directors are obtained from the statutory returns[76].

673. *Entity other than corporation*. The existence of an entity other than a corporation (*e.g.* a partnership, an association or a trust) must be confirmed by referring to a partnership agreement, articles of association or any other similar record (which could include a declaration of trust in the case of a trust) that confirms the entity's existence. Trust companies must identify the settlor (who may be individuals, corporations or entities) and co-trustees of a trust (Section 55 of the PCMLTFA Regulations). In the context of the third party determination, Section 11 of the PCMLTF Regulations sets out the obligation to keep a record of the name, address and principal business and occupation of each of the beneficiaries that are known at the time that the trust company becomes a trustee for the trust. Section 66 of the PCMLTF Regulations sets out very general requirements to ascertain the existence of entities other than corporations and no specific documentation is required to verify the legal status of trusts.

Identification of persons acting on behalf of the customer

674. Financial entities must ascertain the identity of every person who signs a signature card in respect of an account that the financial entity opens, except in the case of a business account of which is signed by more than three persons authorised to act with respect to the account, if the financial entity has ascertained the identity of at least three of those people (Section 54(1)(a) of the PCMLTF Regulations for financial entities). Trust companies (Section 55(d)) and securities dealers (Sections 57(1) and 57(2)(a) must also identify every person – up to three – who is authorised to give instructions in respect of an account. The requirement to identify up to three persons who are allowed to give instructions in respect of an account is too restrictive since any person purporting to act on behalf of the customer should be identified and her/his authorisation to do so should be verified.

Third party determination

675. The PCMLTFA Regulations require financial institutions to determine whether their customers are acting on behalf of another person (see FINTRAC Guidelines 6A, 6C, 6E, 6G). These provisions are generally referred to as "third party determination" (Sections 8 to 11 of the PCMLTF Regulations).

676. Whenever a financial institution is required to keep a large cash transaction record (*i.e.* for cash transactions of CAD 10 000 or more), it must take reasonable measures to determine whether the individual who provides the cash is acting on the instructions of a third party. Whenever a financial institution opens an account, it must take reasonable measures to determine whether the account is to be used by or on behalf of a third party. Such measures also have to be taken by all financial institutions that are required to keep a client information record (MSBs, insurance companies, etc.).

677. Where the person or entity determines that the individual is acting on behalf of a third party, the person or entity shall keep a record that sets out (a) the third party's name and address and the nature of the principal business or occupation of the third party, if the third party is an individual; (b) if the third party is an entity, the third party's name and address and the nature of the principal business of the third party, and, if the entity is a corporation, the entity's incorporation number and its place of issue; and (c) the nature of the relationship between the third party and the individual who gives the cash or between the third party and the account holder. Where the person or entity is not able to determine whether the individual is acting on behalf of a third party but there are reasonable grounds to suspect that the individual is doing so, the person or entity shall keep a record that (a) indicates whether, according to the individual, the transaction is being conducted on behalf of a third party; and

[76] Section 11.1 of the PCMLTF Regulations enacted in June 2007 and coming into force in June 2008, requires financial institutions to take reasonable measures to obtain and keep information on the beneficial owners of corporations, including keeping a record of the name and occupation of all directors and the name, address and occupation of any person who owns or controls 25 per cent or more of the shares of the corporation.

(b) describes the reasonable grounds to suspect that the individual is acting on behalf of a third party. If an account is for or on behalf of future and unknown clients or employees of the individual or entity opening the account, the financial institution must keep a record indicating that the account is to be used by or for third parties who are not known at the time of account opening.

678. If a person is acting on behalf of a corporation, the financial institution must keep a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of the transactions or in respect of the account, as the case may be (see Sections 14(b), 20, 23(1)(b), 26(b), 30(b) of the PCMLTF Regulations).

Identification of beneficial ownership

679. *General.* Apart from the third party determination requirement, there are significant gaps in the current requirements to establishing beneficial ownership. There is only the requirement to identify the person who is acting on behalf of another person. Financial institutions (except securities dealers) are neither required to understand the ownership and control structure of the customer nor obliged to determine who are the natural persons that ultimately own or control the customer. There is no requirement to identify the beneficiaries of life insurance contracts either. OSFI Guidance B-8 states that "*the FATF recommends that financial institutions "understand the ownership and control structure" of their customers. OSFI suggests that this principle is particularly important when dealing with privately owned companies, trusts and customers that may have more complex legal structures*". OSFI Guidance therefore imposes no requirement in this area. The question was raised during meetings with the Canadian Bankers Association about the methods banks would adopt to identify the beneficial owner in a complex scenario involving corporate shareholdings and whether they would drill down until they identified a personal beneficiary. It seems that in practice there is no identification of the natural person who ultimately owns or controls a customer or exercises ultimate effective control over a legal person or arrangement[77].

680. *Securities dealers*. When opening an initial account for a corporation or similar entity, IDA Members (Regulation 1300 on "Beneficial ownership of non-individual accounts") shall: (i) ascertain the identity of any natural person who is the beneficial owner, directly or indirectly, of more than 10% of the corporation or similar entity, including the name, address, citizenship, occupation and employer of each such beneficial owner, and whether any such beneficial owner is an insider or controlling shareholder of a publicly traded corporation or similar entity; and (ii) as soon as is practicable after opening the account, and in any case no later than six months after the opening of the account, verify the identity of each individual beneficial owner identified in using such methods as enable the Member to form a reasonable belief that it knows the true identity of each individual and that are in compliance with any applicable legislation and regulations of the Government of Canada or any province (Regulation 1300). This does not apply to: (i) a corporation or similar entity that is or is an affiliate of a bank, trust or loan company, credit union, caisse populaire, insurance company, mutual fund, mutual fund management company, pension fund, securities dealer or broker, investment manager or similar financial institution subject to a satisfactory regulatory regime in the country in which it is located (ii) a corporation or similar entity whose securities are publicly traded or an affiliate thereof.

681. When opening an initial account for a trust, an IDA Member shall: (i) ascertain the identity of the settlor of the trust and, as far as is reasonable, of any known beneficiaries of more than 10% of the trust, including the name, address, citizenship, occupation and employer of each such settlor and beneficiary and whether any is an insider or controlling shareholder of a publicly traded corporation or

[77] Under Section 11.1 of the PCMLTF Regulations enacted on 27 June 2007 and entering into force in June 2008, financial institutions are required to confirm the existence of an entity and to take "reasonable measures" to obtain information on the beneficial owners. It is also necessary to keep a record of information on all directors, all partners and owners of 25% or more of the shares of an entity. In so doing, financial entities are required to obtain the name, address, date of birth and occupation of all shareholders with more than 25% holdings.

similar entity. (ii) as soon as is practicable after opening the account, and in any case no later than six months after the opening of the account, verify the identity of each individual identified in using such methods as enable the Member to form a reasonable belief that it knows the true identity of each individual and that are in compliance with any applicable legislation and regulations of the Government of Canada or any province. This does not apply to a testamentary trust or a trust whose units are publicly traded.

682. In its Notice of June 7, 2004, IDA provides further guidance to securities dealers on beneficial ownership identification. The requirement is to identify natural persons owning a greater than 10% interest in a corporation or similar entity, or that are settlors or beneficiaries of trusts. Where interests are held through other corporations or entities, Members are required to determine the identities of those individuals whose net interest in the accountholder exceeds 10%. So for example, where Corporation A holds a 50% interest in a corporate client, the Member is required to identify any natural persons beneficially owning, again directly or indirectly, more than 20% of Corporation A. The requirement is keyed on ownership interest, not on voting control. Where a corporation subject to the requirement has a complicated ownership structure, Members will have to make reasoned judgments to determine who falls within the requirements through discussions with the corporation's representatives. Members should, in compliance with their general know-your-client obligations, obtain a good understanding of the control structure of corporate and other non-individual clients and the nature of their business or other purposes. Members should view with suspicion any indications that a corporation has been structured so as to conceal its true beneficial ownership or avoid any requirement to identify beneficial owners. Any such suspicions should result in additional enquiries before a decision is made to do business with the prospective client.

683. In relation to trusts, the requirement applies for both formal and informal trusts. Some trusts are structured such that the identity of the beneficiaries and/or level of their interest is not known or is subject to alteration under specific conditions; some trusts split different types of beneficial interests, for example between income and underlying assets. A Member is expected to make enquiries sufficient to enable it to understand the nature and details of the trust, but may rely on summary representations made by the settlor or trustee or attorneys for either, without having to examine lengthy and detailed constating documents. The Member should record the essential details including any reasons for the beneficiaries being unknown.

Purpose & intended nature of the business relationship

684. There are currently no requirements to obtain information on the purpose and intended nature of the business relationship[78].

685. Certain information obtained when completing the IDA "*New Client Application Form*" (such as client's occupation, type of business, account objectives) give helpful indications on the intended nature of the business relationship. The IDA Guide on "*Deterring ML Activity*" sets out that a firm's AML program should be designed to permit the firm to make a reasonable risk-based determination as to its customers, its customers' source of income and its expected activity.

Ongoing Due Diligence

686. There are currently no requirements to conduct ongoing due diligence on the business relationship (except for IDA members) although the need to identify customers for large cash transactions and electronic fund transfers provide certain automatic trigger points. OSFI Guideline B-8 (that only sets out recommended actions) states: "*where appropriate (for example, where the volume of transactions is high), FRFIs should consider whether monitoring activity could be strengthened by information technology solutions.*" The OSFI Guideline also stipulates that "*the policies and procedures should include measures to permit FRFIs to identify and report large cash transactions*

[78] Paragraph 14(c.1) of the PCMLTF Regulations, enacted in June 2007 and coming into force in June 2008, requires financial entities to keep a record of the intended use of the account.

(…). The policies and procedures should also include measures to monitor transactions". Many banks appear to have introduced transaction monitoring systems. IDA Policy 4 ("*Minimum Standards for Institutional Account Opening, Operation and Supervision*") states that supervisory procedures and compliance monitoring procedures should be reasonably designed to detect account activity that is or may be a violation of applicable securities legislation, including transactions raising a suspicion of ML or TF activity[79].

687. Financial institutions are not required to ensure that documents, data and information collected under the CDD process are kept up-to-date and relevant[80]. However, IDA Policy 2 requires the maintenance of accurate and current documentation to ensure that all recommendations made for any account are appropriate for the client and in keeping with the client's investment objectives.

Higher risk

688. There is currently no requirement in the PCMLFT Regulations to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction[81].

689. OSFI requires FRFIs to understand the nature of the risks associated with the different parts of their operations. OSFI Guidance makes an inventory of risk categories such as products and services, customers, reliance on others and geographic consideration... Certain transactions have been prescribed as low risk which allow FRFIs some exemption from customer identification requirements. On the contrary, OSFI Guidelines suggest that *"certain customers may merit additional due diligence. Examples could include businesses that handle large amounts of cash, or that deal in luxury or high end consumer goods. Finally customers that hold important public positions (often referred to as "politically exposed persons") may require special attention."*

690. With regard to private banking, the Canadian Bankers Association believes that the form of private banking offered by Canadian banks is a lower risk business model since in their view private banking services are an extension of retail banking and brokerage services offered to primarily Canadian high net worth individuals. However, there is a clear recognition at international level that private banking services are a higher ML/TF risk category of business relationships that require enhanced scrutiny, irrespective of the nationality of the customer[82].

691. IDA Guidance ("*Deterring ML activity, a Guide for Investment Dealers*") identifies higher risk customers (such as offshore customers) and provides indicators in assessing the risk posed by particular customers or transactions (whether the customer is an individual, an intermediary, public, private, domestic or foreign corporation, a financial or non-financial institution, or a regulated person

---

79 Regulations enacted in June 2007 and coming into force in June 2008 require all reporting entities to conduct ongoing monitoring for the purpose of detecting suspicious transactions and keep client information up-to-date when a situation or client represents higher risks) (see Section 71.1 of the amended PCMLTF Regulations**).**

80 This has been addressed through December 2006 changes to the legislation and the regulations coming into force in June 2008 (see Section 71.1 of the amended PCMLTF Regulations, which must be read in conjunction with new section 9.6 of the PCMLTFA).

81 New provisions enacted in June 2007 and coming into force in June 2008 require reporting entities to have written policies and procedures to be used in assessing the risk of ML or TF and take, in the case of higher risk situations, reasonable measures to conduct ongoing monitoring, keep information up-to-date and take any other necessary measures to mitigate the risks. The new regulations include enhanced non-face-to-face methods that take into account the higher risk inherent to a non-face-to-face environment, especially when the customer is a non-resident (see Section 71, Section 71.1 and Sections 64(1)(b), 64(1.1)(b), 64(1.2), 64(1.3), 64.1 and Schedule 7 of the amended PCMLTF Regulations).

82 PCMLTF Regulations enacted on 27 June 2007 (Section 71) and coming into force in June 2008 require written policies and procedures to be used in assessing the risk of ML or TF offence under the compliance program to include, taking into consideration the type of client and the nature of the relationship between the person or entity and the client, the type of product, and the delivery channels for the product and the geographic location and any other relevant factor.

or entity; whether the customer has been an existing customer for a significant period of time; how the client became a customer of the firm; whether the business of the customer, or the particular type of account, is a type more likely to be involved in illicit activity (*e.g.* cash intensive businesses); etc.). For higher risk customers, investment dealers may carry out extra due diligence that may include credit checks, checking of outside databases through the Internet, verification of personal details and references or other more extensive background checks using external resources.

Lower risk

692. The PCMLTF Regulations provide for certain exemptions from the client identification and record-keeping requirements in certain specific circumstances of lower risk of money laundering or terrorist financing. These exemptions mean that, rather than reduced or simplified CDD measures, no CDD measures apply whatsoever for these cases, which is not in line with the FATF requirements that only permit reduced or simplified CDD in certain circumstances.

693. Sections 62 and 63 of the PCMLTF Regulations prescribe the exceptions to ascertaining identity of individuals and existence of entities. Section 9 prescribes the exceptions to third party determination. The assessment team was told that these exemptions were developed following extensive discussions between the Department of Finance, FINTRAC, the RCMP and the reporting entities. No more information was provided at the time of the on-site visit.

694. *General exemptions from CDD requirements*. The general exceptions (Section 63) are as follows:

- Once a reporting entity has ascertained the identity of an individual, it does not have to confirm their identity again if it recognizes the individual at the time of a future event that would otherwise trigger the identification requirement.
- Once a reporting entity has confirmed the existence of a corporation and confirmed its name, address and the names of its directors, it is not required to confirm that same information in the future;
- Once a reporting entity has confirmed the existence of an entity other than a corporation, it is not required to confirm that same information in the future.
- When the corporation is a securities dealer, the reporting entity is not required to ascertain the name of the directors.

695. *Specific exemption from CDD requirements*. In the insurance sector, more specific exceptions are proposed under the PCMLTF Regulations (Sections 62 & 63), again to address low risk situations, namely:

- The purchase of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation.
- The purchase of a registered annuity policy in respect of an annuity referred to in subsection (5) or a registered retirement income fund.
- The purchase of an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy.
- A transaction that is part of a reverse mortgage or of a structured settlement.
- The opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account.
- The opening of an employees profit sharing plan account or a deferred profit sharing plan account, unless the account is funded in whole or in part by contributions by a person or entity other than the employer. Or

- The opening of a dividend reinvestment plan account sponsored by a corporation for its investors, unless the account is funded in whole or in part by a source other than the corporation.

696. Financial entities, securities dealers and the insurance sector are not required to ascertain identity if:

- The person already has an account with the financial entity or the securities dealer, as the case may be. Or
- There are reasonable grounds to believe that the account holder is a public body or a corporation that has minimum net assets of CAD 75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange that is prescribed by section 3201 of the *Income Tax Regulations* and operates in a country that is a member of the Financial Action Task Force on Money Laundering (Section 62(2)(b)).

697. The second exemption raises concerns since the exemption is broad in scope (and "the reasonable grounds to believe" element introduces a weak and indefinite threshold). The assessors were told that a thorough risk assessment was conducted before deciding on this exemption. The decision was based on the fact that corporations with a minimum of CAD 75 million in net assets are already under considerable public scrutiny and regulation. There are numerous documents publicly available outlining their financial situation, ownership, structure and management. These corporations are also subject to provincial securities legislation as public issuers and are subject to sanctions if they provide false or misleading information. From the assessment team's point of view, the exemption in the securities industry to identify corporations that, among other criteria, operate in FATF countries is not satisfactory since it is only based on the principle of presumption of conformity. The assessors were told that the decision to exempt entities from FATF member countries is based on the fact that AML/CFT requirements and CDD measures in particular, can reasonably be expected to be stronger and more effective in these countries.

698. Finally, the identity requirement does not apply if the account holder or settlor is a pension fund that is regulated under an Act of Parliament or of the legislature of a province. The assessors were told that pension funds are subject to strict information disclosure requirements and to fines or imprisonment if these rules are violated. Financial entities are not required to ascertain identity in respect of (a) employees profit sharing plan accounts and deferred profit sharing plan accounts, unless the accounts are funded in whole or in part by contributions from a person or entity other than the employer; or (b) dividend reinvestment plan accounts sponsored by a corporation for its investors, unless the accounts are funded in whole or in part from a source other than the corporation. These plans are considered to be lower risk because they do not provide the opportunity for the members to place additional funds in the plan beyond small payroll deductions prescribed under the plan[83].

699. *Exemptions from third party determination*. The third party determination provision does not apply in respect of an account where the account holder is a financial entity or a securities dealer engaged in the business of dealing in securities in Canada. Also, in cases where the account holder is a person or entity engaged in the business of dealing in securities outside Canada only, securities dealers do not have to make a third party determination if any of the following conditions are met:

- The account is in a country that is a member of the FATF.
- The account is in a country that is not a member of the FATF, but, when opening the account, the security dealer gets written assurance from that account holder that the country where the account is located has implemented the FATF Recommendations concerning customer identification. Or

[83] Under regulations that have been enacted in June 2007 and come into force in June 2008, clients that want to make lump-sum payments to these plans will have to be identified in addition to the administrator of the plan (see Subsection 62(3) of the amended PCMLTF Regulations).

- The account is in a country that is not a member of the FATF and that country has not implemented the FATF recommendations concerning customer identification, but the securities dealer has ascertained the identity of all third parties relating to the account.

700. In addition, financial institutions do not have to make a third party determination for an account if the following conditions are met: (1) the account is opened by a legal counsel, an accountant or a real estate broker or sales representative; and (2) the reporting entity has reasonable grounds to believe that the account is to be used only for their clients.

701. The assessors were told that Canada has taken a risk-based approach in deciding to provide certain exemptions to third party determination. As such, all the exemptions are with respect to professionals in Canada that are subject to strict rules and codes of conduct and that are supervised by an SRO that can impose severe sanctions or, where the professional is not in Canada, is located in a FATF country or has identified its clients. The assessment team believes that despite these safeguards the exemptions to carry out third party determination bring in very far reaching exceptions that introduce potential gaps in the customer identification process and create some potential risky situations as far as ML and FT are concerned.

702. FATF Recommendations allow financial institutions to apply simplified or reduced CDD measures to customers resident in another country provided that the original country is satisfied that the other country is in compliance with and has effectively implemented the FATF Recommendations. Section 62(2)(b) and Section 9(5) as described earlier give financial institutions, in certain circumstances, the permission to exempt from CDD requirements or third party determination obligations certain customers resident in another country. However, Canada has not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations.

703. CDD or third party determination exemptions are applicable where there is a suspicion of ML or FT or specific higher risk scenarios apply. This should be corrected.

Guidelines on the risk-based approach

704. Where financial institutions are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should normally be consistent with guidelines issued by the competent authorities. At present, there are no detailed specific guidance measures that permit financial institutions to determine the extent of CDD measures on a risk sensitive basis.

705. OSFI Guideline B-8 refers institutions to the Basel Committee paper on Customer Due Diligence, issued in 2001, and encourages them to familiarise themselves with the standards outlined in the BCBS paper.

706. FINTRAC has issued a range of guidance, including “Implementation of a Compliance Regime” but this focuses primarily on the need to appoint a compliance officer, develop policies and procedures, conduct periodic reviews of policies and procedures and implement a training program. It does not specifically advise reporting entities on how to conduct a risk assessment, the risk-based approach to determination of vulnerabilities and the appropriate and proportional risk-based approaches to high-risk areas.

Timing of Verification

707. In line with the FATF requirements, financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Subsections 64(2), 65(2) and 66(2) of the PCMLTF regulations set out the requirements for ascertaining the identity of individuals, corporations and other entities as follows:

Type of transactions or reporting party in charge of verification	Timelines to carry out verification
Verification of natural person identity	
Signature of a signature card on an account managed by a financial entity	Before any transaction other than an initial deposit is carried out on an account[84]
▪ Large cash transactions of CAD 10 000 or more ▪ Electronic fund transfers of CAD 3 000 or more ▪ Foreign currency exchange transactions of CAD 3 000 or more ▪ Issuance or redemption of money orders, traveller's cheques or other similar negotiable instruments	At the time of the transaction
Trust company	Within 15 days after the trust company becomes the trustee
Life insurance company or life insurance broker or agent	Within six months after the client information record is created[85]
Securities dealers	Within six months after the account is opened[86]
Verification of corporation identity (including directors) or entity other than corporation	
Financial entities	Before any transaction other than an initial deposit is carried out on an account[87]
Trust company	Within 15 days after the trust company becomes the trustee
Life insurance company or life insurance broker or agent	Within six months after the client information record is created[88]
Foreign exchange dealing	Within six months after client information record is created
Money Services Businesses	Within six months after the client information record is created[89]
Securities dealers	Within six months after the account is opened[90]

708. The regulations establish generally acceptable timelines for ascertaining customer identity in some scenarios and especially when such verification is carried out by financial entities (for verification of identity of natural persons, corporations and entities other than corporations). However, certain serious weaknesses exist for the verification of identity carried out by some financial sectors (such as securities and insurance sectors) and/or vis-à-vis certain types of customers (such as corporations or entities other than corporations). The Canadian authorities recognise the risks involved here and the PCMLFT Regulations shorten these timelines in certain circumstances. The assessors believe that the proposed 30 day timeline for corporations' verification in the MSBs, insurance and securities sectors is too long, especially in normal business circumstances.

709. IDA Policy 2 requires IDA members to have procedures in place to ensure supporting documents are received within a reasonable period of time of opening the account. Incomplete New Client Application Form and documentation not received must be noted, filed in a pending documentation file and be reviewed on a periodic basis. Failure to obtain required documentation

[84] In June 2008 credit card issuers will have to identify clients before the card is activated (see Sections 64(2)(b.2) of the amended PCMLTF Regulations).

[85] In June 2008 this timeline will be within 30 days (see Sections 64(2)(d) of the amended PCMLTF Regulations).

[86] In June 2008, before any transaction other than an initial deposit is carried out on an account (see Section 64(2)(a) of the amended PCMLTF Regulations).

[87] In June 2008, credit card issuers must identify the account holder before any card is issued on the account (see Sections 65(2)(a.1) and 66(2)(a.1) of the amended PCMLTF Regulations).

[88] In June 2008 this timeline will be within 30 days (see Sections 65(2)(c) and 66(2)(c) of the amended PCMLTF Regulations) .

[89] In June 2008 this timeline will be within 30 days (see Sections 65(2)(c) and 66(2)(c) of the amended PCMLTF Regulations).

[90] In June 2008 this timeline will be within 30 days (see Sections 65(2)(d) and 66(2)(d) of the amended PCMLTF Regulations).

within 25 clearing days must result in positive actions being taken. The nature of the positive action must be specified in the Member's written procedures.

710. For IDA Members, verification of the identity of the beneficial owners must be completed "as soon as practicable" after account opening, and in any case no longer than six months after the account is opened. Verification procedures must begin at the time of account opening. Delaying efforts to verify the identity of beneficial owners with a view only to the six-month deadline will be viewed by the Association as non-compliance with the regulation. IDA Sales Compliance reviews will examine Members' practices to ensure that verification efforts are begun on a timely basis and are diligently pursued. In keeping with their obligations under anti-money laundering regulations, Members should consider imposing higher standards for accounts posing a higher risk of use for money laundering or other improper activity, for example requiring prior verification of the identity of beneficial owners or maintaining closer supervision of account activity until beneficial ownership has been verified.

711. OSFI has advised FRFIs that with respect to loans, including mortgage loans, there is only one "transaction", which is the disbursement of the proceeds of the loan. OSFI expects institutions to verify the identity of individuals, corporations, and entities other than corporations that open accounts for the borrowing of funds prior to the disbursement of such funds, and to refrain from disbursing such funds until such identify is satisfactorily verified.

Failure to complete CDD

712. In situations where the financial institution has already commenced a business relationship but is unable to perform adequate CDD and establish beneficial ownership, FATF Recommendations require the business relationship to be terminated and consideration given to making a suspicious transaction report. However, the current regulations, in case of failure to satisfactorily complete CDD, are not in line with the FATF standards[91] as there is no explicit requirement to close an account when a financial institution fails to properly identify a customer. However, OSFI Guideline B-8 makes reference to closing accounts, namely *"FRFIs should consider terminating relationships with introducers that cannot, or fail to, provide the FRFI with the requisite customer identification and verification data that the FRFI is required to obtain under the PCMLTFA and Regulations"*. However, as mentioned before, financial entities are generally required to identify their customers at the outset and institutions that continue to operate the business relationship without ascertaining the customer's identity are liable to criminal penalties. FINTRAC has also identified the refusal of a customer to provide information or identification as one of the suspicious transaction indicators that would merit a suspicious transaction report.

713. In IDA Regulation 1300, if securities dealers are unable to obtain the information on the beneficial owner of non-individual accounts, they shall not open the account. If an IDA Member is unable to verify the identities of individuals within six months of opening the account, the Member shall restrict the account to liquidating trades and transfers, payments or deliveries out of funds or securities only until such time as the verification is completed. Similarly, any delays in verification that appear to result from lack of client cooperation should result in a careful assessment of the circumstances. Appropriate responses could include heightened supervision of account activity, filing of suspicious transaction reports with FINTRAC and/or closing of the account.

Existing Customers

714. Financial institutions are not required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times[92].Subsection 63(1) of the PCMLTF Regulations only states that "where a person has ascertained

[91] Section 9.2 of the PCMLTFA that will enter into force in June 2008 prohibits financial institutions from opening an account when the customer's identity was not obtained.

[92] New requirements to come into force in June 2008 will apply the CDD requirements to existing customers on the basis of materiality and risk (see Section 71.1 of the amended PCMLTF Regulations**)**.

the identity of another person in accordance with section 64, the person is not required to subsequently ascertain that same identity again if they recognize that other person". The interpretation that Canada gives to that provision is that if the identity of a person was not ascertained in accordance with Section 64 (*e.g.* because they opened an account 20 years ago before CDD requirements were in place) and this person wants to open another account., this person, even though they are an existing customer, will have to be identified. The assessment team believes that this insufficiently addresses the requirement under Recommendation 5 (criterion 5.13).

Recommendation 6

715. *Legislative and regulatory requirements.* No specific legislative or other enforceable requirements in relation to PEPs are currently in force[93].

716. OSFI Guidance. The OSFI Guideline B-8 advises institutions that "certain customers may merit additional due diligence. Examples could include businesses that handle large amounts of cash, or that deal in luxury or high-end consumer goods. Finally, customers that hold important public positions (often referred to as "politically exposed persons") may require special attention". However, the guidance goes no deeper than this and banks, to a large extent, are left to decide how best to tackle the situation. The assessment team was told that OSFI has communicated its expectations to FRFIs in relation to PEPs and the need to have measures in place commensurate with the risks attached to PEPs although no binding requirement is currently in place.

717. In the insurance sector, although federally regulated life insurance companies are bound by OSFI Guidance B-8 (since the Guidance applies to all FRFIs), the CLHIA, the life insurance association, believes that Guideline B-8 is primarily intended to apply to the banking sector. As a consequence, the assessment team was advised that there is a perception that the guideline does not contain requirements that the insurance sector has to implement, for example no obligation to identify PEPs. The representatives of the association confirmed that no screening for PEPs actually takes place in the industry.

718. Discussions with the banking industry indicate that at least the larger banks have undertaken their own measures to help identify customers who may be PEPs, normally by investing in proprietary software solutions. However, this is not standard across the industry and indeed smaller banks indicated that they were not addressing the issue, largely as a result of cost factors. A similar position appears to exist for other types of financial institutions.

Recommendation 7

719. *Definition.* A correspondent banking relationship is defined in the PCMLTFA as a relationship created by an agreement or arrangement under which banks to which the Bank Act applies, cooperative credit societies, savings and credit unions and *caisses popularies*, companies to which the Trust and Loan Companies Act applies, and trust companies regulated by a provincial act or certain prescribed entities undertake to provide to a prescribed foreign entity services such as international electronic funds transfers, cash management, cheque clearing and any prescribed services.

720. *Legislative and regulatory requirements*. Canada enacted new requirements in June 2007 (that entered into force on June 30, 2007) that deal with correspondent banking related issues, and address many of the requirements of Recommendation 7. Section 9.4 (1) of the PCMLTFA came into force in June 2007 and requires every financial entity to take the following measures before entering into a correspondent banking relationship with a prescribed foreign entity: (1) obtain prescribed information about the foreign entity and its activities; (2) ensure that the foreign entity is not a shell bank as defined in the regulations; (3) obtain the approval of senior management; (4) set out in writing their

[93] New requirements in relation to PEPs that were introduced under amendments to the PCMLTFA (Section 9.3) and the PCMLTF Regulations will come into force on 23 June 2008.

obligations and those of the foreign entity in respect of the correspondent banking services; and (5) any prescribed measures.

721. New provisions in the PCMLTF Regulations in relation to correspondent banking have also been in force since June 30, 2007. These provisions require that every financial entity that enters into a correspondent banking relationship shall (Section 55 of the PCMLTF Regulations):

- Ascertain the name and address of the foreign financial institution by examining a copy of the foreign financial institution's banking licence, banking charter, authorisation or certification to operate from the relevant regulatory agency or certificate of corporate status or a copy of another similar document.
- Take reasonable measures to ascertain, based on publicly available information, whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements and, if so, to conduct, for the purpose of detecting any transactions that are required to be reported under the Act, ongoing monitoring of all transactions in the context of the correspondent banking relationship.

722. The same regulations state that every financial entity shall, when it enters into a correspondent banking relationship, keep a record in respect of the foreign financial institution containing the following information and documents (Section 15.1(2) of the PCMLTF Regulations):

- The name and address of the foreign financial institution.
- The names of the directors of the foreign financial institution.
- The primary business line of the foreign financial institution.
- A copy of the most recent annual report or audited financial statement of the foreign financial institution.
- A copy of the foreign financial institution's banking licence, banking charter, authorisation or certification to operate from the relevant regulatory agency or certificate of corporate status or a copy of another similar document.
- A copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of each entity.
- The anticipated correspondent banking account activity of the foreign financial institution, including the products or services to be used.
- A statement from the foreign financial institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks.
- A statement from the foreign financial institution that it is in compliance with anti-money laundering and anti-terrorist financing legislation in its own jurisdiction.

723. Finally, the Regulations require these types of financial institutions to take reasonable measures to ascertain whether the foreign financial institution has in place anti-money laundering and anti-terrorist financing policies and procedures, including procedures for approval for the opening of new accounts and, if not, for the purpose of detecting any transactions that are required to be reported to FINTRAC, take reasonable measures to conduct ongoing monitoring of all transactions conducted in the context of the correspondent banking relationship. All of these measures apply to all foreign financial institutions, regardless of country of origin. However, there is no requirement to assess the respondent institution's AML/CFT controls, and ascertain that they are adequate and effective. Nor are there requirements for the financial institutions to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain, based on publicly available information, whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements) or the quality of supervision of that entity.

724. *Payable through accounts*. The PCMLTF Regulations require that in situations where the customer of the respondent entity has direct access to the services provided under the correspondent banking relationship, the entity shall take reasonable measures to ascertain that:

- The respondent entity has performed the customer due diligence obligations, in accordance with the measures for ascertaining customer identity set out in the Regulations, in respect of those of its customers that have direct access to the accounts of the correspondent entity.
- The respondent entity has agreed to provide relevant customer identification data upon request to the correspondent entity.

725. The respondent entity must carry out customer identification based on the CDD requirements set out in the PCMLTF Regulations (as applicable from time to time). However the full set of CDD measures in the Regulations will not be in force until June 2008, and the current requirements are not in line with the FATF standards (see conclusions of the report in relation to Recommendation 5). Financial institutions are therefore not currently required to be satisfied that the respondent financial institutions have performed all the normal CDD obligations set out in Recommendation 5 on those of their customers that have direct access to the accounts of the correspondent financial institutions.

726. *OSFI Guidance*. Guidance to all banks and federally regulated trust & loan companies since 2002 has taken the form of a letter from OSFI, dated February 22, 2002 entitled "*Enhanced Due Diligence for Correspondent Accounts*". This letter advises recipients of the introduction of the USA PATRIOT Act and the prohibition on dealing with shell banks. The letter goes on to draw recipients' attention to the Basel Committee Paper *"Customer Due Diligence for Banks"* issued October 2001 and states, *"In light of these two initiatives, we believe that Canadian deposit taking institutions should be aware of the enhanced BIS standard for dealing with correspondent banking accounts and encourage them to adopt measures which will ensure that they do not enter into correspondent accounts with shell banks"*. There is also passing reference in OSFI Guideline B-8 about the risks involved in entering into correspondent relations with shell banks, namely; *"We draw the attention of FRFIs to the risks involved in dealing with "shell" banks…and in the light of applicable international standards, OSFI encourages all FRFIs to adopt measures which will ensure that they do not enter into correspondent relationships with shell banks"*.

727. Canada has indicated that Canadian financial institutions with correspondent banking relationships have branches or subsidiaries in the U.S. These financial institutions have applied to their Canadian operations the requirements of the 2002 US PATRIOT Act on correspondent banking relationships.

Recommendation 8

728. *Legislative and regulatory requirements.* At the time of the on-site visit, there were no specific legislative or other enforceable obligations addressing the risks posed by the application of new technological developments to the provision of financial services other than the fundamental identification requirements of each person or entity under the PCMLTFA, regardless of delivery channel.

729. Financial institutions are currently not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions[94].

730. *OSFI Guidance*. OSFI Guideline B-8 currently encourages Canadian FRFIs to implement the customer due diligence standards set out in the Customer Due Diligence for Banks paper released by the Basel's Committee in 2001 in a manner that is appropriate with the size, the complexity and the

[94] New regulations that will enter into force in June 2008 include enhanced identification measures to ascertain the identity of a client who is not physically present (see Sections 64(1)(b), 64(1.1)(b), 64(1.2) 64(1.3), 64.1 and Schedule 7 of the amended PCMLTF Regulations).

nature of the entity's activities. This paper highlights the necessity for banks to have adequate measures to mitigate higher risks, including non-face-to-face transactions or relationships. The guidelines further require these institutions to have in place a non-face-to-face identification process that is as effective as when the client is physically present. The assessors were told that in the course of its examinations of correspondent banking operations, it has never seen any direct or indirect relationship with a shell bank.

731. The assessors were advised of an emerging technology known as "white label" automated teller machines, the development of which is being monitored by the Department of Finance, together with the use of stored value cards and Internet payment providers. "White label" automated teller machines, are operated by non-financial institutions and represent approximately 60% of the total number of cash dispensers in Canada. They are generally located in non-traditional places, including supermarkets and bars. The main concern is that they can be loaded by the owner and may create opportunities to 'place' illicit cash.

732. Interac has developed limited mechanisms to prevent the misuse of these machines, such as enhancing the process for accepting new members and strengthening the regulation of owners, but concerns reflected by the RCMP suggested that bar owners or other entertainment complexes that provide heavily cash-based services could in effect recycle their own money each night, supplementing it with other illegal funds. Discussions seem to take place with Interac to enhance existing mechanisms in respect of customer due diligence and record keeping. A number of gaps in Interac's existing CDD rules have been identified (*e.g.* the acquirer, or the Interac member that ultimately provides connection for an ATM to the Interac network, has to conduct CDD on their direct business partners only (the payments processor), but are not required to perform CDD on the ATM owner if he is not a direct partner). Discussions are ongoing to determine additional measures.

733. The Department of Finance has also conducted a preliminary analysis of the AML/CFT risks of the stored value card market and intends to examine in more detail the shortfalls in the client identification practices of these vendors. The RCMP acknowledge that such gift cards represent a serious money laundering option, especially in the absence of any money laundering control at retail locations. In addition, the Department of Finance has engaged a number of Internet payment providers to discuss the AML/CFT risks and the structure of that sector. These are positive moves at the Government level but there remains nothing in force at the financial institution level that requires them to implement policies and procedures addressing new technologies when face to face identification is not possible.

734. The current CDD measures in relation to non face-to-face business are rather weak (see comments in relation to Recommendation 5 – *Required CDD measures*) since the only measure for the reporting entities is to ascertain the identity of the individual by confirming that a cheque drawn by that individual on an account at a financial entity has been cleared[95].

735. Some large financial institutions met during the on-site visit seem to apply higher internal standards in this area. However, the assessment team met with a limited sample of financial institutions and was also told that in other institutions such higher standards were not in place yet.

3.2.2 Recommendations and Comments

736. *Scope issues*. Financial leasing, factoring, finance companies (entities specialized in consumer lending, credit cards, equipment financing and small business loans); providers of e-money; Internet payment providers; cheques cashiers when only cashing cheques issued to denominated persons are not currently included in the scope of the PCMLTFA, and are thus not covered by the CDD

[95] The PCMLTF Regulations (Section 64) introduce new non-face-to-face identification methods that are applicable to any person or entity covered by the PCMLTFA and are applicable to any non-face-to-face circumstances.

requirements. This is an important omission and Canada should take steps to bring them within the CDD requirements unless it can prove, based on a formalised and thorough risk assessment analysis that these categories of institutions are of lower ML/TF risks.

737. So far, financial institutions (except the securities dealers monitored by the IDA) have received very little guidance spelling out the measures to take to implement proper AML/CFT measures. FINTRAC guidance focuses primarily on meeting record keeping and reporting requirements and is not very detailed. OSFI Guidance is also very limited since it covers a limited range of requirements. It is important for financial institutions to have detailed and comprehensive guidance at their disposal as a tool to properly and uniformly implement the AML/CFT requirements.

738. *Recommendation 5*. With regard to numbered or confidential accounts, Canada should consider adopting detailed rules or guidance on the use of such accounts by financial institutions. Such rules should clearly set out the obligation for compliance officers to have access to CDD information.

739. New provisions will come into force in 2008 with regard to the circumstances where financial institutions have to perform customer identification. Canada should ensure that the new provisions are fully in line with the FATF requirements.

740. With regard to the identification measures for natural persons, Canada should ensure that only reliable CDD documentation is acceptable, especially in non face-to-face situations. Canada should consider introducing additional requirements for identifying foreign customers.

741. New provisions will come into force in June 2008 with regard to identification of beneficial owners. Canada should ensure that the new provisions are fully in line with the FATF requirements and are properly implemented by all financial institutions.

742. The requirement to identify up to three persons who are authorised to give instructions in respect of an account should be extended to any person purporting to act on behalf of the customer.

743. The PCMLTF Regulations, enacted in June 2007 and coming into force in June 2008 require financial entities to keep a record of the intended use of the account. Canada should ensure that such requirement is implemented by all financial institutions in line with the FATF standards. Based on the provisions adopted in June 2007 and coming into force in 2008, Canada should ensure that financial institutions fully implement the obligation to conduct ongoing due diligence on the business relationship and ensure all documents, data and information collected under the CDD process in line with the FATF standards (as it is already the case for securities dealers) are kept up-to-date and relevant.

744. In relation to ML/FT risks, Canada should ensure that financial institutions perform enhanced due diligence for higher risk categories of customer, business relationship or transaction once the new regulations enter into force in June 2008. This should be done in line with the FATF standards. Current scenarios of full exemptions from CDD and third party determination should be subject to simplified or reduced CDD. Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that Canada is satisfied are in compliance with and have effectively implemented the FATF recommendations (*i.e.* Canada should not rely on presumption of conformity of FATF countries for instance). Canada should adopt explicit provisions that set out that such exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. Canada should consider developing guidelines for financial institutions that are permitted to determine the extent of the CDD measures on a risk sensitive basis.

745. With regard to the timing of customer's identity verification, new regulations that will enter into force in June 2008 should be implemented in line with the FATF standards and Canada should

consider adopting shorten timelines in the insurance, foreign exchange, MSBs and securities sectors for corporations' or entities' identification, especially in normal business circumstances.

746. *Recommendation 6.* Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.

747. *Recommendation 7.* Canada should require financial entities to assess the respondent institution's AML/CFT controls and to ascertain that these controls are adequate and effective. Institutions should also be required to further determine the reputation of the foreign financial entity and the quality of supervision of that entity.

748. In the context of payable through accounts, financial institutions should be required to be satisfied that the respondent financial institutions have performed all the normal CDD obligations set out in Recommendation 5 on those of their customers that have direct access to the accounts of the correspondent financial institutions. Canada should ensure that reporting entities implement measures that meet the FATF standards.

749. *Recommendation 8.* Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.

3.2.3 Compliance with Recommendations 5 to 8

Rec.	Rating	Summary of factors underlying ratings
Rec.5	NC	*Scope issue* • The requirement to conduct CDD does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). *Numbered accounts* • *Although numbered accounts are permissible and used, there is no direct requirement to maintain them in such a way that full compliance can be achieved with the FATF Recommendations.* *When CDD is required* • There is no requirement to carry out CDD measures when there is a suspicion of ML or TF and when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. • Customer identification for occasional transactions that are cross-border wire transfers takes place for transactions above CAD 3 000. This threshold is currently too high and no equivalent requirement is in place for domestic wire transfers. *Required CDD measures* • The current customer identification measures for natural persons are insufficient, especially in relation to non face-to-face business relationships. *Identification of persons acting on behalf of the customer* • The requirement to identify up to three persons who are allowed to give instructions in respect of an account is too limitative. *Third party determination and identification of beneficial owners* • Except for IDA supervised entities, financial institutions are neither required to understand the ownership and control structure of the customer nor obliged to determine who are the natural persons that ultimately own or control the customer. *Purpose & intended nature of the business relationship* • There are currently no requirements (except for securities dealers) to obtain information on the purpose and intended nature of the business relationship.

Rec.	Rating	Summary of factors underlying ratings
		Ongoing Due Diligence • Except for securities dealers, there are currently no requirements to conduct ongoing due diligence on the business relationship although the need to identify customers for large cash transactions and electronic fund transfers provide certain automatic trigger points. • Except for securities dealers financial institutions are not required to ensure that documents, data and information collected under the CDD process is kept up-to-date and relevant. *ML/FT risks – enhanced due diligence* • There is no requirement to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction. *ML/FT risks – reduced or simplified due diligence* • The current exemptions mean that, rather than reduced or simplified CDD measures, no CDD apply, which is not in line with the FATF standards. • Exemptions from CDD and third party determination bring in very far reaching exceptions that introduce potential gaps in the customer identification process (especially the exemptions apply to financial entities that operate in FATF countries based on presumption of conformity only). • There is no explicit provisions that set out that CDD or third party determination exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. • Financial institutions, in certain circumstances, are given the permission to exempt from CDD requirements or third party determination obligations certain customers resident in another country. However, Canada has not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations. *Timing of verification* • PCMLTF Regulations sets out unreasonable verification timelines to be carried out by certain financial sectors and/or in relation to certain customers. *Failure to satisfactorily complete CDD* • Financial institutions (except securities dealers in some circumstances) are not prevented from opening an account or commencing business relationship or performing a transaction and they are not required to make a suspicious transaction report. • In situations where the financial institution has already commenced a business relationship but is unable to perform adequate CDD and establish beneficial ownership, there is no requirement to terminate the business relationship and to consider making a suspicious transaction report.
Rec. 6	NC	• There were no mandatory legislative or other enforceable requirements in relation to PEPs at the time of the on-site visit.
Rec. 7	PC	• Financial entities are not required to assess the respondent institution's AML/CFT controls and to ascertain that these controls are adequate and effective. • Financial institutions are not required to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of AML/CFT requirements) and the quality of supervision of that entity. • In the context of payable through accounts, the respondent entity is not required to perform all the normal CDD obligations set out in Recommendation 5 on its customers that have direct access to the accounts of the correspondent institution in line with the FATF standards. • The effectiveness of the measures in place cannot yet be assessed.
Rec. 8	NC	• There are no specific legislative or other enforceable obligations. addressing the risks posed by the application of new technological developments. • Financial institutions are not required to have policies and procedures in

Rec.	Rating	Summary of factors underlying ratings
		place to address any specific risk associated with non face-to-face business relationships or transactions. • No effective CDD procedures for non face-to-face customers are in place.

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

750. *General*. The two scenarios of introduced business (where CDD is completed by someone who is neither an employee, nor a person in a contractual agency relationship) and outsourcing or agency relationships agreements (where the agent is to be regarded as synonymous with the financial institution *i.e.* the processes and documentation are those of the financial institution itself) exit in Canada. Under the Regulations, only two scenarios of introduced business are contemplated (Sections 56(2) and 57(5)). Outside these two situations, the assessment team was told that financial institutions are expected to either carry out the CDD process themselves or enter into an agency agreement with the entity authorised to act on their behalf[96].

751. *Regulatory provisions on agency relationships*. Section 6(2) of the PCMLTF Regulations addresses the issue of agency relationships. Where a person, other than a life insurance broker or agent, is an agent of or is authorised to act on behalf of another person or entity (banks, trust companies, etc.), it is that other person or entity rather than the agent or the authorised entity or person who is responsible for meeting the requirements under the PCMLTF Regulations. Based on that provision, FINTRAC and OSFI have developed further guidance, including with respect to persons or entities who may be appointed as agent but who are not subject to the regulations.

752. *Regulatory provisions on introduced business*. In the PCMLTF Regulations, only two provisions are applicable to the introduced business scenario (although in a very indirect way). Section 56(2) states that a life insurance company or life insurance broker or agent is not required to ascertain the identity of a person where there are reasonable grounds to believe that the person's identity has been ascertained by another life insurance company or life insurance broker or agent in respect of the same transaction or of a transaction that is part of a series of transactions that includes the original transaction. Section 57(5) states that a securities dealer is not required to ascertain the identity of a person who is authorised to give instructions in respect of an account that is opened for the sale of mutual funds where there are reasonable grounds to believe that the person's identity has been ascertained by another securities dealer in respect of (a) the sale of the mutual funds for which the account has been opened; or (b) a transaction that is part of a series of transactions that includes that sale. These are the only exceptions where reliance on a third party or introduced business is allowed without an agreement or arrangement (and where the outsourcing scenario applies). When these scenarios apply, there is no explicit requirement in the Regulations for financial institutions to obtain from the third party the necessary information concerning certain elements of the CDD process and satisfy themselves that copies of identification data are made available from the third party upon request without delay. The Regulations do not set out that the ultimate responsibility for customer identification and verification should remain with the financial institution relying on the third party.

753. *Existing guidance*. In FINTRAC guidance on record keeping and client identification, where reporting entities choose to rely on a third party (called "agent") to identify their customers, they should enter into a written agreement with the agent outlining what they expect the agent to do for them. The guidelines clearly states that even if reporting entities use an agent, they remain responsible for making sure the identification requirements are met. FINTRAC Interpretation Notice n°3 of January 17, 2006 sets out that all persons and entities subject to the PCMLTFA can rely on the use of the agent scenario to ascertain customer's identity; however the ultimate responsibility of ascertaining identity and making any third party determination remains with the person or entity and not their

[96] An amendment enacted in June 2007 and coming into force in June 2008 clarifies the requirements in respect of agency agreements.

agent. FINTRAC Interpretation Notices provide technical interpretation and positions regarding certain provisions contained in the PCMLTFA and related regulations.

754. OSFI Guideline B-10 ("*Outsourcing of Business Activities, Functions and Processes*") deals with outsourcing arrangements that are outside the scope of Recommendation 9. OSFI Guideline B-8 clearly refers to outsourcing record keeping or other functions (including customer identification) that form part of their obligations, or that utilize introducers to gather new business.. In this Guideline, FRFIs that outsource record keeping or other functions that form part of their PCMLTFA compliance regime, or that utilize introducers to gather new business (such as deposit brokers, mortgage brokers, correspondents, law firms, accounting firms, etc., including those outside Canada) are reminded that they retain full accountability for having customer identification and verification processes, and for obtaining customer records with respect to accounts opened through such sources. With respect to introduced business, FRFIs must obtain the necessary customer information for their records prior to, at, or at a reasonable time after, the time that the business is accepted. OSFI recommends that relationships with introducers be subject to written agreements to ensure that the responsibility for collecting and verifying customer identification information is clearly understood. FRFIs should consider terminating relationships with introducers that cannot, or fail to, provide the FRFI with the requisite customer identification and verification data that the FRFI is required to obtain under the PCMLTFA and the Regulations.

755. *Business practice*. As confirmed by the financial sector representatives during the on-site visit, introduced business mechanisms are broadly used by the industry in Canada. For instance, in practice, where banks are not able to verify the identity of a customer directly, verification is typically provided through a Canadian embassy, lawyers, and in the case of businesses, lawyers external to the business, accounting firms, referrals from another financial institution, or other types of agents for particular products or services that a financial institution provides. here is typically no formal contract between the bank and these other parties (there is no outsourcing arrangement). The banking sector believes that in some circumstances, a requirement to enter into contractual arrangements is operationally impractical, as banks would need to enter into multiple contracts with agents in every country in which clients reside or operate or in which signing officers reside or work. In this case, the introduced business scenario takes place (since financial institutions do not enter into formal outsourcing arrangements) although no measures in line with Recommendation 9 are in force.

756. In the securities sector, there are many situations in which businesses make use of agents to act on their behalf. The relationship between a dealer and individuals acting on its behalf may be a principal-agent relationship. IDA By-law 39 covers such relationships. In such cases the agent may be largely indistinguishable from an employee. By contrast, the term "introducer" has a variety of meanings in different contexts. In general, it suggests a pre-existing relationship between the introducer and the customer or prospective customer. It refers to a specific type of services relationship between dealers. IDA Members make use of accounting and law firms to conduct money laundering verification on their behalf using letters of instruction rather than contracts. For IDA, it is always essential that the terms of the relationship be clear. The principal is always responsible for the acts of its agent done within those terms and for keeping proper records of things done by the agent on its behalf.

757. Insurance companies invariably use introduced business too. In the life insurance field, independent brokers and agents are a separate reporting entity under the PCMLTFA and are permitted to identify customers under the PCMLTF regulations. The MSB sector relies largely on its own agents to promote and expand the business network and companies enter into agreements with agents as a general practice.

758. Trust companies utilise introducers to varying degrees to gather new deposit and loan business but remain well aware of their ultimate responsibility and accountability for having full customer identification and verification. Introducers fall under two categories, namely SRO and Non-SRO. Under the former category, they source new business through the IDA or the MFDA members who are

subject to the PCMLTFA. Non-SRO introducers include mortgage brokers and "Guaranteed Investment Certificate" (GIC) Agents/Brokers such as the FCIDB. Business introduced by this category is considered to have a somewhat higher risk profile relative to compliance because they are not directly subject to the PCMLTFA and therefore do not represent the same assurance of compliance. Risks are mitigated by requiring agent/broker certifications as required in signed agreements. In order for business to be accepted by trust companies, each introducer must have a signed agreement in place which specifies the customer information requirements and provides rights of audit to ensure the introducer has appropriate processes in place to meet trust company requirements.

759. *Conclusion*. Outside the very specific situations covered under Sections 56(2) and 57(5), no other introduced business scenarios are contemplated or controlled by the PCMLTF Regulations although the financial sector uses introduced business mechanisms (in addition to outsourcing or agency arrangements) as a business practice. However, no specific requirements as set out in Recommendation 9 apply to these scenarios (since Section 6(2) of the PCMLTF Regulations exclusively covers agency relationships type of arrangements that are outside the scope of Recommendation 9).

3.3.2 Recommendations and Comments

760. Since introduced business arrangements exist in Canada in other circumstances than those captured by Sections 56(2) and 57(5) of the PCMLTF Regulations, Canada should adopt provisions that address all aspects of Recommendation 9 and ensure that financial institutions implement them.

3.3.3 Compliance with Recommendation 9

Rec.	Rating	Summary of factors underlying ratings
Rec.9	NC	• In the only two scenarios where reliance on a third party or introduced business is legally allowed without an agreement or arrangement, the measures in place are insufficient to meet the FATF requirements. • In addition to the two reliance on third parties/introduced business scenarios contemplated by the Regulations, the financial sector uses introduced business mechanisms as a business practice. However, no specific requirements as set out in Recommendation 9 apply to these scenarios.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

761. *Access to information for competent authorities*. Section 8 of the Canadian Charter of Rights and Freedoms (the Charter) establishes a fundamental principle that everybody has the right to be secure against unreasonable search and seizure. This Charter protection has a direct impact on law enforcement's ability to seize information and evidence and generally, prior judicial authorisation is required before intrusions can be made upon individual privacy.

762. Section 5 of PIPEDA (which is Canada's data protection law) requires organizations to comply with specific obligations concerning the collection, use and dissemination of customers' personal information but Subsection 7(2) of PIPEDA provides that an organisation can elect to disclose personal information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed and the information is used for the purpose of investigating that contravention. Further subsections of PIPEDA allow an organisation to voluntarily disclose personal information without disclosing the fact to their customer and to comply with subpoenas, warrants and court orders to compel the production of court orders. Section 7(3)(c.1) allows organizations to disclose personal information to government institutions without the knowledge or consent of the individual and without judicial authorisation in certain specified circumstances related to law enforcement and national

security (especially the government institution must identified its lawful authority to obtain the information)[97].

763. The assessment team was told that law enforcement efforts are actually being thwarted by stringent interpretations of PIPEDA with respect to obtaining non-sensitive personal information on a voluntary basis from companies. This finding is also reflected in the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics that published a review of PIPEDA in May 2007[98]. The report mentions that in some occasions (for instance, a police officer may be in the early stages of an investigation, in which he or she is trying to determine if in fact a crime has occurred. He or she may have to solicit the assistance of a financial institution because he or she needs to know if that person used a credit card for instance and for this information he or she relies on paragraph 7(3)(c.1), which permits disclosure upon lawful authority), companies insist on seeing a court order from a law enforcement or investigative agency before disclosing any personal information pursuant to Section 7(3)(c.1). Some companies interpret "*lawful authority*" to mean that a warrant or court order is required before they comply. This interpretation may not be consistent with the intent of the drafting of the Act and seems overly restrictive. The Standing Committee agrees that there is a valid concern around what constitutes lawful authority for the purposes of disclosure under section 7(3)(c.1). The Committee agrees that clearly something other than judicial authorisation is required for the purposes of this section given that section 7(3)(c) provides for disclosure without knowledge or consent in compliance with a warrant or subpoena[99]. The RCMP indicated to the assessment team that this issue is not a concern as far as AML/CFT investigations are concerned and the RCMP has access to the information it needs to carry out such investigations. Nevertheless, the assessment team believes that further clarification should be brought to the Act to ensure that competent authorities have the ability to access information they require to properly perform their functions.

764. *Sharing of information between competent authorities.* The Canadian Privacy Act requires all federal departments, agencies and most Crown corporations to have lawful, authorised purposes for collection of the personal information of individuals. It also requires these departments, agencies and corporations to notify individuals of those purposes; restricts the purposes for which information collected can later be used or disclosed; and provides individuals a right of access to the personal information about them held by government institutions. The implementation of the Privacy Act does not seem to have caused problems as far as AML/CFT issues are concerned. More issues seem to arise from the PCMLTFA and the interpretation of FINTRAC of "designated information"[100] (see Section 2.5 of the report for further comments).

---

97 Section 7(3)(c.1) says: "*For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defense of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province*".

98 Pursuant to its mandate under Standing Order 108(2), the Committee publishes Statutory Reviews of the Personal Information Protection and Electronic Documents Act (PIPEDA).
See http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/reports/rp2891060/ethirp04/05-rep-e.htm

99 The Committee believes that it is important, for both organizations and law enforcement agencies, that what is meant by "lawful authority" be clarified in section 7(3)(c.1). Moreover, the Committee feels that consideration should be given to changing the word "may" in the opening part of section 7(3) in order to make the provision mandatory as opposed to permissive.

100 FINTRAC obligation to disseminate financial information to domestic authorities for further action when it has reasonable ground to suspect that the information would be relevant to the investigation or prosecution of a money laundering or terrorist activity offence seems to be too strictly implemented using a higher threshold that the one required by law. The assessors have concerns about the interpretation that is made by FINTRAC of the "threshold to disclose" level that might be reached to disclose.

765. *Sharing of information between financial institutions.* The Bank Act contains provisions regulating the use and disclosure of personal financial information by banks. Most provinces have legislation dealing with consumer credit reporting. These acts typically impose an obligation on credit reporting agencies to ensure the accuracy of the information, place limits on the disclosure of the information and give consumers the right to have access to, and challenge the accuracy of, the information. Provincial laws governing credit unions typically have provisions dealing with the confidentiality of information relating to members' transactions. There are a large number of provincial acts that contain confidentiality provisions concerning personal information collected by professionals. Such provisions do not seem to inhibit the implementation of the FATF Recommendations.

766. Generally the banks are of the view that the PIPEDA has served Canadians well in protecting information collected, used and disclosed about them by private sector organizations and has provided the necessary structure to allow private sector organizations to effectively implement its requirements into their business operations. The assessment team was told that FRFIs can share information with foreign financial institutions where this information is required by Recommendations 7, 9 or Special Recommendation VII. The exchange of information in the context of SRVII has raised concern in the past in relation to Principle 4.1.3 of Schedule 1 of the PIPEDA[101]. In 2006, the Office of the Privacy Commissioner of Canada received a complaint against six Canadian financial institutions as a result of the disclosures by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) of personal information to US authorities. The complainant was of the view the banks were responsible for the personal information that was transferred to SWIFT for processing of money orders and maintained that the disclosures were for an inappropriate purpose since they circumvented established approved processes for transferring data as set out in the PIPEDA. The Privacy Commissioner of Canada analysed the issue (see "Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities", PIPEDA case summary 365) and considered the contractual documentation that exists between SWIFT and the banks. She concluded that they are meeting their obligations under the Act, specifically, Principle 4.1.3, to ensure a comparable level of protection when processing wire transfers.

767. A comparable case was also discussed by the Privacy Commissioner of Canada in a context of outsourcing of financial services by a Canadian bank to the United States. While the PIPEDA does not prohibit the use of foreign-based third-party service providers, it does oblige Canadian-based organizations to have provisions in place, when using third-party service providers, to ensure a comparable level of protection. The Privacy Commissioner of Canada concluded that the Canadian Bank had in place a contract with its third-party service provider that provided guarantees of confidentiality and security of personal information and that an organization with a presence in Canada that outsources the processing of personal information to a U.S. firm cannot prevent its customers' personal information from being lawfully accessed by U.S. authorities. the Commissioner finally recommended that a company in Canada that outsources information processing to a third country should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country.

768. Sharing information within corporate groups is another issue raised by the banking sector. Many corporations that have multiple separate subsidiary companies, as required by federal/provincial regulatory requirements nevertheless operate as one unit under a single management team. With AML requirements, the parent bank's compliance officers must look at the activities of each client across their dealings with the entire banking group, not just each entity separately. In the securities field too, related parties assessments must include information from all parts of the financial group, not each entity separately. The AML requirements require that information about individuals be available to

[101] Principle 4.1.3 sets out that "an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party".

compliance officers, which may result in the sharing of information. In this situation, the institutions must fully apply the PIPEDA provisions and insure that their customers are aware of and consent to that practice so as to satisfy PIPEDA's requirements not to share information with different parts of the corporate group. The banking sector has called for amendments to PIPEDA that would acknowledge these other legislative requirements and facilitate regulatory reporting[102].

3.4.2 Recommendations and Comments

769. Canada should verify that the implementation of the data protection law (PIPEDA) is not subject to excessively strict interpretations that might prevent law enforcement authorities accessing information in the course of investigations.

3.4.3 Compliance with Recommendation 4

Rec.	Rating	Summary of factors underlying ratings
Rec.4	C	• The Recommendation is fully met.

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10

770. Section 6 of the PCMLTFA states that every reporting entity shall keep and retain prescribed records in accordance with the regulations.

771. The requirement to retain records for a period of at least five years applies across the board to all reporting entities, although it seems a general practice to have a record retention policy and procedures in place to maintain records for at least seven years, largely for tax purposes. Section 69 of the PCMLTF Regulations states that all records that relate to signature cards, account operating agreements, client credit files and account application forms must be kept for at least five years after the date the account is closed. Client information records (i.e. client's name and address and the nature of the client's principal business or occupation), records of certificates of corporation status, records that ascertain the existence of a corporation or entity must be kept for at least five years after the last business transaction is conducted. In respect of all other records, the records must be maintained from the day on which they have been created.

772. Financial entities have to keep the following records:

- Large cash transaction records.
- Account opening records.
- Certain records created in the normal course of business.
- Certain records about the operation of an account (such as account statements).
- Foreign currency exchange transaction tickets.
- Certain records about transactions with non-account holders.
- The name and address of the client initiating a wire transfer for CAD 3 000 or more when the financial entity is acting as an MSB.
- Trust related records (trust companies)[103].

[102] See in particular the Canadian Bankers Association response to the Office of the Privacy Commissioner of Canada on PIPEDA, 7 September 2006.

[103] Receipt of funds records will have to be kept from June 2008 (see Sections 1(2), 36(1), 39(1) (these provisions were finalized on June 27, 2007) and 33.2 and 33.4 (these provisions were pre-published on June 30, 2007) of the amended PCMLTF Regulations).

773. *Large cash transaction record*. For any large cash transaction, the information to be kept in a large cash transaction record includes the following:

- The amount and currency of the cash received.
- The name of the individual from whom the financial entity received the cash and that individual's address and principal business or occupation[104].
- The date of the transaction.
- The purpose, details and type of transaction (for example, the cash was deposited, or the cash was used to buy traveller's cheques, etc.) including whether any other individuals or entities were involved in the transaction.
- How the cash was received (for example, in person, by mail, by armoured car, or any other way).
- If an account was affected by the transaction, include the following:
    - The number and type of any such account.
    - The full name of the client that holds the account.
    - The currency in which the account's transactions are conducted.

774. If the financial entity has to identify the individual, the large cash transaction record also has to contain the following information:

- The individual's date of birth.
- The type of document used to confirm the individual's identity, the document's reference number and its place of issue.

775. In the case of a deposit, the large cash transaction record also has to include the following:
776.

- The name of the client in whose account the amount is deposited. If the amount was deposited to more than one client's account, the record has to include the names of each client.
- The time of the deposit, if it was made during normal business hours, or an indication of "night deposit" for any such deposit made outside your normal business hours.

777. *Account opening records*. These records include those required when the financial entity opens an account, such as signature cards, copies of official corporate records (binding provisions) and other information[105].

778. *Certain Records Created in the Normal Course of Business.* Financial entities have to keep the following records:

- Account operating agreement.
- Debit or credit memos.
- Client credit files[106].

779. *Certain Records About the Operation of an Account.* Financial entities have to keep the following records relating to the operation of an account:

- A copy of every account statement.
- A deposit slip[107] for every deposit made to an account.

---

104 The regulations enacted in June 2007 and coming into force in June 2008 require that the person's date of birth also be recorded (see Subsection 1(2), of the amended PCMLTF Regulations).

105 Information in relation to the intended use of the account will have to be recorded from June 2008 (see Sections 14(c.1) and 23(1)(a.1) of the amended PCMLTF Regulations).

106 "Client credit file" means a record that relates to a credit arrangement with a client and includes the name, address and financial capacity of the client, the terms of the credit arrangement, the nature of the principal business or occupation of the client, the name of the business, if any, and the address of the client's business or place of work.

- Every cleared cheque drawn on or deposited to an account.

780. *Foreign Currency Exchange Transaction Tickets.* For every foreign currency exchange transaction financial entities conduct, regardless of the amount, they have to keep a transaction ticket. A transaction ticket means a record that sets out the following information:

- The date, amount and currency of the purchase or sale.
- The method, amount and currency of the payment made or received.

781. *Transactions of CAD 3 000 or More with Non-Account Holders.* Financial entities have to keep a record for every one of the following transactions that they conduct with a person or entity that is not an account holder:

- If they receive CAD 3 000 or more for the issuance of traveller's cheques, money orders or other similar negotiable instruments. In this case, they shall keep a record of the date, the amount received and the name and address of the individual who carried out the transaction. This record also must indicate whether the amount was received in cash, cheques, traveller's cheques, money orders or other similar negotiable instruments.
- If they cash CAD 3 000 or more in money orders. In this case, they must keep a record of the name and address of the individual cashing the money order. This record also must indicate the name of the issuer of the money order. Or
- If they remit or transmit CAD 3 000 or more by any means or through any individual, entity or electronic funds transfer network. In this case, keep a record of the name and address of the client who initiated the transaction[108].

782. *Trust-Related Records.* Every trust company shall also keep the following records in respect of a trust for which it is trustee: (a) a copy of the trust deed; (b) a record of the settlor's information record; and (c) where the trust is an institutional trust and the settlor is a corporation, a copy of the part of official corporate records that contains any provision relating to the power to bind the settlor in respect of the trust (Section 15(1)).

783. *Third Party Records.* In case of third party determination, financial entities have to keep a record of the following information:

- The third party's name, address and principal business or occupation.
- The incorporation number and place of incorporation if the third party is a corporation.
- In the case of a large cash transaction, the nature of the relationship between the third party and the individual who gives the cash. Or
- In the case of an account, the nature of the relationship between the third party and the account holder.

784. If financial entities are not able to determine that there is in fact a third party, but they have reasonable grounds to suspect that there are instructions of a third party involved, they have to keep a record to indicate the following:

- In the case of a large cash transaction, whether, according to the individual giving the cash, the transaction is being conducted on behalf of a third party. Or
- In the case of an account, whether, according to the individual authorised to act for the account, the account will be used by or on behalf of a third party.

---

[107] A "deposit slip" means a record that sets out the date of a deposit, the holder of the account in whose name the deposit is made, the number of the account, the amount of the deposit and any part of the deposit that is made in cash.

[108] For all these transactions, the date of birth will have to be recorded from June 2008 (see Sections 14(k), (l), (m), 30(c), (d) and(e) of the amended PCMLTF Regulations).

785. This record must also indicate details of why financial entities suspect the individual is acting on a third party's instructions.

786. Life insurers offering certain annuities or life insurance with a savings component or a cash surrender value must retain client information records, including the date of birth (Section 19).

787. Every securities dealer shall keep the following records:

- In respect of every account that the securities dealer opens, a signature card, an account operating agreement or an account application that (i) bears the signature of the person who is authorised to give instructions in respect of the account, and (ii) sets out the account number, where that person's identity was ascertained.
- Where the securities dealer opens an account in respect of a corporation, a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of that account.
- Where the securities dealer opens an account in the name of a person or of an entity other than a corporation, a record of the name and address and the nature of the principal business or occupation of the person or entity, as the case may be.
- Every new account application, confirmation of purchase or sale, guarantee, trade authorisation, power of attorney and joint account agreement, and all correspondence that pertains to the operation of accounts, that the securities dealer creates in the normal course of business.
- A copy of every statement that the securities dealer sends to a client, if the information in the statement is not readily obtainable from other records that the securities dealer keeps and retains under the Regulations (Section 23).

788. Every money services business shall keep the following records:

- Every client information record that is created for the purpose of an ongoing business relationship between the money services business and a client.
- Where a client information record is in respect of a client that is a corporation, a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of transactions with the money services business, if the copy of that part is obtained in the normal course of business.
- Where CAD 3 000 or more is received in consideration of the issuance of traveller's cheques, money orders or other similar negotiable instruments, a record of the date, the amount received, the name and address of the person who in fact gives the amount and whether the amount received was in cash, cheques, traveller's cheques, money orders or other similar negotiable instruments.
- Where money orders of CAD 3 000 or more are cashed, a record of the name and address of the person cashing the money orders and the name of the issuer of the money orders.
- Where CAD 3 000 or more is remitted or transmitted by any means or through any person, entity or electronic funds transfer network, a record of the name and address of the client who initiated the transaction (Section 30 of the PCMLTF Regulations).

789. The PCMLTF Regulations set out detailed rules to maintain records of account files and business correspondence. Canadian financial institutions are not required to necessarily retain copies of the documentation upon which reliance is placed for verification of the customer's identity. Reporting entities are expected to note down the type and reference number and place of issue of the identity document but the actual market practice in this area seems to vary. At a provincial level, financial entities are prevented in some cases from taking copies of personal health cards while other banks advised that they would routinely take and retain copies of photo identification, a practice that is supported if not actively encouraged by OSFI. Other banks advised that this practice was not feasible on the basis of practical storage issues.

790. In the PCMLTF Regulations, the obligation to retain records of transactions is limited to certain operations that are listed by type of financial institutions. This may create potential gaps (for instance, there is no obligation in the Regulations to keep a record of all types of business correspondence but only of a limited list of such correspondence).

791. Section 68 of the PCMLTF Regulations states that where any record is required to be kept, a copy of it may be kept (1) in a machine-readable form, if a paper copy can be readily produced from it or (2) in an electronic form, if a paper copy can be readily produced from it and an electronic signature of the person who must sign the record in accordance with the Regulations is retained.

792. Financial institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days (Section 70). Although this may describe an extreme scenario and despite that financial entities advised that they can normally comply in a much shorter timescale, the current rule does not meet the requirement to make CDD records available on a *timely* basis to competent authorities, especially in normal business circumstances.

793. IDA Regulation 200 sets out detailed record keeping requirements of business transactions. The Regulation does not require the various books and records to be kept in any prescribed form. It is expected, however, that the means of recording the information will be complemented by appropriate internal controls to guard against the risk of falsification and will make available clear and accurate information to the Financial Compliance within a reasonable length of time.

Special Recommendation VII

794. At present, Canada has no provisions that address the requirements in relation to SRVII[109].The only existing obligations in relation to electronic funds transfers in the PCMLTF Regulation are as follows:

- Financial entities shall ascertain the identity of every person who requests an electronic funds transfers of CAD 3 000 or more (Section 54(1)(b)) of the PCMLTF Regulations)[110]. The identity of such person shall be ascertained by referring to the person's birth certificate, driver's licence, provincial health insurance card, passport or any similar record (Section 64(1)(a)). The current threshold of CAD 3 000 (that only applies to cross-border transfers) is not in line with SR VII;
- Financial entities (Section 12(1)(b) & (c) and money services businesses (Section 28(1)(b) & (c)) are required to report incoming and outgoing international electronic funds transfers of CAD 10 000 or more to FINTRAC. Information to be reported includes the name, address and account number of the client ordering the electronic funds transfer.

795. There are currently no requirements for ordering financial institutions either to obtain or maintain full originator information or to include such information in cross border wire transfers. The assessors were told that, at present, only originating customer name and address are included in such transfers as the account number is considered to be private personal information.

796. While the assessors were told that financial entities and money services businesses are taking measures in identifying and handling wire transfers that are not accompanied by complete originator information, there is currently no regulatory or legal requirements to adopt risk-based procedures or conduct enhanced due diligence.

---

109 New provisions will come into force on 23 June 2008 (see Section 66.1 of the amended PCMLTF Regulations that must be read in conjunction with Section 9.5 of the amended PCMLTFA).

110 "Electronic funds transfer" means the transmission – through any electronic, magnetic or optical device, telephone instrument or computer- of instructions for the transfers of funds, other than the transfers of funds within Canada. In the case of SWIFT messages, only SWIFT MT 103 messages are included" (PCMLTF Regulations).

797. FINTRAC has a responsibility to ensure compliance with the legislative requirements under the PCMLTFA, including the customer due diligence and originator information inclusion requirements for wire transfers. Until the legislative changes take effect and formalise the requirement for full originator information, enforcement measures can only be on a best efforts basis without any formal powers of sanction or penalty.

798. The assessment team was advised that casinos process electronic funds transfers using their own internal corporate system, *i.e.* outside the banking sector. The team is not aware of any controls that exist, and no more details were provided despite the team's request (in this situation, casinos are considered as financial institutions since they conduct a business that is covered under the FATF definition of financial institutions).

3.5.2 Recommendations and Comments

799. *Recommendation 10*. Canada should ensure that all types of transactions (including business correspondence) carried out by financial institutions (except for IDA members) are subject to proper record keeping requirements that permit their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. Canada should ensure that all customer and transactions records and information are available on a timely basis to domestic competent authorities.

800. *SR.VII*. Canada should ensure that the new provisions enacted in December 2006 and coming into force in June 2008 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. Canada should ensure that the wire transfers operated by casinos outside the banking network are subject to equivalent requirements.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

Rec.	Rating	Summary of factors underlying ratings
Rec.10	LC	*Scope issue* • The record keeping requirement does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies); • Financial institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which does not meet the requirement to make CDD records available on a *timely* basis to competent authorities, especially in normal business circumstances.
SRVII	NC	• Canada has not implemented SRVII.

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

801. Under the PCMLTFA, there is currently no explicit provision requiring that financial institutions must pay special attention to all complex, unusual large transactions[111]. As noted earlier, there is no explicit obligation to conduct on-going monitoring of accounts or transactions under the current legislation.

802. Thus, such a requirement may only be indirectly deduced from the requirement to report to FINTRAC suspicious transactions that may be related to money laundering or terrorist financing, as well as the obligation to report large international electronic funds transfer reports involving CAD 10 000 or more (EFTRs) and large cash transaction reports of CAD 10 000 or more (LCTRs).

803. In its Guidelines, which are provided as general information only, FINTRAC provides indicators, both common and industry-specific, to financial institutions on how suspicious transactions

[111] The PCMLTFA as amended in June 2007 sets out new requirements in this area that will enter into force in June 2008.

can be detected. These indicators include, among others, patterns of unusually large or complex transactions with no economic purpose, such as :

- Transaction that seems to be inconsistent with the client's apparent financial standing or usual pattern of activities.
- Transaction that appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the client.
- Transaction that is unnecessarily complex for its stated purpose.
- Activity that is inconsistent with what would be expected from declared business.
- Client who starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Client who asks reporting entity to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.

804. It is worth noting that some regulators or regulatory organizations have introduced additional recommendations or rules relating to the monitoring of unusual transactions:

- Concerning federally regulated financial institutions, OSFI states in very general terms in its Guidelines, that *"the policies and procedures should […] include measures to monitor transactions. These measures will help FRFIs to identify potentially suspicious transactions by using criteria that will enable them to detect unusual or abnormal activity"*. OSFI also encourages FRFIs to implement the Basel *Customer Due Diligence for Banks* paper *"in a manner appropriate to the size, complexity and nature of the institution's business activities"*.
- Concerning securities dealers firms, the IDA has issued regulations and policies related to the supervision of accounts (see Regulation 1300 and Policy n° 2) which contain precise rules relating to the performance by members of reviews aiming at detecting *"items for further investigation or an examination of unusual trading activity or both"*. The IDA Guide on "Deterring money laundering activity – A Guide for Investment Dealers" sets out that "a firm should adopt procedures setting forth appropriate parameters and methods of monitoring account activity so that unusual or suspicious transactions can be detected".

805. The assessors were not provided with any specific AML requirements (excluding FINTRAC non-binding guidelines) that included obligations relating to unusual transactions issued by primary supervisors to other sectors such as credit unions. However, the AMF, in Quebec, indicated that it was in the process of developing AML/CFT standards.

806. The assessors met with a number of large financial institutions, and in practice it seems that such institutions have adopted procedures and systems to detect and further examine complex, unusual large transactions in order to comply with their reporting obligations. Such transactions are usually identified by financial institutions in two different ways: 1) at the front line in executing the transaction for the client; and 2) through the use of software based on rules or profiles to monitor and identify unusual transactions. Unusual transactions are forwarded to corporate security and/or the AML compliance group for further analysis. Where the unusual transaction meets the test of reasonable grounds to suspect ML or TF, a suspicious transaction report is prepared and sent to FINTRAC.

807. Nevertheless, there is insufficient information available to determine whether this practice is universal and the current legislative and regulatory framework remains too general and implicit with respect to the monitoring of complex, unusual large transactions to meet the FATF requirements. In particular, there is no specific requirement that financial institutions examine the background and purpose of such transactions and, especially, set forth their findings in writing. Under the current

legislation, financial institutions are not required to keep a record of the STRs that they file with FINTRAC[112].

808. As a business practice, a number of financial institutions that detect such unusual transactions indicated that they would usually conduct further research on the customer's transactions in order to determine whether, based on the knowledge in hand, the threshold for determining suspicion has been met and hence an STR must be filed with FINTRAC. The section of the report describing the suspicious activity is very important as it explains what led the financial institution to believe there is something suspicious about the transaction. Financial institutions are expected to clearly and completely describe all of the factors or unusual circumstances which led them to a suspicion of money laundering or terrorist financing, and provide as many relevant details as possible to support this determination. Financial institutions are also required to describe what action, if any, was taken by them, as a result of the suspicious transaction, in addition to reporting to FINTRAC. Such action could include, for example, sending a report to law enforcement in addition to FINTRAC. Nevertheless, there are no provisions under the PCMLTFA and PCMLTFR requiring that such actions and their results be documented and kept available for competent authorities, especially if no STR is finally filed with FINTRAC[113].

809. Large financial institutions met by the assessment team such as banks generally appear to comply with this requirement on a voluntary basis. Moreover, concerning securities dealers, the IDA Rulebook requires in Policy n° 2 that *"evidence of supervisory reviews must be maintained. Evidence of the review, such as inquiries made, replies received, actions taken, date of completion etc. must be maintained for seven years and on-site for 1 year"*. But there is no evidence that this practice is generalized among the other types of financial institutions.

Recommendation 21

Special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations

810. Requirement to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. On every occasion that the FATF has invoked Recommendation 21 in the context of the NCCT (Non-cooperative Country and Territory) process, FINTRAC and OSFI have issued advisories asking financial institutions and reporting entities to pay special attention with respect to any business or affairs being transacted with persons or entities from identified countries or territories. Financial institutions are requested to take this into account directly or through any subsidiary or branch operations. In addition, competent authorities in Canada (including FINTRAC, OSFI and IDA) communicated on a regular basis with the reporting entities to provide regular updates and required financial institutions to pay "special attention by exercising appropriate due diligence and caution in conducting any transactions with such persons or entities"[114].

---

112 The PCMLTF Suspicious Transaction Reporting Regulations enacted in June 2007 that will come into force in June 2008 require reporting entities to keep a copy of every STR they file with FINTRAC for five years (Section 12.1).

113 As mentioned above and under Section 12.1 of the PCMLTF Suspicious Transaction Reporting Regulations financial institutions will be required from June 2008 to keep a record of every STR that they file with FINTRAC for five years. A Suspicious Transaction Report, and the related record includes detailed information about the person or entities involved, the nature and type of transaction and a description of the suspicious activity. The Regulations require details of suspicious attempted transaction reports to also be kept on file for five years. Under the new regime, financial institutions have to ensure that such records can be provided to a FINTRAC compliance officer within 30 days. Law enforcement representatives can access these records if they obtain a search warrant or production order from a court.

114 In October 2007 and consistent with the FATF action, OSFI and FINTRAC issued statements to indicate that Canadian financial institutions and reporting entities should give heightened attention to transactions to Iran.

811. Advisories describe how OSFI administers and interprets provisions of existing legislation, regulations or guidelines, or provide OSFI's position regarding certain policy issues. OSFI clearly states that advisories are not law and that readers should refer to the relevant provisions of the legislation, regulation or guideline, including any amendments that came into effect subsequent to the Advisory's publication, when considering the relevancy of the Advisory. The assessment team was told that failure to implement OSFI advisories could result in regulatory action by OSFI.

812. In FINTRAC and OSFI advisories, reporting entities are generally asked to exercise an enhanced level of scrutiny when dealing with transactions from or in NCCTs involving exercising appropriate due diligence and caution in conducting transactions.

813. Based on these advisories, FINTRAC has included the monitoring of transactions and enhanced due diligence with respect to NCCTs within its compliance verification structure although the advisories are not enforceable and failure to implement them cannot be subject to sanction. There is a section related to NCCTs in FINTRAC's Compliance Questionnaires. As well, it is standard practice in FINTRAC examinations of financial institutions to review the policies and procedures of an entity, with respect to enhanced due diligence with any jurisdictions that the FATF has identified as being of particular concern.

814. FINTRAC Guideline 2 on suspicious transaction reporting provides indicators for identifying suspicious transactions involving other countries, including "transactions involving countries deemed by the FATF as requiring enhanced surveillance". OSFI Guideline B-8 also addresses the need for federally regulated financial institutions to develop higher levels of due diligence when processing transactions connected to NCCTs.

815. When the FATF no longer has concerns regarding a particular jurisdiction, e.g. when NCCTs were de-listed or their status was otherwise changed, both FINTRAC and OSFI have issued further advisories to reporting entities to inform them on the change and request them to continue monitoring transactions from such a jurisdiction as long as it remains of concern.

816. For securities dealers, the IDA requires its members to heighten scrutiny of accounts and transactions from NCCT countries: it requires that its members give special attention to business relations and transactions with persons, including companies and financial institutions, from the NCCT list. The IDA requires that its members ensure strict adherence to the client identification and verification requirements of the Regulations under the PCMLTFA and that relevant sales and operational personnel are made aware of the countries and territories which have been identified as NCCTs.

817. *Measures to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.* As regards countries (other than NCCT countries) which do not or insufficiently apply the FATF Recommendations, FINTRAC and OSFI Guidelines call for special vigilance when doing business with a range of entities, including those in countries with inadequate AML/CFT controls; located in offshore jurisdictions; located in countries with highly secretive banking and corporate law; or in countries known or suspected of facilitating money laundering activities. FINTRAC Guideline points out the International Narcotics Control Strategy Report, released by the U.S. Department of State, to assist reporting entities in undertaking a risk analysis of foreign dealings. OSFI also advises banks with correspondent banking operations to implement additional safeguards when dealing with banks operating in jurisdictions they consider to be of higher risk. The IDA advises its members to ensure proper application of the provisions under the PCMLTFA to clients in countries without adequate anti-money laundering regimes such as in the case of the FATF NCCTs list. With the exception of the general advice described above, financial institutions have not been advised of concerns about specific countries that do not or insufficiently apply the FATF Recommendations, or which have specific weaknesses in their AML/CFT systems(even if their system overall could be considered adequate). For example, such advice could result from a mutual evaluation within the FATF or within an FATF Style Regional Body).

818. *Requirement to examine the background and purpose of transactions and keep written records*. There is no explicit requirement for financial institutions to examine the background and purpose of those transactions that have no apparent economic or visible lawful purpose. Financial institutions are not required to document in writing the findings in relation to these transactions and to keep the later available for competent authorities and auditors.

Countermeasures

819. When counter-measures have been considered by FATF against some NCCTs, FINTRAC and OSFI have advised reporting entities to apply enhanced due diligence to financial transactions emanating from, or destined to the specified jurisdiction and viewed them as potentially suspicious. Reporting entities were urged to exercise an enhanced level of scrutiny when dealing with transactions involving the identified jurisdiction and undertake heightened customer identification due diligence measures to ensure that the principals or beneficial owners are identified. In FINTRAC non-binding advisories, financial institutions were advised that financial transactions emanating from, or destined to countries subject to FATF countermeasures had to be viewed by reporting entities as potentially suspicious.

820. The Minister of Finance, under the *Bank Act*, has the authority to approve the establishment of subsidiaries and branches of foreign financial institutions. In addition to requiring criminal checks and broad fit and proper tests, the Minister considers the "National Security" and "Canada's international relations and obligations" tests during the application process. The assessment team was told that this includes consideration of whether a country was found to be severely deficient in its implementation of AML/CFT standards by the FATF. However, there is no evidence that this mechanism has not been used in the context of countermeasures.

821. Canada also notes that it takes counter-measures against countries that pose specific economic and security risks to Canada through the *Special Economic Measures Act (SEMA)*. This legislation provides for a wide range of economic and financial measures against a foreign state, including: seizing or freezing assets of a foreign state, or of persons from that state, restricting or prohibiting Canadians from dealing in property of that state, from exporting, selling, importing, acquiring goods from that state or from providing or acquiring any financial or other services to or from that state. These mechanisms have not been used in a context of a country that continues not to apply or insufficiently applies the FATF recommendations[115].

3.6.2 Recommendations and Comments

822. *Recommendation 11*. In order to comply with Recommendation 11, Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.

823. *Recommendation 21*. The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to all financial institutions. Effective measures should be put in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems. This should be completed by a provision requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

[115] For example, Canada used SEMA in December 2007 against Myanmar - on December 13, 2007, the *Special Economic Measures (Burma) Regulations* came into force in order to respond to the "abhorrent human rights and humanitarian situation in Burma".

3.6.3 Compliance with Recommendations 11 and 21

Rec.	Rating	Summary of factors underlying ratings
Rec.11	PC	• There is no explicit nor enforceable requirement for financial institutions to examine all complex, unusual large transactions under the current legislation (except for IDA members). Except for IDA members, the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11; • There is no explicit requirement to examine the background and purpose of these unusual transactions (except for IDA members) • There is no requirement to keep record of financial institutions' findings in relation to complex, unusual large or unusual patterns of transactions.
Rec.21	PC	• There is no general enforceable requirement for financial institutions to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations. • There are no effective measures in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems • There is no requirement to examine the background and purpose of these transactions and to document the related findings.

3.7 Suspicious transaction and other reporting (R.13-14, 19, 25, 32 & SR.IV)

3.7.1 Description and Analysis

Recommendation 13 & Special Recommendation IV

824. *Suspicious transactions reporting obligation*. All financial institutions subject to the PCMLTFA are required to report to FINTRAC transactions of any amount for which there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist financing offence (Section 7 of the PCMLTFA). The requirement applies to all persons and entities subject to Part I of the PCMLTFA, including the following financial institutions:

825.

- Financial entities: banks, credit unions, *caisses populaires*, trust and loan companies and agents of the Crown that accept deposit liabilities.
- Life insurance companies, brokers and agents.
- Securities dealers including portfolio managers and investment counsellors.
- Money services businesses including the business of foreign exchange dealing and alternative remittance systems, such as *hawala, hundi* and *chitti*.
- Canada Post for money orders.

826. However, as stated above in Section 3.1 of the report, several categories of financial institution, such as financial leasing, factoring, electronic money institutions, finance companies of customer credit, credit and debit cards companies are not subject to the PCMLTFA and, consequently, to any mandatory reporting requirement to FINTRAC.

827. In the PCMLTFA, the terms "money laundering offence" and "terrorist financing offence" refer directly to their definition in the Criminal Code which indicates that suspicious transaction reports must be made in relation to all the predicate offences to money laundering and terrorist financing. These offences include virtually all indictable offences under the Criminal Code or any other federal Act. The few exceptions are for offences such as those related to tax evasion or breach of copyright and some others that involve administrative and monetary penalty structure.

828. The PCMLTF Suspicious Transaction Reporting Regulations establish the form and manner for reporting, including the list of information to report and prescribe the reporting time limits. A Suspicious Transaction Report must be filed with FINTRAC within 30 days from the date the

suspicion was formed about the transaction. Failure to report a suspicious transaction could lead to up to five years imprisonment, a fine of CAD 2 million, or both.

829. FINTRAC's Suspicious Transactions Reporting guideline further elaborates on the requirement and explains that financial institutions should look at what is reasonable under the circumstances, including normal business practices and systems within the industry, to reach the "reasonable grounds to suspect" threshold. The guideline also provides an extensive list of general and sector specific indicators to help financial institutions assess the behaviour of the customer and their transactions.

830. A Suspicious Transaction Report must include detailed information about the person or entities involved, the nature and type of transaction and a description of the suspicious activity. Certain fields in the report must be filled on a mandatory basis, while others on reasonable efforts, which means that the financial institution must make every effort to obtain the information required in the report. If the information is available or can be obtained from the financial institution's records, it must be included in the report. The suspicious transaction report explains what led the financial institution to identify the transaction as suspicious (part G of the suspicious transaction report). Financial institutions are expected to describe clearly and completely all of the factors or unusual circumstances which led them to a suspicion of money laundering or terrorist financing, and provide as many relevant details as possible to support this determination. Financial institutions are also required to describe what action, if any, has been taken by them as a result of the suspicious transaction, in addition to reporting to FINTRAC. Such action could include, for example, sending a report to law enforcement in addition to FINTRAC, monitoring or closing the account.

831. *Attempted transactions and threshold.* There is no monetary threshold associated to the requirement to report STRs to FINTRAC, all suspicious transactions must be reported regardless of the amount of the transaction.

832. Under the current legislation, reporting entities are only required to report completed transactions to FINTRAC. FINTRAC Guideline 2 indicates that "*the requirement (…) to report a suspicious transaction applies only when the financial transaction has occurred. (…) If you decide or the client decides not to complete the transaction, there is no obligation to report it as a suspicious transaction to FINTRAC*".

833. Financial institutions can choose to report an uncompleted transaction and a suspicion about it directly to law enforcement and can also decide to report it to FINTRAC on a voluntary basis. As a matter of fact, IDA, in a notice of October 2001 about the "Implementation of Suspicious Transaction Reporting Regulations" strongly recommends that its members voluntarily report to either to FINTRAC or the police, of any approach that raises a suspicion of being related to criminal activity or money laundering. Nevertheless, the assessment team was told that by the banking sector that sending such reports is not a current practice in this sector.

834. The PCMLTF Regulations broaden the reporting requirement to the reporting of any suspicious attempted transactions related to money laundering or terrorist financing, but as the implementation of the measure requires IT developments both at FINTRAC and in financial institutions, it will not be in force until June 2008.

835. *Tax matters*. The PCMLTFA requires the reporting of all completed transactions, where there are reasonable grounds to suspect that they relate to the commission of a money laundering or a terrorist financing offence, regardless of the involvement in tax matters. Furthermore, the PCMLTFA allows FINTRAC to disclose information to the Canada Revenue Agency when it meets the dual test of firstly having reasonable grounds to suspect that the information contained in the disclosure would be relevant to money laundering or terrorist financing investigation and secondly, if FINTRAC also determines that the information is relevant to an offence of evading or attempting to evade paying taxes or fraudulently attempting to obtain a tax rebate, refund or credit.

836. *Additional elements*. The predicate offences for money laundering include the commission in Canada of a designated offence or an act or omission anywhere that, had it occurred in Canada would have constituted a designated offence.

837. *Statistics*. The number of STRs reported to FINTRAC is as follows:

	2001/2002	2002/2003	2003/2004	2004/2005	2005/2006	2006/2007	**Total**
STR	3 772	17 358	14 794	19 113	29 367	18 431	**102 835**

838. The following table indicates the number of STRs per fiscal year and by financial sector:

	2001/2002	2002/2003	2003/2004	2004/2005	2005/2006	2006/2007	**Total**
Banks	576	3 623	4 077	5 665	12 084	5 174	**31 199**
Caisses Populaires	1 045	3 357	1 946	3 151	4 918	5 185	**19 602**
Cooperative Credit Society	20	29	-	1	6	0	**56**
Life insurance brokers or agents	1	1	11	2	4	0	**19**
Life insurance companies	10	30	52	29	32	78	**231**
MSBs	1 207	6 962	5 165	6 176	8 090	5 826	**33 426**
Provincial Savings Office	5	61	17	202	336	114	**735**
Credit Unions	639	2 415	2 767	3 905	2 837	1 377	**12 940**
Securities dealers	42	169	80	74	83	48	**496**
Trust and loan companies	31	37	64	214	438	388	**1 172**
Total	3 576	16 684	14 179	19 419	23 910	18 190	**95 958**

839. The total number of STRs sent by the financial sector appears globally satisfactory (an average of 20 000 every year since 2004). Since FINTRAC first became operational, in fiscal year 2001-2002, it has received about one hundred thousand STRs from financial institutions (95 958), representing 97 % of the total of STRs received. The annual total number of STRs has been steadily increasing since 2001/2002.

840. The different categories of financial institutions have however contributed unequally to the total number of STRs received by FINTRAC, with the majority of STRs received from MSBs, followed by banks, *caisses populaires* and credit unions. On the other hand, securities dealers, life insurance companies and, even more noticeably life insurance brokers and dealers have sent limited numbers of STRs.

841. Based on further statistics made available to the assessment team (on Canada request, such statistics cannot be published), it appears that only a limited number of MSBs report STRs to FINTRAC considering the wide range of MSBs active in Canada. Most of the STRs filed are sent by the larger players of the sector.

842. The quality of the reports is improving, following the numerous information and training sessions delivered by FINTRAC to reporting entities. The electronic format of the STRs, although quite constraining (see comments in Section 2.5 of the Report), and the electronic feedback of missing

information on every report filed electronically, help financial institutions to meet their obligations in that respect. An extensive use of the section of the STR intended to receive comments describing the suspicious activity generally helps however to overcome the rather rigid format of the STRs.

843. Indicators of terrorist financing (*e.g.* terrorist listings, particular products and countries involved) have been used by reporting entities in the narrative section of a number of reports submitted to FINTRAC. However, FINTRAC was not able to provide to the assessors the approximate number of STRs reported which have involved suspected terrorist financing.

Recommendation 14

844. *Protection from criminal liability of reporting entities*. Section 10 of the PCMLTFA prescribes the immunity provisions for reporting entities. No criminal or civil proceeding lie against persons and entities for making a suspicious transaction report, a terrorist property report, a large cash transaction report or an electronic funds transfer report in good faith or for providing FINTRAC with information about suspicions of money laundering or of the financing of terrorist activities. In addition, Section 462.47 and 487.014 of the Criminal Code establishes a safe harbour defence for persons or entities disclosing a suspicion of money laundering to the police or the Attorney General.

845. *Tipping off*. Section 8 of the PCMLTFA specifies that no person or entity can disclose that they have made a suspicious transaction report, or disclose the contents of a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. Failure to comply with these requirements could result in up to two years imprisonment.

846. *Additional elements*. Subsection 58(2) of the PCMLTFA prohibits FINTRAC from disclosing any information that would directly or indirectly identify an individual who provided a report or information to FINTRAC, or a person or an entity about whom a report or information was provided. FINTRAC employees and contractors are subject to criminal penalties of up to five years in jail or a fine of CAD 500 000 or both, for unauthorised disclosure or use of information.

847. FINTRAC is subject to the Privacy Act that strictly regulates how federal institutions can use and disclose personal information collected about individuals. In addition, the PCMLTFA stipulates that one of FINTRAC's objectives is to ensure that the personal information under its control is protected from unauthorised disclosure. High standards of information privacy and security are important for FINTRAC and FINTRAC continually monitors its systems and recently made improvements to its security monitoring capabilities.

848. Based on the discussions that took place during the on-site visit, the assessment team came to the conclusion that no major issues arise in relation to the implementation of the requirement sunder Recommendation 14.

Recommendation 25 (only feedback and guidance related to STRs)

Guidance related to STRs

849. FINTRAC gives very detailed guidance related to STRs to assist financial institutions in implementing and complying with STR requirements. FINTRAC has developed standard reporting form for all types of existing reporting. Such guidelines are posted on the FINTRAC website.

850. In relation to STR requirements, FINTRAC has adopted two guidelines that deal specifically with STRs: Guideline 2: Suspicious Transactions provides information on identifying suspicious transactions, including common an sector-specific indicators related to money laundering and indicators related to terrorist financing. Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC; delivers very detailed information on, among other things: timelines and format (electronic vs. paper) of the report, instructions for completing reporting forms including the type of information to deliver under each field of the reporting form, etc.

851. The industry bodies spoken to by the evaluation team expressed satisfaction at the guidance provided in relation to the reporting requirement.

Feedback

852. The ways FINTRAC may provide feedback includes the following general and specific elements:

- The Annual Report provides general feedback such as:
  - statistics on reports received
  - disclosures made
  - contribution of each type of report to these disclosures
  - a sanitized ML case
  - typologies and indicators of ML and TF
- Electronic feedback on every report filed electronically.
- Feedback session, at least once a year, to the Canadian Bankers Association (CBA) and the CBA Anti-Money Laundering Working Group.
- Annual presentation to ten of the largest providers of reports.
- Presentations to each reporting sector at least once a year.
- Meeting on a one-on-one basis with individual reporting entities to discuss any issues an entity may have.
- FINTRAC staff also make presentations at, and participate in, industry conferences attended by representatives of reporting entities.
- Macro analysis of patterns, typologies and trends (international, national, regional and sectoral) that characterize money laundering and terrorist activity financing.

853. FINTRAC provides financial institutions and DNFPBs with general and specific feedback.

General Feedback

854. FINTRAC provides feedback presentations to each reporting entity sector (*e.g.* at industry association conferences or other meetings) at least once a year. These feedback sessions include discussions of general reporting trends for the sector and how STRs and other reports from that sector contributed to FINTRAC's disclosures to law enforcement. Other issues, including quality of reporting, are also discussed.

855. Presentations are tailored specifically to either a reporting entity, or an association covering a group of reporting entities, by illustrating the percentage of reports they submitted versus other reporting entities and pinpointing the percentage of their reports that factored into ML and/or TF disclosures.

856. For example, FINTRAC meets at least once a year with the Canadian Bankers Association (CBA) and the CBA Anti-Money Laundering Working Group. CBA members provide approximately 65% of all reports received by FINTRAC. These feedback sessions are a minimum of half a day in duration and address everything from their membership's contribution to reporting (by report type), systematic quality or timing issues, and the way in which their member's reports contributed to ML and/or TF disclosures. FINTRAC tactical analysts participate to these sessions and present various sanitized ML and/or TF cases.

857. FINTRAC also provides similar presentations to about ten of the largest providers of reports. In 2005-06, FINTRAC staff prepared 17 presentations to be delivered to individual reporting entities and industry associations representing different types of reporting entities and in 2004-05, there were 20 such meetings.

858. FINTRAC provides reporting entities with information about internationally recognized trends and typologies. With time, the volume of STRs (and other reports) and the number of disclosures continue to increase considerably, allowing FINTRAC to identify patterns, typologies and trends based on its own work (international, national, regional and sectoral) that characterize domestic money laundering and/or terrorist activity financing.

859. FINTRAC's annual report is another way to provide feedback to reporting entities. For instance, the 2006 annual report presents a very complex sanitized ML case to demonstrate how it uses reports received from reporting entities and what FINTRAC includes in a disclosure to law enforcement. FINTRAC's annual reports also provide statistics on various types of reports received from reporting entities and on disclosures made to law enforcement and the contribution of each type of report to these disclosures. Annual reports also present indicators of ML and TF. Every year, FINTRAC's Annual Report is tabled before the Canadian Parliament in the fall, and is provided in hardcopy format to reporting entities, as well as posted on the FINTRAC's website.

860. There is a need for FINTRAC to publish more concrete and targeted information on ML and TF. The information published by FINTRAC is in general very descriptive and does not provide very in depth analysis. FINTRAC should be able to provide more comprehensive data on techniques and trends in specific sectors. The Annual Report 2006 for instance publishes one sanitised case; the assessors are of the view that more ML/TF cases should be made public in sanitized form in order to increase awareness and improve compliance and reporting. FINTRAC is in quite a unique position to develop and disseminate strategic intelligence but has not taken advantage so far to develop more substantive information.

Specific Feedback

861. FINTRAC automatically provides electronic feedback on every report filed electronically (over 99% of reports submitted to FINTRAC are filled electronically). This feedback highlights to reporting entities any data quality issues that are present or any potential data quality issues they may want to review on a report-by-report basis. FINTRAC also immediately advises a reporting entity if its report was accepted or rejected due to significant data quality issues. FINTRAC can also request that reporting entities re-submit reports received if certain data elements are missing.

862. Given the time sensitivity of STRs, FINTRAC will also provide direct verbal follow-up on the quality of the reports. However, the PCMLTFA prohibits FINTRAC from providing feedback on the outcome of the individual reports made to FINTRAC.

863. FINTRAC has developed comprehensive guidance and quite good general feedback for reporting entities. FINTRAC has initiated a series of feedback presentations for a number of large reporting entity sectors and entities. These presentations offered initial insights on reporting levels, the use of reports in our case disclosures, as well as some examples of sanitized cases. However, the general feedback concentrates more on large financial institutions.

Recommendation 19

864. The PCMLTFA requires reporting entities to submit reports to FINTRAC on large cash transactions and electronic funds transfers.

865. Section 9 of the PCMLTFA establishes a requirement for all persons and entities subject to Part 1 of the PCMLTFA to report to FINTRAC any transaction prescribed in regulations. Two types of reportable transactions are prescribed under the PCMLTF Regulations: large cash transactions and international electronic funds transfers.

866. Financial institutions (as well as accountants, casinos and real estate brokers and sales representatives) are required to report to FINTRAC the receipt of an amount in cash of CAD 10 000 or more in Canadian currency or its equivalent in foreign currency. Reportable cash transactions include

single transactions and two or more transactions by or on behalf of the same individual or entity that are conducted in a 24-hour period and that total CAD 10 000 or more, as described under section 3 of the PCMLTF Regulations. A Large Cash Transaction Report (LCTR) must be submitted to FINTRAC within 15 days of the transaction.

867. With respect to the large cash transaction reporting regime, an exception scheme – called the Alternative to Large Cash Transaction Reports to FINTRAC – is provided for in the PCMLTF Regulations. In order to assist reporting entities, FINTRAC has developed a guideline on the Alternative to LCTRs, Guideline 9, which is posted on the FINTRAC website.

868. Alternative to sending large cash transaction reports applies only to certain clients of financial entities (banks, credit unions, *caisses populaires*, trust and loan companies and an agent of the crown that accepts deposit liabilities) that are corporations. Criteria have to be met before financial entities can choose for the alternative to large cash transaction reports:

- The client of the financial entity is a corporation that carries on business within a list of business excluding business with high risk of ML or TF.
- The client of the financial entity must have an account with the financial entity or another financial entity for at least 24 months.
- The client deposited CAD 10 000 or more in cash at least twice a week, on average, for the preceding 12 months.
- The cash deposits are consistent with the usual practices of the business;
- Reasonable measures have been taken to determine the source of the cash for the deposits.

869. Where these conditions are met, financial entities are not obliged to submit large cash transaction reports to FINTRAC but have to:

- Send a report to FINTRAC about the business client for whom they are making this choice.
- Report certain changes about the business client to FINTRAC.
- Verify annually that conditions are met for each client and report this to FINTRAC.
- Maintain a list with the name and address of each client for whom they have chosen not to report large cash transactions.

870. Reportable information in a LCTR is listed in Schedule 1 to the PCMLTF Regulations. The record includes identifying and banking information on the person or entities involved, including persons on behalf of who the transaction is conducted and the purpose and details of the transaction.

871. Similar reporting requirements apply to deposit taking institutions and money services businesses (including foreign exchange dealers) in respect of outgoing and incoming international electronic funds transfers of CAD 10 000 or more (including single transactions and two or more transactions by or on behalf of the same individual or entity that are conducted in a 24-hour period and that total CAD 10 000 or more). These include both transfers made using the SWIFT system, as well as those using proprietary systems (non-SWIFT). An Electronic Funds Transfer Report (EFTR) must be filed within five working days of the transfer.

872. Since FINTRAC first became operational, in fiscal year 2001-2002, it has received about 16 million LCTRs and 29 million EFTRs.

873. The criminal penalty for failure to report a LCTR or EFTR could lead to a fine of up to CAD 500 000 for a first time offence and CAD1 000 000 for a subsequent offence.

874. FINTRAC devotes resources to improving the data quality, refining analytical tools and upgrading systems.

875. High standards of information privacy and security are important for FINTRAC, as already explained in section 2.5. FINTRAC continually monitors its systems and recently made improvements to its security monitoring capabilities.

Statistics

876. Statistics available at FINTRAC are generally very comprehensive (especially on STRs, LCTRs and EFTRs). However, this report delivers a limited range of them on Canada request and for confidentiality purposes.

3.7.2 Recommendations and Comments

877. All financial institutions covered by the definition of the FATF should be subject to the suspicious transactions reporting requirement unless a proven low risk of ML and FT is established in the sectors that are currently exempted. The different categories of financial institutions contribute unequally to the total number of STRs received by FINTRAC, this is an issue that FINTRAC should address further.

878. FINTRAC should develop more general feedback for smaller reporting entities. While legislation prevents FINTRAC from giving feedback on how it has used specific reports, FINTRAC should consider implementing more specific feedback mechanisms.

879. FINTRAC could consider disseminating more figures and data that do not breach applicable confidentially rules. This would certainly help increasing awareness and improving general compliance and reporting. FINTRAC should collect more data on the number of reports that it receives in relation to suspected terrorist financing.

3.7.3 Compliance with Recommendations 13, 14, 19, 25 and Special Recommendation IV

Rec.	Rating	Summary of factors underlying ratings
Rec.13	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report; ▪ There is no requirement to report attempted transactions; ▪ The low numbers of STRs sent by certain financial sectors raise concerns in relation to the effectiveness of the reporting system.
Rec.14	C	▪ The Recommendation is fully met.
Rec.19	C	▪ The Recommendation is fully met.
Rec.25	LC	▪ There is not enough general feedback given outside the large financial institutions sector.
SR.IV	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report; ▪ There is no requirement to report attempted transactions.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis

Recommendation 15

880. Currently, the PCMLTFA itself contains no specific requirement for the development and maintenance of an AML/CFT compliance regime by the reporting entities[116]. Such a requirement is

[116] Article 9.6 (1) of the PCMLTFA provides for a general compliance program requirement in force in June 2008. The compliance regime requirements will be expanded to include, among other things, a written

prescribed in Section 71 of the PCMLTF Regulations that requires every person or entity subject to the PCMLTFA to establish a compliance regime for complying with the PCMLTFA. The compliance regime must include, "as far as practicable", the following four core elements:

a. The appointment of a person who is responsible for the implementation of the compliance regime.
b. The development and application of compliance policies and procedures.
c. A review of those policies and procedures that is conducted as often as necessary to test their effectiveness by an internal or external auditor of the person or entity or, if it does not have such an auditor, by the person or entity itself (the proposed regulations require minimum review once every 2 years).
d. Where the person or entity has employees or agents or persons authorised to act on behalf of the person or entity, an ongoing compliance training program for those employees, agents or persons.

881. The "as far as practicable" illustrates the need to adopt more or less sophisticated or formal policies and procedures depending on the size of the business.

882. FINTRAC's Guideline 4 provides more specific direction on what is expected to be in place for each component of the compliance program based on the type and the size of the business of the reporting entity. Other financial sector regulators impose similar requirements on their respective supervised entities.

Internal Policies, Procedures and Controls

883. The current PCMLTF Regulations require reporting entities to develop and apply policies and procedures to comply with the anti-money laundering and anti-terrorist financing requirements imposed under Part I of the PCMLTFA. FINTRAC's Guideline 4 provides further details on what these policies and procedure should encompass, including policies and procedures that must show the business's commitment to prevent, detect and address non-compliance. In addition, such policies and procedures must incorporate, at a minimum, the reporting, record-keeping and client identification requirements applicable to the business and it is suggested that they specify situations where an enhanced level of caution is required. Nevertheless, it is not specifically required that rules regarding detection of unusual and suspicious transactions be included. However, when performing its compliance assessments, FINTRAC does inform reporting entities that they should have policies and procedures to identify and report suspicious transactions.

884. OSFI Guideline B-8 goes beyond the basic requirements laid down by the PCLMLTF Regulations and the FINTRAC Guidelines by specifying that "*the policies and procedures should include measures to permit the FRFIs to identify and report Large Cash Transactions. The policies and procedures should also include measures to monitor transactions*". The IDA rules specify that "*firms should have procedures in place that are designed to assist personnel in detecting unusual or suspicious activities*". The IDA has generally advised that AML/CFT policies and procedures should be integrated into a dealer's general compliance regime, for example in the guide "Deterring Money Laundering Activity", the IDA notes: *"a firm's existing policies and procedures for its various business functions should form the basis for its overall money laundering prevention program. This will assure that anti-money laundering compliance reaches all aspects of a firm's business. As an initial matter, a firm could consider reviewing and evaluating those procedures and, where appropriate, enhance them to address anti-money laundering issues"*.

885. The degree of detail and formality of the procedures and policies depends on the business's type of activities and on risk of exposure to money laundering and terrorist financing. Currently, it is not

assessment of the money laundering and terrorist financing risks through regulations enacted in June 2007 and in force in June 2008.

specified in the PCMLTF Regulations that such procedures and policies should be written and kept up to date[117], even if this requirement is considered by FINTRAC as being implicit. OSFI specifies in its Guideline B-8 that "*policies and procedures should be formally documented*". IDA requires "*written anti-money laundering procedures*" in its non-binding "*Deterring money laundering activity*" Guide.

886. According to FINTRAC Guidelines, the business's policies and procedures must be communicated, understood and adhered to by any employee who deals with clients and their assets or who could be affected by the requirements under Part1 of the PCMLTFA and its Regulations. They need enough information to process and complete a transaction properly as well as to identify clients and keep records as required. They also need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering regimes consistent with international standards. Information about this, including updates to the list of NCCTs issued by the FATF is available on FINTRAC's website[118] and all of the advisories that FINTRAC has issued throughout the years can be found in the 'FINTRAC Advisories' section of the website[119]. Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and the entity itself.

Appointment of a Compliance Officer

887. Section 71 of the PCMLTF Regulations requires reporting entities to appoint a compliance officer who is responsible for the implementation of the compliance regime.

888. According to FINTRAC Guidelines, the compliance officer should have the authority and the resources necessary to discharge his or her responsibilities effectively. Depending on the type of business, the compliance officer should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator.

889. If the reporting entity is a small business, the appointed officer could be a senior manager or the owner or operator of the business. If the reporting entity is comprised of an individual, this person can appoint themselves as compliance officer or they may choose to appoint another individual to help them implement a compliance regime. In the case of a large business, the compliance officer should be from a senior level and have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed compliance officer in a large business should not be directly involved in the receipt, transfer or payment of funds.

890. For consistency and ongoing administration of the compliance regime, the appointed compliance officer may choose to delegate certain duties to other employees, for example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented and enforced at that location.

891. OSFI's Guideline B-8 states that the compliance officer should ensure that every division potentially exposed to money laundering or terrorist financing activities appoints an officer to ensure that these divisions implement their policies and procedures. These officers should report regularly on compliance issues and weaknesses in policies and procedures. The financial institution should also designate employees to be accountable for ensuring that policies and procedures intended for these branches are applied. The identification of the AML/CFT compliance officer (CAMLO) must be communicated to OSFI as part of the annual "OSFI-57: Return of Corporate Information" report (for domestic entities) and "OSFI-57A Return of Corporate Information (for foreign entities. In addition, an amended return must be filed disclosing the name of a new CAMLO should a new person be

---

117 The PCMLFT Regulations enacted on 27 June 2007 fill this gap. They require that compliance policies and procedures are written, approved by a senior officer and kept up to date (see Section 71 of the amended PCMLTF Regulations).

118 http://www.fintrac-canafe.gc.ca/intro-eng.asp.

119 http://www.fintrac-canafe.gc.ca/publications/avs/1-eng.asp.

appointed to the position during the year. OSFI Guideline B-8 advises that the CAMLO's mandate be enterprise-wide.

892. Other regulators of financial institutions in Canada have had similar requirements in place, that in some cases have preceded the PCMLTFA requirements. For example, every IDA member is required to designate its Chief Executive Officer, its President, its Chief Operating Officer or its Chief Financial Officer (or such other officer designated with the equivalent supervisory and decision-making responsibility) to act as an "Ultimate Designated Person", responsible for the conduct of the firm and employees. An "Alternate Designated Person" must also be approved to act as Chief Compliance Officer (see IDA By-Law No.38). Firms may be required to designate more than one Chief Compliance Officer depending on the scope and complexity of its business. Alternatively, the Ultimate Designated Person can also act as the Chief Compliance Officer. The responsibilities of the Ultimate Designated Person and Chief Compliance Officer include ensuring firm compliance with IDA and provincial Securities Act regulations, along with federal regulations, such as, the PCMLTFA.

893. Apart from the very generic wording in the FINTRAC Guidelines, there is no explicit requirement to ensure that the AML/CFT compliance officer has timely access to customer identification data and other CDD information, transactions records and other relevant information. The assessors were told that OSFI, in conducting its AML/CFT assessments, has never identified a situation where the CAMLO has not had timely access to all the information needed.

Review of the Compliance Policies and Procedures

894. Another component of a comprehensive compliance regime is a review of the reporting entity's compliance policies and procedures, as often as is necessary, to test their effectiveness.

895. Section 71 of the PCMLTF Regulations requires reporting entities to review their anti-money laundering and anti-terrorist financing policies and procedures "as often as necessary" to test their effectiveness by an internal or external auditor, or if there is no auditor, by the person or entity itself. FINTRAC's Guideline 4 provides a list of triggers that might suggest when a review is needed, such as changes in the legislation, the issuance of new products or services and non-compliance issues[120].

896. It is specified in FINTRAC Guideline 4 that the review is to be completed by an external or internal auditor, if the entity has one. It is indicated that the review could include interviews, tests and sampling. The scope and results of the review should be documented and deficiencies should be identified and reported to senior management or the board of directors. A request for a response indicating corrective actions and a timeline for the implementation of such actions must be sent with the report to senior management and both the request and the response should be documented.

897. FINTRAC's Guideline 4 also indicates that reporting entities must conduct a self-review when it is impossible to have an auditor. The person conducting the review has to be independent, "if feasible", of the reporting, record-keeping and compliance monitoring functions. The review has the same objectives as those conducted by an auditor and should be documented. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements. It should include corrective measures and follow-up actions.

898. The scope and details of a review will depend, according the FINTRAC's Guideline 4, on the nature, size and complexity of the operations of the reporting entity.

899. Thus, there is no actual requirement for an independent audit function to test AML/CFT regime compliance for small financial institutions (including small MSBs)for which a simple self-assessment is admitted. Moreover, the review of the AML/CFT compliance has to be performed only "as often as

[120] Amendments to section 71 will require, as of June 2008 that this review be conducted every two years.

necessary" and the methods to be used to perform the review (including sample testing) are only quoted in the FINTRAC Guideline as an indication.

900. OSFI's Supervisory Framework considers internal audit to be a key risk management function and assesses it accordingly during the review cycle. Moreover, pursuant to OSFI's Guideline E-13 - Legislative Compliance Management (LCM), FRFIs are obligated to implement a compliance management control on an enterprise-wide basis to ensure that they have the ability to meet all regulatory requirements.

901. OSFI Guideline B-8 states that the independent audit of the AML/CFT Compliance Program should be conducted annually. The Guideline indicates that the review of the business's AML/CFT program should encompass three processes. First, FRFIs have to establish an internal compliance reporting process, which should demonstrate at a minimum conformity with all AML and CFT requirements. It should also review regularly compliance issues and identify and document any weaknesses. These weaknesses shall be reviewed with OSFI.

902. The second process is an annual self-assessment, which must evaluate on a group-wide basis the effectiveness of the AML/CFT procedures to identify the areas and types of risks and suggest corrective measures to address weaknesses and gaps in the risk management system. The results must be reported to senior management and the board of directors. The document should contain the scope of the review, the main elements of policies and procedures, as well as the extent to which policies and procedures comply with the PCMLTFA and its Regulations and OSFI's Guidelines.

903. The last process consists of independent procedures testing to be conducted by the internal audit department, compliance department, or by an outside party such as an external auditor. The testing must cover the entire operation of the entity and must be performed at least annually. The results should be documented and reported to senior management and the board of directors. The report should not only include steps to be taken to address weaknesses and gaps, but could also address areas such as the employees' knowledge of policies and procedures, systems for client identification, large cash transaction and suspicious transactions identification and reporting, and record keeping.

904. Together, the annual self-assessment and independent procedures testing, coupled with LCM requirement, create a control environment which, if implemented effectively, will identify weaknesses or compliance deficiencies in a timely fashion and permit corrective measures to be taken by the financial institutions' senior management and boards of directors. To reinforce the importance of a strong control framework, evidenced through measures such as policies, procedures and other controls, OSFI held information sessions for the industry on November 9, 2005 and October 17, 2006.

905. Other regulators of financial institutions in Canada require similar policies and procedures. In the securities industry for example, IDA By-law 29.27 requires member firms to establish and maintain internal procedures, policies and controls, including compliance procedures for monitoring and reporting adherence to all laws, rules, regulations, requirements, policies and procedures governing their business. The broad scope of the requirement covers AML/CFT laws and regulations. IDA members must establish a compliance monitoring system to prevent and detect violations, that includes a procedure for reporting results of its monitoring efforts to management and, where appropriate, the Board of Directors or its equivalent. Under IDA By-law 38 IDA the Chief Compliance Officer must, at a minimum, report annually to the Board of Directors or its equivalent on the state of compliance at the dealer. The Board of Directors is subsequently required to review the report and determine necessary actions to address any compliance deficiencies noted in the report. Another example can be found in Quebec where the designation of a Compliance Officer (CO) is required by Québec securities regulation and the compliance officer must have access to all necessary information to carry out his function.

906. Furthermore IDA "*Deterring money laundering activity*" Guide specifies that "except for very small firms", the audit should be at least annual and that firms should keep records of measures taken to correct any weaknesses identified in the audit.

Ongoing Compliance Training

907. Section 71 of the PCMLTF Regulations requires every reporting entity to provide ongoing training to their employees, agents or any other person authorised to act on behalf of the business.

908. As further explained in FINTRAC's Guideline 4, reporting entities must not only develop compliance policies and procedures, but ensure that these policies and procedures are understood by all employees within the organization and agents who have contact with customers, who see customer transaction activity, or who handle cash in any way understand the reporting, client identification and record-keeping requirements. This includes those at the front line as well as senior management. In addition, others who have responsibilities under the compliance regime, such as information technology and other staff responsible for designing and implementing electronic or manual internal controls should receive training. This could also include the appointed compliance officer and internal auditors.

909. Reporting entities must address standards for the frequency and method of training, such as formal, on-the-job or external. New people should be trained before they begin to deal with customers. All should be periodically informed of any changes in anti-money-laundering or anti-terrorism legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs. Those who change jobs within the organization should be given training as necessary to be up-to-date with the policies, procedures and risks of exposure to money laundering or terrorist financing that are associated with their new job.

910. The method of training may vary greatly depending on the size of the business and the complexity of the subject matter. The training program for a small business may be less sophisticated and not necessarily formalized in writing. In line with FINTRAC guidelines and when assessing training needs, a reporting entity should consider the following elements:

- *Requirements and related liabilities:* the training should give those who need it an understanding of the reporting, client identification and record-keeping requirements as well as penalties for not meeting those requirements.
- *Policies and procedures:* the training should make the entity's employees, agents, or others who act on its behalf aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing that are associated with their jobs. It should also give each one a clear understanding of his or her responsibilities under these policies and procedures and of how their institution, organization or profession is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities. Training should include examples of how the entity's particular type of organization could be used to launder illicit funds or fund terrorist activity.
- *Background information on money laundering and terrorist financing*: any training program should include some background information on money laundering so everyone who needs to understand what money laundering is, why criminals choose to launder money and how the process usually works. They also need to understand what terrorist financing is and how that process usually works. FINTRAC makes material available on its website that can provide help with training.

911. OSFI's Guideline B-8 further stipulates that employees of FRFIs should receive sufficient training. This training must encompass the policies and procedures of the entity, the techniques used by money launderers in financial institutions and current AML/CFT legislation and regulation. Special attention must be given to front-line staff.

912. When OSFI undertakes AML/CFT assessments it reviews the material produced by each financial institution to train its staff. The assessors were told that employee knowledge is ascertained through interviews, during on-site reviews and assessing the account opening process. It is expected that all new employees receive adequate training before dealing with customers and that continuing employees receive training appropriate to their responsibilities at least on an annual basis. In this regard, a number of recommendations and requirements have been given to improve the AML/CFT training given by financial institutions to assist employees in understanding money laundering and terrorist financing and its consequent reporting processes.

913. AML/CFT requirements have been included in the IDA's mandatory courses for those dealing with the public or holding supervisory positions. Those courses touch on conduct and practices handbook for securities industry professionals, partners, directors and senior officers' examination, branch managers' course and chief compliance officers course (under development).

914. In addition to mandatory courses, the IDA has a mandatory continuing education program and sets guidelines for acceptable continuing education course content, length and rigor (see IDA Policy 6). The guidelines recommend a process to aid firms in identifying appropriate suppliers and courses. The IDA requires that certain persons successfully complete a compliance course within a three-year cycle. These courses must review critical regulations and application, regulatory changes, rules relating to new products and ethics. Anti-money laundering laws and regulations and their implementation at the member is highlighted in the IDA Policy 6. As part of the audit process, the IDA will review member-developed compliance courses to ensure they satisfy the guidelines. IDA member firm AML/CFT training is reviewed during the IDA's sales compliance audits.

Screening procedures when hiring employees

915. There is currently no general enforceable requirement for Canada's financial institutions to screen candidates for employment.

916. Under OSFI's Supervisory framework, the FRFI's senior management and/or the board of directors are responsible for planning, directing and controlling the strategic direction and general operations. One of their key responsibilities includes developing sound business practices, culture and high ethical standards within the financial institution that help protect its reputation. This is primarily achieved by the developing of sound human resource policies associated with staff selection, hiring, retention, conflict of interest and code of conduct. As such, it is in the best interest of senior management and the board at the financial institutions to adopt appropriate and relevant screening procedures when hiring employees to ensure that potential employees have high ethical standards so as to minimize exposure by the financial institution or its clients to potential abuses or reputational risks issues. Consequently, as part of its supervisory role and in assessing the board and senior management control functions, OSFI would expect them to have adopted appropriate screening procedures at the financial institution to ensure high standards when hiring potential new employee. In this respect, OSFI has issued a draft Guideline (E-17) outlining principles to assist FRFIs in establishing policies and procedures regarding the conduct of assessments of their Responsible Persons (*i.e.* directors, senior officers, principal officers, chief agent or any person playing a significant role in the management of the financial institution) upon their initial appointment and at regular intervals. This Guideline will nevertheless remain limited to responsible persons and will not concern all employees.

917. As a practice, Canada's largest banks screen all new potential employees to determine if they have criminal records. Such screening is made possible by a Memorandum of Understanding between the Canadian Bankers Association and the RCMP. In addition, participating banks can screen the names of potential employees against a list of previous bank employees who may have been dismissed by another participating bank for undertaking unethical activities against the bank or its client.

918. The IDA also oversees the professional standards and educational programs that ensure the competence of securities industry employees. The IDA screens all investment advisors employed by

member firms to ensure that those entering the industry are of good character and have successfully completed all the required educational courses and programs. The IDA requires that member firm employees who deal with the public interest must be licensed. The IDA does this more as part of its mandate to protect the public interest and the integrity of the capital markets rather than as a service to members. The IDA has good access to information that its members may not have, such as reports from previous employers and occasionally other confidential information.

Recommendation 22

919. Section 15(4) of the Bank Act states that "subject to this Act, a bank has the capacity to carry on its business, conduct its affairs and exercise its powers in any jurisdiction outside Canada to the extent and in the manner that the laws of that jurisdiction permit." A similar provision is set out in the Insurance Companies Act (Section 15.4). However, Canadian financial institutions and any branches or subsidiaries are generally subject to the laws of the jurisdiction in which they are incorporated. The assessment team believes that the provisions as set out in the Bank Act and in the Insurance Companies Act are insufficient to address the specific requirements in the context of Recommendation 22.

920. Currently, the PCMLTFA and PCMLTF Regulations contain no specific enforceable provision requiring financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements[121]. There is no legal obligation in the PCMLTFA and PCMLTF Regulations that, where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (*i.e.* host country) laws and regulations permit. Equally, there is no requirement that financial institutions be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (*i.e.* host country) laws, regulations or other measures.

921. As the home regulator, OSFI already expects FRFIs with international operations to implement enterprise-wide policies consistent with the Core Principles. One such policy would relate to the implementation of an enterprise-wide AML/CFT Programme, as outlined in its Guideline B-8. As such, OSFI expects the international operations of financial institutions to implement policies and procedures consistent with the domestic financial institutions enterprise-wide standards - regardless of whether the country is an FATF member or not.

922. The one exception to this would be where the AML/CFT standard in a particular jurisdiction is higher than or in addition to the enterprise-wide standard. Under those circumstances OSFI would expect the international operation in the particular jurisdiction, whether the operation is a branch of a domestic financial institution or a separate legal subsidiary, to implement AML/CFT standards that go beyond the enterprise-wide or group standards.

923. Moreover, Guideline B-8 states that FRFIs should ensure that subsidiaries having potential exposure to money laundering or terrorist financing activities follow the guideline.

924. OSFI examinations in financial institutions are performed on all parts of the FRFIs' enterprise-wide operations, including branches and subsidiaries located outside Canada. Deficiencies in any subsidiary or branch of the financial institution have been subject of deficiency letters by OSFI, or can trigger the issuance of a direction of compliance if the deficiency amounts to the commission of an unsafe or unsound practice in conducting the business of the institution. With respect to subsidiaries, OSFI's usual practice is to share any identified material weaknesses with host regulators. Furthermore, OSFI shares the results of its AML/CTF examinations with FINTRAC (except for information

[121] Some provisions in relation to Recommendation 22 have been adopted in the PCMLTFA in December 2006. They will enter into force in June 2008.

pertaining to non-Canadian subsidiaries) who, in turn, has the ability to impose legal sanctions with respect to compliance deficiencies.

925. To date OSFI has undertaken 6 separate reviews of the international operations of Canadian domestic banks to verify that AML/CFT policies and procedures are being implemented on an enterprise-wide basis.

3.8.2 Recommendations and Comments

926. *Recommendation 15.* The current requirements should be expanded, made more explicit and enforceable, in particular:

- Written policies and procedures should be explicitly required, and should be kept up to date, and their minimum mandatory content should include the detection of unusual and suspicious transactions.
- There should be an explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information.
- The requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened for MSBs and small financial institutions, and made more explicit generally.
- Canada should impose screening procedures when hiring employees for financial institutions.

927. *Recommendation 22*. Canada should ensure that the provisions in relation to Recommendation 22 that will enter into force in June 2008 are in line with the FATF requirements and are properly implemented by all financial institutions.

3.8.3 Compliance with Recommendations 15 & 22

Rec.	Rating	Summary of factors underlying ratings
Rec.15	LC	• The requirement for internal controls does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). • There is no mandatory explicit requirement to maintain up to date internal procedures, policies and controls and such policies do not include the detection of unusual and suspicious transactions. • There is no explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information. • There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance for small financial institutions (including some MSBs) for which a simple self-assessment is admitted. • There is no general requirement concerning screening procedures when hiring employees.

Rec.	Rating	Summary of factors underlying ratings
Rec.22	NC	• Currently, the PCMLTFA and PCMLTF Regulations contain no explicit provision requiring financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements although foreign branches of Canadian financial institutions are Canadian entities under the Bank Act and the Insurance Companies Act that are subject to Canadian laws. • There is no requirement that particular attention be paid to branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendations. • There is no legal obligation in the PCMLTFA and PCMLTF Regulations that, where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (*i.e.* host country) laws and regulations permit. • There is no requirement that financial institutions be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (*i.e.* host country) laws, regulations or other measures.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

Establishment or continued operations of shell banks

928. The Bank Act does not permit the incorporation of a shell bank since all banks operating in Canada must have a physical presence. All banks incorporated in Canada must be listed in Schedule I or Schedule II of the Bank Act and such a listing must always include a reference to the place in Canada where the head office is situated. Section 237 of the Bank Act also provides that a bank incorporated in Canada must have, at all times, a head office within Canada that is specified in either the Bank's incorporating instrument or its by-laws.

Correspondent banking relationships with shell banks

929. Legislative amendments enacted in December 2006 and regulatory amendments that were brought into force on 30 June 2007 specifically address the issue of shell banks in Canada's AML/CFT legislative and regulatory texts. Section 9.4(2) of the PCMLTFA specifically prohibits Canadian financial entities from entering into a business relationship with shell banks. There is no prohibition to continue business relationships with shell banks.

930. Prior to these legislative changes, financial regulators had issued guidance and regulations in this area. OSFI, for example, has been providing guidance to all banks and federally regulated trust and loan companies in the area of correspondent banking since 2002. OSFI Guideline B-8 ''encourages FRFIs to pay special attention to business relationships with shell banks and to adopt measures that will ensure that they do not enter into correspondent banking relationships with shell banks''. The practice was first communicated in guidance sent to banks and trust and loan companies on February 22, 2002 encouraging them to adopt measures to ensure that they do not enter into correspondent banking relationships with shell banks and added to Guideline B-8 when it was subsequently revised. In the securities sector, the IDA has had a regulation in place since 2004 that prohibits member securities dealers from dealing with shell banks, with an exception for affiliates of banks subject to a suitable regulatory regime in their home jurisdiction.

931. It should be noted that as part of its assessment of a bank's correspondent banking business, OSFI verifies that the bank has adopted in writing such controls against dealing with shell banks and that it does not have any correspondent banking relationships with shell banks.

Possible use of respondent financial institutions accounts by shell banks

932. Under the December 2006 PCMLTFA provisions that entered into force on June 30, 2007, there is a compulsory requirement for financial institutions to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks. Section 15 of the PCMLTF Regulations adopted on June 27, 2007 and in force since June 30, 2007 requires every financial entity that enters into a correspondent banking relationship to obtain a statement from the foreign financial institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks.

933. The assessors were advised that when OSFI reviews the files of the correspondent accounts, it expects to see evidence that the bank has conducted enhanced due diligence in managing the money laundering and terrorist financing risks associated with correspondent banking activities. OSFI looks for evidence that the bank has requested information and documentation from the respondent bank that verifies, among other things, that the respondent is a regulated bank, is not a shell bank and does not deal directly or indirectly with shell banks. The assessment team was told that OSFI has never encountered instances where one of its regulated institutions had correspondent relationships with a shell bank.

3.9.2 Recommendations and Comments

934. Canada should adopt a requirement for financial entities to terminate business relationships with shell banks as well as with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. Canada should ensure that the measures adopted in relation to shell banks are fully implemented by financial institutions.

3.9.3 Compliance with Recommendation 18

Rec.	Rating	Summary of factors underlying ratings
Rec.18	LC	• Financial entities are not required to terminate business relationships with shell banks, nor with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. • The effectiveness of the measures in place cannot yet be assessed.

Regulation, supervision, guidance, monitoring and sanctions

3.10 Supervision and oversight (R. 23, 30, 29, 17, 32, & 25)

3.10.1 Description and Analysis

Authorities/SROs roles and duties & Structure and resources - R.23, 30

General

935. The overall Canadian supervisory regime is complex due to the federal and provincial structure of government. However, AML/CFT compliance is in principle straightforward as FINTRAC is solely responsible. In order to assist it, FINTRAC has signed MOUs with certain regulators or supervisors to share information. In addition to this, some regulators have provisions under their own legislation or codes of conduct that impose similar requirements to, or which complement the key provisions in the PCMLTFA through separate enforcement powers (for example, OSFI advises FRFIs to have proper due diligence procedures; IDA requires securities dealers to properly identify beneficial owners). FINTRAC supervision provides the minimum standard; however, having regard to all the elements, it is not easy to get a complete overview of the supervision of AML/CFT compliance that is being applied in practice to each category of financial institution.

936. It is worth mentioning that the financial sectors which are currently not covered by the PCMLTFA (see Section 3.1 of the report) are generally subject neither to specific regulation nor to prudential supervision concerning AML/CFT issues. For example, for financial leasing, the industry is

represented by the Canadian Leasing and Finance Association (CLFA) which provides information on the industry and input into the policy-making process, but does not provide any regulatory oversight. Membership in the CLFA is voluntary. As stated above, it is only on a voluntary basis that some finance companies have decided to comply with minimum AML/CFT standards and they are not subject to any supervision in that area.

937. The following table generally summarizes the list of existing regulators per reporting entities:

Reporting Entities	Number of reporting Entities	Sector Particularities	Primary Regulator	AML/CFT Regulator
Banks	71	Biggest six hold 90% of assets	OSFI	FINTRAC
Credit unions and *caisses populaires*	1 250	Majority located in Quebec	Provincial authorities (*e.g.* AMF in Quebec)	FINTRAC
Life insurance companies	105 - federal 33 - provincial	Five largest are federally regulated and handle 64% of net premiums	OSFI - 90% of firms Provincial authorities - 10% of firms	FINTRAC
Life insurance brokers and agents	73 000	A significant number work for insurance companies	Provincial authorities (*e.g.* AMF, FSCO)	FINTRAC
Trust and Loan companies	81	Largest are banks' subsidiaries	OSFI and some provinces[1]	FINTRAC
Investment dealers firms[2]	208	Biggest 11 firms hold 71% of revenues. 6 of these are owned by the largest banks	IDA	FINTRAC
Mutual Fund dealers firms[2]	197	Only deal in mutual funds. Many of the largest are owned by the large banks.	MFDA AMF in Quebec	FINTRAC
Investment Counsel and Portfolio Management firms[2]	397	Activities limited to providing investment advice and counselling	Provincial authorities (*e.g.* AMF and OSC)	FINTRAC
Other securities firms[2]	309	Limited trading in securities	Provincial authorities (*e.g.* AMF and OSC)	FINTRAC
Money service businesses	700	A few large firms cover the large majority of the market	None	FINTRAC

Notes:

1 Ontario only permits the operation of federally regulated trust companies.

2 Some 90 000 securities participants are licensed/registered to sell securities in these firms and are subject to AML/CFT requirements.

OSFI: Office of the Superintendent of Financial Institutions.

AMF: L'Autorité des marchés financiers du Québec.

OSC: Ontario Securities Commission.

FSCO: Financial Services Commission of Ontario.

IDA: Investment Dealers Association of Canada.

MFDA: Mutual Fund Dealers Association of Canada

938. The basis on which the regulators (excluding FINTRAC) perform AML/CFT compliance supervision varies from one organization to another, as they are not specifically mandated by law to ensure compliance with PCMLTFA/PCMLTF Regulations:

- OSFI, for instance, as the prudential regulator of federal financial institutions is primarily concerned with ensuring safety and soundness which are key elements in its supervisory interventions in the AML/CFT area. If OSFI determines that a FRFI has failed to implement AML/CFT requirements in a manner that amounts to the commission of an unsafe or unsound practice it can apply a full range of supervisory enforcement actions including a "Direction of Compliance". It has adopted AML/CFT guidance (Guideline B-8) to help FRFIs to comply

with the various legal requirements. Failure to comply with B-8 gives rise to recommendations aimed at strengthening risk management controls.

- Under various provincial Acts governing financial institutions, compliance with federal law and regulation is a condition for obtaining and keeping a license. Thus regulators, even if they do not have direct jurisdiction to administer the PCMLTFA, are entitled to verify that the entities they supervise comply with it as they have, in a number of cases, the mandate to ensure compliance with any federal or provincial legislation. But some actually do not look specifically at those aspects in their compliance regime or look at it in a very cursory and limited way: for instance, average time spent by DICO, which is in charge of the supervision of credit unions in Ontario, to the review of AML/CFT compliance (*i.e.* the review of the financial institution report to FINTRAC) is two hours per inspection. Alberta Securities Commission compliance officers look only at the existence of procedures and policies but would not make sample testing to assess their effectiveness. For its part, FSCO, the Ontario provincial regulator for life insurance companies (4 provincially regulated) and agents[122], which has a memorandum of understanding with OSFI for the supervision of the four Ontario life insurance companies does not perform any on-site review for AML/CFT purposes in the other entities it supervises. Another example of limited on-site reviews performed by the provincial regulator is the control exercised by the AMF, the provincial regulator of Quebec of the *caisses populaires* of the Desjardin group, as it relies mainly on the controls performed by the Federation itself on its member entities.

- Other regulators, such as the IDA for investment dealers, have issued code of conducts or mandatory regulations establishing standards comparable to or higher than PCMLTFA and control the compliance of reporting entities with these standards.

939. Thus the role of the different regulators and SROs regarding the control of AML/CFT compliance may differ considerably, and, depending on their different levels (and in some cases absence) of involvement in that area, the different financial sectors are subject to disparate degrees of supervision for AML/CFT purposes.

940. The MSBs sector which comprises 700 identified reporting entities and possibly more than 20 000 branches or agents is only supervised by FINTRAC. FINTRAC has given priority to inspections in this sector after commencing its compliance reviews and has covered about 300 entities during the last four last fiscal years.

941. FINTRAC has entered in agreements with 12 regulators and SROs in the financial sector to exchange AML/CFT supervisory information, the most recent having been signed in February 2007. Information provided by these regulators to FINTRAC feeds into FINTRAC's risk assessment.

942. In general, under the MOUs, the regulators provide FINTRAC with the following information regarding their activities related to the compliance of the entities they regulate with the PCMLTFA: lists of entities that they plan to examine; a copy of their compliance review program; results of compliance reviews undertaken; copies of correspondence regarding deficiencies; descriptions of actions the regulator has required to be taken to correct deficiencies; and descriptions of corrective actions taken by entities.

943. The following table describes FINTRAC's MOU partners in the financial sector, the entities supervised by the regulator, and the process undertaken by the given regulator to carry out AML/CFT inspections.

[122] The definition of agents in the Insurance Act of Ontario is intended to capture all conduct for someone placing business with a life insurance company, whether the person is appointed by an insurance company or he/she is acting on behalf of the consumer.

Region	Regulator	Number of FIs Supervised by the Regulator	Regulator AML/CFT Inspections Methodology
Canada	Office of the Superintendent of Financial Institutions	71 Banks 46 Trust Companies 22 Loan Companies 96 Life Ins. Companies	Detailed exams in all sectors Risk based Examine one-quarter of regulated entities annually
Canada	Investment Dealers Association of Canada	208 securities firms	Risk based. One-third annual coverage.
British Columbia	Financial Institutions Commission of British Columbia (FICOM)	53 Credit Unions 2 Life Ins. Companies, 5 500 agents 7 Trust Companies	Risk & random. No set examination program with exams primarily selected by weaknesses identified in risk management system
Manitoba	Credit Union Deposit Insurance Corporation	58 Credit Unions	Risk based. 25% annual exam coverage
New Brunswick	New Brunswick Office de stabilisation de la Fédération des caisses populaires acadiennes	33 *Caisse Populaires*	Risk & random. All entities examined within 18-month exam cycle
New Brunswick	New Brunswick Department of Justice, Insurance Branch	2 Life Ins. Companies	Random, 3-year exam cycle
Newfoundland	Credit Union Deposit Guarantee Corporation of Newfoundland and Labrador	13 Credit Unions	All entities examined within a 2-year cycle
New Brunswick	New Brunswick Credit Union Federation Stabilization Board	23 Credit Unions	Risk & random. All entities examined within 18-month exam cycle
Nova Scotia	Nova Scotia Credit Union Deposit Insurance Corporation	34 Credit Unions	Risk & random, with each entity examined in 18-month cycle
Ontario	Deposit Insurance Corporation of Ontario	221 Credit Unions & *Caisses populaires*	Risk based, currently being refined. Conduct apprx. 70 exams annually, with 15-20 targeted
Québec	L'Autorité des marchés financiers du Québec	300 securities firms 600 *Caisses populaires* 28 Life Ins. Companies	Risk based
Saskatchewan	Saskatchewan Credit Union Deposit Guarantee Corporation	88 Credit Unions	Risk based, annual exams of each entity

944. FINTRAC provides these regulators with information related to the risk assessment undertaken by FINTRAC, results of FINTRAC's compliance actions and copies of correspondence between FINTRAC and the supervised entities.

945. It is to be noted that FINTRAC does not delegate its supervisory role through MOUs to other regulators. Information obtained by other regulators through their own supervisory activities, including examinations, is provided to FINTRAC under the MOU and is taken into consideration by FINTRAC during its risk assessment process. In addition to the audits and examinations performed by the regulators under their own supervisory framework, the results of which, with respect to AML/CFT relevant issues are provided to FINTRAC, FINTRAC conducts examinations in each sector, whether or not it is covered by an MOU. In fact, FINTRAC has conducted examinations in every sector covered by the PCMLTFA with the exception of financial institutions supervised by OSFI since FINTRAC fully relies on OSFI to conduct AML/CFT compliance initiatives.

946. Sanctions available under the PCMLTFA can only be administered by FINTRAC (see below-Recommendations 17 and 29).

947. In conclusion, beyond the centralized role of FINTRAC, it has been difficult for the assessment team to have a completely reliable overview of the efficiency of the supervision of AML/CFT compliance, except at the federally regulated level.

948. These preliminary remarks and observations will be illustrated and further developed in the following parts of this section, describing some of the main features and participants in the AML/CFT regime. The assessment team has opted for a sample approach whereby the AML/CFT supervision carried out by FINTRAC, OSFI and IDA, being the principal players, will be developed in more depth and detail when compared with the supervisory regimes implemented by SROs or provincial regulators where detailed and comprehensive information is not so readily available.

Overview of the main regulators acting in the AML/CFT area (with the exception of FINTRAC)

OSFI

949. OSFI is the prudential regulator for all banks, federally regulated trust and loan companies, federally regulated insurance companies, cooperative retail associations and cooperative credit associations and is given its responsibilities and authority by the OSFI Act and federal financial institution legislation.

950. FRFIs supervised by OSFI are subject to prudential regulation through legislated authorities and powers provided in the Bank Act, the Trust and Loan Companies Act, the Insurance Companies Act, and the Cooperative Credit Associations Act. The Office of the Superintendent of Financial Institutions Act provides the Superintendent with authority to assess controls designed to ensure that each FRFI is operated in a safe and sound manner and complies with its governing statute.

Securities regulators

951. *General*. The regulation of the securities industry is under provincial and territorial jurisdiction and is carried out through provincial/territorial securities regulatory authorities (SRAs). Self-regulatory organizations (SROs) and market infrastructure entities, such as exchanges and clearing agencies, supplement direct regulation by the SRAs in Canada's ten provinces and three territories. All SROs and market infrastructure entities set and enforce requirements that restrict access to the securities markets; however, some are for-profit organizations, others are not, and some have competitors while others are monopolies. The Canadian securities regulatory regime relies on these organizations and entities to help protect investors and promote fair, efficient and competitive capital markets. They develop standards of practice and business conduct, monitor their members' or participants' compliance with these standards and take appropriate enforcement actions against those who violate these requirements.

952. The current regulatory regime provides for parallel regulation of members and participants of these organizations and entities. For instance, SRAs make general rules for dealers, while SROs make rules that are consistent but may be more restrictive on the same subject matter; therefore, both SRAs and SROs may take enforcement actions against members. Some provinces and territories have delegated certain powers under their securities legislation to the SROs, such as registration and compliance[123].

953. Since there are different types of SROs and market infrastructure entities with varying functions and purposes, the nature and degree of the reliance of securities regulators on them may vary. For example, they rely heavily on certain SROs, such as the Bourse de Montréal Inc. (Bourse)[124], the

[123] The Alberta Securities Commission, the British Columbia Securities Commission and the Ontario Securities Commission have delegated certain registration functions to the Investment Dealers Association of Canada. The Autorité des marchés financiers (Québec) delegated registration and inspection functions and powers to the Investment Dealers Association of Canada.

[124] The Bourse is an exchange and also a recognized SRO in Quebec.

Investment Dealers Association of Canada (IDA), the Mutual Fund Dealers Association of Canada (MFDA) and Market Regulation Services Inc. (RS) to perform front-line regulatory functions.

954. The principle of reliance on SROs is well entrenched in Canadian securities legislation, for example, through explicit authorisation for the SRAs to recognize SROs[125]. In order to ensure the on-going reliance is appropriate, SRAs conduct regular oversight of SROs to evaluate their effectiveness, to confirm that they are acting in the public interest and to ensure that any conflicts of interest between the public and their members/users and any conflicts among members/users are properly managed. Legislation in many jurisdictions outlines this responsibility when regulators rely on SROs[126].

955. *IDA.* The IDA is a provincially recognized SRO in all provinces[127]. Recognition is done through an order of the SRA in the Province, generally subject to conditions set forth in or with the order. The IDA is the front-line regulator of investment dealers and a number of provisions in provincial securities regulations recognize IDA rules as an alternative to provincial regulations, generally by explicitly granting or allowing the granting of exemptions from the provincial rules to members who abide by IDA rules.

956. *MFDA.* The MFDA, established in June 1998, is the national SRO for the distribution side of the Canadian mutual fund industry. The MFDA regulates the operations, standards of practice and business conduct of its members and their representatives with a mandate to enhance investor protection and strengthen public confidence in the Canadian mutual fund industry. In general, the MFDA has a similar regulatory regime as the IDA, which includes rules and detailed requirements MFDA members must comply with, including particulars respecting business structures, capital requirements, insurance, books and records, client reporting, and business conduct. Subject to limited exceptions (for example, for firms for whom the mutual fund business is incidental to their primary business of advising), in British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick and Nova Scotia, a mutual fund dealer must be a member of the MFDA[128].

957. *OSC.* The following provides examples where SRAs regulate registrants directly. These examples pertain specifically to the case of securities regulation in the largest province, Ontario, by the Ontario Securities Commission (OSC).

958. Investment Counsel/Portfolio Managers (IC/PMs). This is the largest category of registrants reviewed directly by the OSC. IC/PMs have discretionary investment authority over client funds. The OSC considers them to be low risk for AML/CFT purposes since most advisers do not have access to client funds, trades are executed through an IDA member and assets are held by a custodian. As a result, the OSC only reviews policies and procedures relating to compliance with money laundering legislation and does only limited substantive testing such as the client identification procedures as part of its know-your-client testing procedures. To the extent that the policies and procedures are deficient,

---

125 For example, section 2.1 of the *Securities Act* (Ontario) states, in part, that "In pursuing the purposes of this Act, the Commission shall have regard to the following fundamental principles: ... 4. The Commission should, subject to an appropriate system of supervision, use the enforcement capability and regulatory expertise of recognized self-regulatory organizations". Section 21.1 of the Securities Act (Ontario) sets out the statutory authority to recognize SROs.

126 For example, section 2.1 of the Securities Act (Ontario) sets out the principle of "an appropriate system of supervision." Subsection 21.1(4) provides that "the Commission may, if it is satisfied that to do so would be in the public interest, make any decision with respect to any by-law, rule, regulation, policy, procedure, interpretation or practice of a recognized self-regulatory organization." Subsection 21.7(1) allows the Ontario Securities Commission to hear appeals from "a direction, decision, ruling or order" made by a recognized SRO.

127 With the exception of Prince Edward Island which has no authority in its Securities Act to recognize a SRO and there is a pending recognition application with New Brunswick.

128 While the MFDA is not formally recognized as an SRO by the *Autorité des marchés financiers* (AMF), it has entered into a co-operative agreement with the AMF and actively participates in the regulation of mutual fund dealers in Québec.

the OSC issues a deficiency notice as part of its field review deficiency report and provides a copy of the deficiency notice to FINTRAC periodically.

959. Scholarship Plan Dealers (SPDs). SPDs are relatively low risk for AML/CFT purposes because they deal with relatively small amounts of money from a large numbers of investors. Given the nature of the scholarship plans, the risk of money laundering was considered low. Money is locked in for a number of years. Although the money can eventually be withdrawn, only the amount net of enrolment fees would be returned.

960. Limited Market Dealers (LMDs). In Ontario, there are approximately 550 LMDs engaged in the business of selling "exempt" securities to accredited investors. The majority of LMDs do not receive money from clients. Client cheques are payable directly to the issuer of a security. In January 2006, 78 of those LMDs were registered both as mutual fund dealers and LMDs and therefore were subject to on-site compliance reviews by MFDA. LMDs are subject to on-site compliance reviews of OSC.

Credit Unions regulators

961. All credit unions and *caisses populaires* are provincially incorporated and almost exclusively regulated at the provincial level. The legislative and regulatory framework for credit unions and *caisses populaires* generally run parallel to that of federal financial institutions, such as banks. In addition, the provinces provide deposit insurance for members of credit unions or *caisses populaires*.

962. *Regulation in Ontario.* The Financial Services Commission of Ontario (FSCO), an arm's-length agency of the Department of Finance, regulates registration of credit unions and *caisses populaires* under the Credit Unions and *Caisses Populaires* Act, 1994. The Deposit Insurance Corporation of Ontario (DICO) has signed a Letter of Understanding (LOU) with the FSCO. DICO is responsible for conducting onsite verifications and reviews and copies of all on-site examinations reports are shared with FSCO.

963. *Regulation in Quebec*. The Autorité des marchés financiers (AMF), the integrated supervisor in Quebec, regulates *caisses populaires*, securities firms and insurance companies and agents, regulates *caisses populaires* under an Act respecting financial services cooperatives. Under this Act, the Desjardins federation, the joint supervisor of the *caisses populaires* with the AMF, must inspect the internal affairs of each *caisse populaire*, including that AML/CFT requirements are being followed, at least once every 18 months and must transmit to the AMF its findings.

Insurance regulators

964. Canadian insurance companies can be either federally or provincially incorporated. Branches of foreign insurance companies are regulated at the federal level only. Federally incorporated regulated life insurance companies dominate Canada's life and health sector. At the end of 2005 there were about 107 active life insurance companies operating in Canada and out of these, some 80 (which includes 30 foreign branches) were federally regulated, generating almost 92% of total life and health premium income. In addition the 3 largest federally regulated insurance companies and their life insurance subsidiaries account for 81% of the life and health sector's assets.

965. OSFI also prudentially supervises provincially chartered life companies regulated by three provinces; Manitoba, Ontario and New Brunswick under MOUs with those provinces. In 2005 these MOU's together cover 6 provincial companies. The remaining active provincial life insurers were incorporated in Quebec (17), British Columbia (2) and Alberta (1).

966. *Provincial Regulation*. In Ontario, FSCO licenses and regulates insurers that sell life and health insurance in the province of Ontario to ensure they comply with the provincial market conduct legislation. Life and health insurance products are sold to consumers directly by companies or through insurance agents. In Québec, the Autorité des marchés financiers supervises life insurers while the Chambre de la sécurité financière oversees insurance agents.

Recommendation 30 (Structure and resources of the supervisory authorities)

967. Due to the number of existing supervisors and regulators liable to intervene in the area of AML/CFT, a complete overview of their resources and efficiency would be quite complex, so for the purpose of this report, only the principal authorities, namely, FINTRAC, OSFI and IDA will be assessed in more detail.

968. With regard to the level of resources made available to the different supervisory authorities, there are contrasting situations. Generally, FINTRAC, as the primary regulator specifically empowered with ensuring compliance with PCMLTFA has resources that are too limited to ensure proper supervision in the AML/CFT area. It has to rely on other primary regulators in a number of cases (securities dealers, FRFIs, credit unions, etc.) who themselves do not always have sufficient resources to dedicate to the task.

969. Professional standards applicable to the staff of the main regulators and supervisors are quite comprehensive. The quality and frequency of training for combating ML and TF are also satisfactory as far as FINTRAC, OSFI and IDA are concerned. Again, the assessors believe that training of FINTRAC staff is essential to carry out properly its supervisory responsibility in a very diverse range of businesses.

FINTRAC

970. *Resources*. In its budget of May 2006, the Government of Canada announced its priority to bolster existing capacity to combat money laundering and terrorist financing by providing incremental resources to FINTRAC in the amount of CAD 16.2 million and 102 employees. FINTRAC has a total of 233 employees (as of September 30, 2006) and a current budget of almost CAD 51 million.

971. Although the total headcount may seem adequate, the deployment of staff between the different FINTRAC departments appears to be unbalanced, with the bulk being dedicated to IT management (FINTRAC was created as an FIU that would rely heavily on technology) and comparatively fewer human resources assigned to AML/CFT inspections, especially if compared with the vast number of entities that are subject to supervision.

972. Within FINTRAC, Regional Operations and Compliance (ROC), is responsible for the development, implementation and monitoring of the national compliance program. This includes interpreting policy and regulations, providing advice and assistance to reporting entities; conducting risk assessment and examinations; monitoring data quality, timing and volume; providing feedback to reporting entities; making disclosures of non-compliance to law enforcement; conducting regional liaison with disclosure recipients (*i.e.* law enforcement agencies); and developing and implementing new programs.

973. ROC is comprised of the Compliance and Program Development Units in Ottawa and three regional offices with responsibilities for compliance and for liaison with law enforcement. The Western regional office in Vancouver covers British Columbia, Alberta, Saskatchewan, and the Yukon. The Central regional office in Toronto covers Manitoba, the Northwest Territories, Nunavut, and Ontario. The Eastern regional office in Montreal covers Quebec, New Brunswick, Nova Scotia, Prince Edward Island and Newfoundland & Labrador.

974. ROC has a budget, for the fiscal year of 2006-07, of approximately CAD 5 million. ROC in Ottawa, which includes the Compliance and Program Development Units, as well as the Assistant Director's Office, has a total of more than 20 staff members. The three regional offices have approximately 10 staff members each.

975. With approximately 50 people dedicated to compliance, FINTRAC manages to perform about 150 examinations in financial institutions annually which has to be compared with an estimated

number of reporting financial entities exceeding 150,000 (not taking into account DNFBPs). However, it should be noted that the examinations are targeted at firms and in most cases, a single FINTRAC examination of a parent entity will cover a number of reporting entities, as the parent entity may cover hundreds of individual entities (for example, in a corporate entity securities dealers or an MSB). Therefore, FINTRAC exams cover significantly more than 150 reporting entities in a year, but there are no statistics on the exact number of entities effectively assessed.

976. Moreover, in order to optimize the allocation of its supervisory resources, FINTRAC has adopted a risk-based approach, based on the risk profiles both of the sector and the individual entities, which are regularly updated through the collection of information from a large range of various sources. Reporting entities are mainly selected for examination on the basis of the scores resulting from this approach, while 10% of the examined entities are selected randomly. The assessment team believes that FINTRAC has developed a sophisticated risk-based model that certainly helps FINTRAC to prioritise its supervisory functions.

977. From a technical resource perspective, ROC makes use of the FINTRAC Risk Assessment Tool (FRAT), database software that was developed in-house. This tool helps to ensure that Compliance Officers have access to accurate and up-to-date information, as well as ensuring the timely maintenance of reporting entity information and risk assessment information. This is an important element in meeting information management needs and helping to manage effectively FINTRAC's national compliance program. In addition, FINTRAC Compliance Officers are equipped with various types of technological hardware.

978. However, the FRAT does not cover all reporting entities, as it is mainly focused at the firm level: it covers about 26 000 entities. Moreover, under the risk-based approach, lots of entities included in the FRAT would never have an examination by FINTRAC, even if a limited number of examinations are selected randomly each year. In these conditions, it is the opinion of the assessment team that, unless FINTRAC can rely to a greater degree on primary regulators and SROs in the future, its current organisation and resources dedicated to supervision do not allow it to perform its compliance function in a totally effective way.

979. It is to be noted that ROC is currently expanding as the result of new legislative initiatives that were introduced by the Government of Canada in late 2006.

980. *Professional standards*. ROC is comprised of a diverse group of people with relevant experiences and skills from both the public and private sectors such as the financial industry, accounting, law enforcement, customs, revenue, and public safety. In general, Compliance Officers possess a university degree in such disciplines as the social sciences, accounting, commerce and administration. In addition, many FINTRAC employees are affiliated with professional associations such as Chartered Accountants and Certified Fraud Examiners.

981. ROC team members must conform to the enhanced security measures that FINTRAC has implemented. Like all other FINTRAC employees, compliance officers must obtain 'Top Secret' security clearance as a condition of employment.

982. Further to this, ROC team members receive Compliance Officer Authorisation Training, which assists in preparing the Compliance Officer for conducting examinations in the field, including on how to comport themselves in this kind of environment. A number of policies and procedures have also been developed to guide Compliance Officers, including one on the Professional Expectations for Compliance Officers which comprises fair treatment, courtesy and consideration, privacy and confidentiality, bilingual service, information.

983. Moreover, the following provisions apply to all FINTRAC compliance officers, who are the public face of FINTRAC :

- *Integrity*: perform their work with honesty, diligence, and responsibility; observe the law and make disclosures expected by the law and the PCMLTFA; not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the organization; and respect and contribute to the legitimate and ethical objectives of the organization.
- *Objectivity:* not participate in any activity or relationship that impairs or will be seen as impairing their unbiased assessment; not accept anything that may impair or be presumed to impair their professional judgment; and disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under examination.
- *Confidentiality:* be prudent in the use and protection of information acquired in the course of their duties; and not use information for any personal gain or in any manner that would be contrary to the law.
- *Competency:* engage only in those services for which they have the necessary knowledge, skills, and experience; perform compliance examinations in accordance with FINTRAC policies and procedures; and continually improve their proficiency and the effectiveness and quality of their services. Compliance Officers are required to pass a written course examination in order to become an authorised compliance officer. Compliance officers also then undergo an annual review to maintain their authorisation.

984. FINTRAC Compliance Officers are expected to apply and uphold these principles and rules in addition to the FINTRAC Code of Conduct and Ethics for all employees, available on FINTRAC's Intranet. This is consistent with the Code of Values and Ethics for the Public Service of Canada which came into effect in September 2003. In addition, there are severe penalties in place for any unlawful disclosure made by a FINTRAC employee.

985. *Training.* FINTRAC's Compliance Officers receive rigorous training. New team members receive Orientation training shortly after their arrival. This training focuses on the following: FINTRAC's Legal Framework; the Canadian AML/CFT Regime; International Efforts and Cooperation; Regional Operations and Compliance; Macro Analysis and Integration; Tactical Financial Intelligence (Analytical and Disclosure Process; Production Orders; Sanitized Cases); Macro Analysis and Integration (Strategic intelligence; Operational Statistics; Research and Analysis).

986. In addition, FINTRAC Compliance Officers also receive Compliance Officer Authorisation Training, a nine day comprehensive course that covers numerous areas relating to risk assessment and compliance examinations with cases study.

987. Following the successful completion of the training, all Compliance Officers are authorised in writing by FINTRAC's Director, which then permits them to perform examinations of reporting entities.

988. FINTRAC's Regional Operations and Compliance Section also holds training sessions twice yearly. These are usually a week long and address various subject matters relevant to the work undertaken by Compliance Officers. Team members also attend various AML/CFT conferences and a number are members of the Association of Certified Anti-Money Laundering Specialists (ACAMS).

OSFI

989. *Resources*. OSFI is the sole supervisor of banks and other federally incorporated financial institutions. The OSFI Act provides that the Minister of Finance is responsible for OSFI. It also provides that the Superintendent is solely responsible for exercising the authorities under the financial legislation and is required to report to the Minister of Finance from time to time on the administration of the financial institutions legislation. The Superintendent is given operational independence through an appointment for a fixed term of seven years.

990. The OSFI Act authorises the Superintendent to act independently in order to meet staffing and other resource requirements to fulfil the supervisory obligations. The Superintendent is authorised to

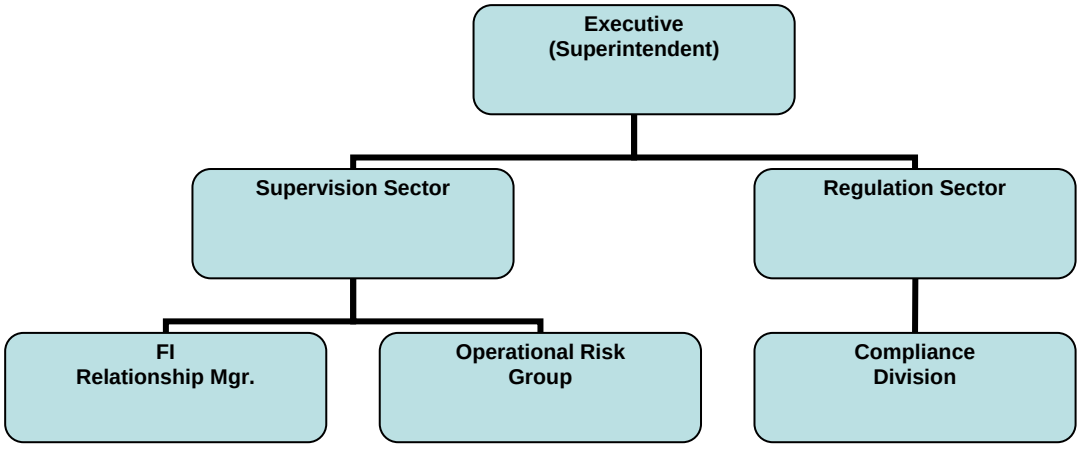
exercise the powers and perform the duties and functions of Treasury Board under the Financial Administration Act that relate to personnel management, including the determination of terms and conditions of employment and the responsibility for employer/employee relations.

991. OSFI's revenue attributable to the regulation and supervision of FRFIs is raised through asset-based, premium-based or membership-based assessments on the financial services industry, and a user pay program for selected services. In the fiscal year ended March 31, 2007, this revenue amounted to CAD 69.7 million. Assessments are allocated to industry sectors based on the approximate amount of time spent on supervising and regulating the industry. Costs are then assessed to individual FRFIs in each sector based on a formula, with a minimum or base level assessment for the smallest FRFIs. The assessments are required by law to be paid and there is no appeal on assessments allocated to FRFIs. Thus, OSFI's program of supervision and regulation of FRFIs is not funded by the government. This affords OSFI a further measure of operational independence from government.

992. OSFI has a staff complement of about 450 and is organized primarily into three sectors:

- The Regulation Sector (123 personnel) is primarily concerned with rule-making, administering registrations and approvals, compliance, and the supervision of pension plans.
- The Supervision Sector (162 personnel) is responsible for supervising and monitoring federally regulated financial institutions.
- The Corporate Services Sector (115 personnel) is responsible for administrative, human resources, systems and technical services.

993. The Compliance Division, which is a part of the Regulation Sector, is responsible for leading AML/CFT assessments of financial institutions in conjunction with the Supervision Sector. The following diagram illustrates the placement of the AML/CFT unit within the OSFI organizational structure:



994. In 2001 two factors contributed to OSFI's decision to allocate more resources to AML/CFT as well as introduce a specific AML/CFT assessment program: the passage of the legislation creating FINTRAC and the introduction of mandatory transaction reporting, and the events of September 11, 2001 with the implementation shortly thereafter of the requirement of financial institutions to search for listed terrorist and terrorist entities and to freeze their assets, with mandatory monthly reporting of frozen assets to regulators.

995. In September 2002, OSFI designated two fulltime employees from OSFI's Compliance Division to commence an AML/CFT assessment program. By 2006, the resources allocated to AML/CFT had grown to 10 employees, of which 8 perform on-site assessments. In addition to this, three employees were redeployed internally from the Supervision Sector in 2006 to support AML/CFT assessments of Canadian conglomerate banks.

996. This increase in staff allowed OSFI to extend its program of examinations into smaller institutions for the first time in 2005. With the current staffing level, it manages to perform 10 to 30 examinations per year, eventually covering a higher number of individual entities when subsidiaries are also concerned (40 entities covered in 2006 for a total number of missions of 13). Excluding from the 215 FRFIs subject to the PCMLTFA those that are otherwise part of conglomerate groups already included or which bear no inherent AML/CFT risk (*e.g.* reinsurers, restricted foreign branches), OSFI is supervising 135 reporting entities. OSFI has instituted a target frequency of about 3 years for institutions presenting higher inherent risk. This includes all conglomerate banks and most conglomerate life insurance companies, and is generally consistent with OSFI's regular prudential examination cycle. Smaller entities will be risk ranked using various ML/TF risk criteria unrelated to financial risk (capital, earnings, liquidity, etc.). Smaller entities that present medium to high inherent risk (due to their business profile matched against the AML/CFT criteria) will also be cycled through an assessment approximately every 3 years. The small, low- to no-risk entities will be the subject of regular monitoring with on site work taking place at longer intervals.

997. *Professional standards.* OSFI's minimum qualification for employment includes a degree from a recognized university or college in a relevant field and/or being a member in good standing in a professional organization. All OSFI employees are subject to a Code of Professional Conduct, and are also subject to an annual review to ensure compliance. The Code requires that OSFI staff act in a professional manner in undertaking their responsibilities. Among other things, the Code requires staff to treat all information obtained in the course of their work as confidential. This refers particularly to any information regarding the affairs of a financial institution and of persons dealing with them. Unauthorised disclosure of any information or use of information for personal reasons by OSFI staff is prohibited in accordance with section 22 of the Office of the Superintendent of Financial Institutions Act, the Privacy Act and employees' oaths of office and secrecy.

998. The Code also contains a Conflict of Interest Code to which staff must adhere. The Conflict of Interest Code minimizes the possibility of conflicts arising between an OSFI employee's private interests and the employee's public service duties and provides for the resolution of unavoidable conflicts in a timely fashion. Failure to comply with the Code of Professional Conduct or the Conflict of Interest Code can lead to appropriate disciplinary measures including termination of employment.

999. All new OSFI staff must pass an enhanced reliability check. At a minimum this involves a background check by law enforcement (RCMP), a credit check and a check of the employee's references to determine the employee's suitability. In situations where the employee will deal with information classified beyond the normal confidentiality level, the check will also include a more extensive review that is conducted by security intelligence officials.

1000. Finally, as part of the employment contract, OSFI employees are required to take an oath of allegiance to Her Majesty in Right of Canada, and each employee's performance is assessed annually to ensure that work is completed in a satisfactory manner.

1001. Taken together, all these controls ensure that OSFI employees are competent in undertaking their responsibilities, subject to high professional and ethical standards and treat information that they deal with during the course of their duties in a confidential manner.

1002. *Training.* All OSFI supervisory staff receive compulsory training on OSFI's Supervisory Framework. Most OSFI staff involved in AML/ CFT assessments were originally general supervisors before transferring to the Compliance Division.

1003. The staff in Compliance Division receive both formal and on-the-job training related to money laundering and terrorist financing. All staff assigned to AML/CFT assessments are experienced examiners and many have extensive industry experience.

1004. To date, six OSFI staff members (four of which are in the Compliance Division) have attended training at the Office of the Comptroller of the Currency (OCC) AML School in Washington, DC. In addition nine Compliance employees are members of the Association of Certified Money-Laundering Specialists (ACAMS) and three of these employees have qualified as Certified Anti-Money Laundering Specialists. OSFI employees have attended financial crime and AML/CFT conferences in Canada, the United States and Europe. In addition senior Compliance Division staff have made numerous presentations on the subject of AML/CFT at industry conferences in Canada and elsewhere.

IDA

1005. *Resources.* The Investment Dealers Association of Canada has four offices across Canada: Montreal, Calgary, Vancouver and its head office located in Toronto. Its 280 employees fulfill its mission of protecting investors and enhancing the efficiency and competitiveness of the Canadian capital markets. It has attracted a group of highly skilled professionals with collective experience in all facets of the securities industry, as well as expertise in various fields including law and accounting.

1006. The IDA Sales Compliance Department has an authorised staff complement of 48. The Enforcement Department has 83. It manages to review all reporting entities at least every five years, but the most important firms may be reviewed yearly.

1007. *Professional standards*. The IDA has a set of values that shapes the way its employees and members carry out their responsibilities and work with each other and the industry. The IDA maintains integrity by conducting itself in an honest and ethical manner and ensures a high degree of professionalism. It is dedicated to carrying out its duties in a timely and reliable fashion. It is accountable through a transparent process with open communication with stakeholders.

1008. The IDA also has a Code of Business Conduct, a Privacy Policy and a Whistleblower policy and process.

1009. *Training.* The IDA's training program for new Sales Compliance Officers includes AML training. The IDA Enforcement Department also organise seminars the AML/CFT topic.

MFDA

1010. *Resources.* The Mutual Fund Dealers Association of Canada has three offices across Canada: Calgary, Vancouver and its head office located in Toronto. Its 155 employees fulfill its vision of raising the standard of firm, fair and transparent regulation in Canada for the protection of investors through commitment to collaboration, staffing excellence and regulatory best practices. MFDA staff is comprised of highly skilled professionals with expertise in various fields including the securities industry, securities regulation, law and auditing and accounting.

1011. The MFDA Compliance Department is comprised of 52 compliance staff, the majority of which or members of a professional association. The Enforcement Department has 45 staff. The MFDA reviews all Members at least once every three years but may perform more frequent examinations if necessary.

1012. *Professional standards and training*. The MFDA has established policies and procedures for the conduct of its activities. These standards are continually reviewed and assessed annually by the MFDA and subject to oversight by the Canadian Securities Administrators. The MFDA had devoted significant resources to staff training and has conducted AML seminars for staff including sessions with FINTRAC.

1013. The MFDA also has a Code of Business Conduct, a Privacy Policy and a Whistleblower policy and process.

Other regulators

1014. During the on-site visit, several regulators asserted that they could not perform on-site reviews or in-depth AML assessments as they are not mandated to do so and lack resources. In particular, resources within the AMF, DICO and the MFDA are limited to deal with AML/CFT issues especially in carrying out supervisory visits and examinations.

Authorities' powers and sanctions (Recommendations 29 & 17)

Recommendation 29

FINTRAC

1015. FINTRAC has responsibility for ensuring compliance with the PCMLTFA. The PCMLTFA includes certain key provisions that assist FINTRAC in meeting its responsibility.

1016. FINTRAC has the right to enter any premises (other than a dwelling-house), to access any document, computer system or data and to reproduce any document under Sections 62(1) and 62(2) of the PCMLTFA, and records that are required to be kept by the reporting entity under the regulations must be retained in such a way that they are accessible to an authorised person (including a FINTRAC Compliance Officer, Section 70). However, this provision authorises a possible period up to 30 days to deliver the information, which seems somewhat excessive (see comments in Section 3.5 of the report). If consent is not granted by the reporting entity for a compliance officer to enter a dwelling, FINTRAC must obtain a warrant to allow a compliance officer to do so although to date this has not been necessary. Reporting entities located in dwelling houses represent a small percentage of the total number of reporting entities. To date, whenever consent has been requested by FINTRAC, it has been granted.

1017. In most circumstances, a FINTRAC compliance officer will contact the reporting entity to be examined a minimum of 30 days before an examination is to commence to allow adequate time for the reporting entity to prepare the requested records for examination. FINTRAC, however, still maintains the authority to conduct on-site compliance examination activities, with no advance notice to the reporting entity.

1018. Subsections 65(2) and 65(3) of the PCMLTFA also provide FINTRAC with an important tool to ensure effective supervision of financial institutions which enables it to exchange compliance information with federal and provincial agencies that regulate entities and individuals with obligations under the PCMLTFA. Subsection 65(10) allows FINTRAC to exchange information with foreign regulators regarding the compliance of reporting entities.

1019. In addition, Section 63.1 of the PCMLTFA provides FINTRAC with the authority to require reporting entities to provide any information that FINTRAC needs for compliance purposes. Reporting entities are therefore obliged to complete and return compliance questionnaires sent by FINTRAC.

1020. Finally, FINTRAC currently has no powers to sanction non compliant institutions and the only action it can take is to transmit the file to law enforcement for investigation related to the criminal sanctions provided by the PCMLTFA (see comments below)[129].

OSFI

1021. OSFI has no mandate under PCMLTFA to ensure compliance of FRFIs with the PCMLTFA. Its mandate, under the Office of the Superintendent of Financial Institutions Act is to supervise financial

[129] Part 4.1 of the PCMLTFA, Notices of Violation, Compliance Agreements and Penalties, provides for an administrative and monetary penalties regime for FINTRAC with reporting entities that do not comply with their AML/CFT obligations. The regulations implementing this regime were enacted in December 2007 and will come into force in December 2008.

institutions in order to determine whether they are in sound financial condition and are complying with their governing statute law and supervisory requirements under that law as well as to promote the adoption by management and boards of directors of financial institutions of policies and procedures designed to control and manage risk. OSFI also has specific powers of supervision under the governing statutes of all federal financial institutions.

1022. More specifically, Subsection 6(1) of the OSFI Act indicates the Superintendent's powers and duties in relation to the *Bank Act*, the *Trust and Loan Companies Act*, the *Cooperative Credit Associations Act* and the *Insurance Companies Act.* The supervisory powers of the Superintendent are uniform under these Acts. The Bank Ac (Articles 643 and 644), for instance, illustrates the Superintendent's power as follows: "*the Superintendent, from time to time, but at least once in each calendar year, shall make or cause to be made any examination and inquiry into the business and affairs of each bank that the Superintendent considers to be necessary or expedient to determine whether the bank is complying with the provisions of this Act and whether the bank is in a sound financial condition and, after the conclusion of each examination and inquiry, shall report on it to the Minister. (2) The Superintendent or a person acting under the Superintendent's direction (a) has a right of access to any records, cash, assets and security held by a bank; and (b) may require the directors, officers and the auditor or auditors of a bank to provide information and explanations, to the extent that they are reasonably able to do so, in respect of the condition and affairs of the bank or any entity in which the bank has a substantial investment. The Superintendent has all the powers of a person appointed as a commissioner under Part II of the Inquiries Act for the purpose of obtaining evidence under oath, and may delegate those powers to any person acting under the Superintendent's direction."*

1023. The indirect involvement of OSFI in ensuring AML/CFT compliance tends to place a limit on its powers. It is only insofar as incidences of AML non compliance can be considered as an unsafe or unsound practice in conducting the business of the bank, that the Superintendent may take enforcement actions and direct the bank or person to cease or refrain from pursuing the course of conduct or to perform such acts as in the opinion of the Superintendent are necessary to remedy the situation. Unlike FINTRAC, it cannot make a direct disclosure of non compliance with PCMLTFTA to law enforcement authorities.

1024. The assessment team was told that OSFI has never been denied access to any information or documentation it requests to conduct an AML/CFT assessment.

Securities regulators including IDA

1025. The SRAs are not mandated by PCMLTFA to ensure compliance of reporting entities with the AML legislative requirements. Nevertheless, they may also rely on the principle of "safe and sound business practice" and on the fact that compliance with the law and regulations is part of the fit and proper criteria that a financial entity must meet to be granted and to maintain registration or a license. In general, the investigation and enforcement powers of the SRAs are comprehensive but specific powers may vary among the provinces and territories. Generally, the SRAs have the power to compel testimony and evidence as well as large powers of sanction. There is also authority in some jurisdictions for the SRA to recover investigation and hearing costs.

1026. The IDA is given the authority to ensure compliance by financial institutions through the individual SRAs. For example, in the case of Ontario, section 21.1 of Ontario's Securities Act recognizes the IDA as a self-regulatory organization, and sets conditions that the IDA must meet. For example (this list is not exhaustive), the IDA shall enforce compliance by its members to IDA rules, provide prompt report and notification of any misconduct by its members to the SRA, advise the public and media of any disciplinary settlement hearing, provide monthly notifications to the SRA of all new investigations, operational reviews and similar matters.

1027. As the national self-regulatory organization of the Canadian securities industry, it has enforcement rules and regulations of member firms and their registered employees, including non-compliance with obligations that are similar to those of the PCMLTFA. These conditions can be found in the IDA By-Laws. The IDA reports all compliance deficiencies to FINTRAC and has on occasion provided extra notice of egregious cases.

1028. Concerning AML issues, the IDA may be considered to have more direct enforcement powers than some other regulators since it has its own set of enforceable by-laws, which sometimes go beyond FINTRAC's requirements and have been used previously to sanction some of its members.

Recommendation 17

FINTRAC

1029. Canada has designated FINTRAC as the authority responsible for determining if a violation has occurred and when appropriate for forwarding that information to law enforcement for investigation. The PCMLTFA outlines the sanctions that can be imposed on reporting entities if they fail to comply with their AML/CFT obligations. In addition, FINTRAC uses warning letters (deficiency letters) and can order action plans to enforce compliance.

1030. Under the current version of the PCMLTFA and its Regulations, FINTRAC itself has very limited powers of enforcement against reporting entities and their directors or senior management for failure to comply with or properly implement AML/CFT requirements. FINTRAC cannot impose penalties but only has the option of referring cases to law enforcement for investigation. The PCMLTFA provides for a series of criminal sanctions for contraventions of various provisions of the Act. This can lead to criminal penalties of up to CAD 2 million in fines and five years in prison for non-compliance.

1031. Until the recent amendments brought to the PCMLTFA enacted in December 2006, these sanctions were applicable in a limited range of cases, namely for the violations of: (1) the record keeping duties, (2) the duty to answer and comply with the request of an officer in the reporting of currency and monetary instruments during cross border movements; (3) the limitations related to disclosure and use of information; (4) the duty to assist and provide information to FINTRAC; (5) the obligation of retention of documents as it applies to legal counsel who claims privilege, as well as (6) the reporting obligations (STRs, TPRs and prescribed transactions). For instance, failure to implement a compliance program was not subject to sanctions under the law. The recent amendments have expanded the regime of criminal sanctions to the violations of most of the law and regulations provisions.

1032. Sanctions are applicable to any officer, director, or agent of the person or entity who directed, assented to, acquiesced in, or participated in its commission, as described in Section 78 of the PCMLTFA.

1033. Most of the sanctions provided by Sections 74 to 77 of the PCMLTFA are punishable (a) on summary conviction to a fine of not more than CAD 50 000 or to imprisonment for a term of not more than six months, or both, or (b) on conviction on indictment, to a fine of not more than CAD 500 000 or to imprisonment for a term of not more than five years, or both. Knowingly contravening to the obligation of reporting suspicious transactions or transactions suspected of being related to terrorist financing is an offence punishable (a) on summary conviction, (i) for a first offence, to a fine of not more than CAD 500 000 or to imprisonment for a term of not more than one year, or both, or (ii) for a subsequent offence, to a fine of not more than CAD 1 000 000 or to imprisonment for a term of not more than one year, or both, or (b) on conviction on indictment, to a fine of not more than CAD 2 000 000 or to imprisonment for a term of not more than five years, or both. Contraventions to the reporting of prescribed financial transactions are punishable (a) on summary conviction to a fine of not more than CAD 500 000 for a first offence and of not more than CAD 1 000 000 for each subsequent offence.

1034. Finally every person or entity that contravenes Section 8 is (a) guilty of an offence punishable on summary conviction, or (b) guilty of an indictable offence and liable to imprisonment for a term of not more than two years.

1035. In nearly 4 years, FINTRAC has disclosed 7 such cases of egregious non-compliance by reporting entities including financial institutions, to law enforcement agencies. In the event a disclosure is made, the responsibility falls to law enforcement to investigate and, where appropriate, pursue criminal sanctions for non-compliance. Disclosures have so far resulted in only one conviction for non-compliance with the PCMLTFA. The person convicted was also convicted for money laundering.

Non-Compliance Disclosures					
	2003/04	**2004/05**	**2005/06**	**2006/07***	**Total**
Number of disclosures	0	2	3	2	7

*As of end of the second quarter.

1036. In the absence of other powers of sanction and, especially, of administrative and monetary penalties, FINTRAC has favoured a "cooperative approach" to compliance, based on the principle "trust but verify" and deals with less severe non compliance issues by issuing deficiency letters, which require the reporting entity to respond with an action plan.

1037. In the majority of cases where FINTRAC has identified deficiencies in a reporting entity's compliance with the PCMLTFA, the entity takes corrective action based on a letter from FINTRAC that outlines these deficiencies.

1038. Once the detailed examination findings have been communicated to the reporting entity identifying the need for corrective action ("deficiency letter"), the reporting entity is required to submit a corrective action plan to FINTRAC. The action plan, which must be submitted in writing, must include timelines for correcting the identified deficiencies. If an action plan is received that does not adequately address the deficiencies identified during the examination, the FINTRAC Compliance Officer contacts the reporting entity compliance officer, both verbally and in writing, to request that they provide a new action plan in order to rectify the deficiencies in a timely manner. The written correspondence is sent to the senior executive of the reporting entity, with a copy to the reporting entity's compliance officer. The letter clearly outlines that the reporting entity is in non-compliance with its legislative obligations under the PCMLTFA.

1039. Should a reporting entity submit a further inadequate action plan, the reporting entity is clearly informed of the shortcomings and is required to re-submit an acceptable plan. The action taken by the reporting entity may influence FINTRAC's decision to refer to the non-compliance disclosure to law enforcement. The compliance officer then follows up with the reporting entity to ensure that the action plan is being undertaken in a timely manner and that deficiencies are being corrected appropriately.

1040. Where a reporting entity makes no demonstrable effort to address deficiencies identified by FINTRAC, FINTRAC can disclose such a case of non-compliance to law enforcement for investigation and prosecution.

1041. The current regime of sanctions administered by FINTRAC is clearly insufficient as it does not allow FINTRAC to apply a graduated and proportionate range of sanctions and limits the possibilities of imposing prompt corrective actions in cases where criminal sanctions would not apply. Thus, it cannot be considered as effective, proportionate and dissuasive[130].

[130] In order to enhance the effectiveness of the system and provide greater flexibility and authority for FINTRAC in ensuring compliance with the PCMLTFA and its regulations, it was decided to create an administrative and monetary penalties regime. Such a measure has been incorporated in the December 2007

OSFI

1042. The federal financial institutions' governing legislation gives OSFI the power to oversee financial institutions' AML/CFT risk management controls. OSFI has the power under the Office of the Superintendent of Financial Institutions Act to impose sanctions when the nature of the non-compliance is determined to be an unsafe and unsound practice.

1043. OSFI has a range of supervisory tools and sanctions at its disposal, including written interventions, staging (which involves higher CDIC – Canada Deposit Insurance Corporation – premiums), directions of compliance, placing terms and conditions in the FRFI's Order To Commence And Carry On Business (operating licence) and imposing an Administrative Monetary Penalties (AMP) under the OSFI Act. Section 25 of the OSFI Act sets out a range of administrative monetary penalties that OSFI can use. However, these AMPs, which were introduced in 2005, only apply in case of a contravention of a provision of a financial institutions Act or in case of non-compliance with any order or Direction of Compliance, any terms and conditions imposed, any undertaking given or any prudential agreement entered into under a provision of a financial institutions Act. Thus, they cannot be administered directly in cases of non-compliance with the PCMLTFA or its regulations which do not amount to unsafe or unsound practice, which would have justified such an intervention in any event. Stronger sanctions include the ability to go to court to obtain an order to stop the unsafe or unsound practice, or in extreme cases OSFI can remove a director from the board or senior officer for his or her position. These supervisory tools or sanctions are further detailed in the following paragraphs.

1044. OSFI issues Supervisory letters after each AML/CFT assessment. The letters contain "required actions" on compliance issues or "recommendations" as follows:

- "Required action" speaks to a deficiency that relates to non-compliance with a specific provision of the PCMLTFA. Failures to comply with Guideline B-8 are met with a "requirement for action" when it also involves a breach of the PCMLTFA or in some cases, when OSFI feels it necessary to deliver a strong signal to the financial institution.

- "Recommended action" speaks to a deficiency in risk management controls or other supervisory requirement not directly related to a legal requirement. Failures to comply with Guideline B-8 provisions that are not requirements under the PCMLTFA are in principle subject to recommended actions (for instance when a financial institution fails to have measures in place in relation to PEPs for which legal requirements are not in force yet).

1045. OSFI can also impose a more intrusive supervisory schedule on institutions, called Staging, which consists of raising the stage rating of a FRFI (normal stage, for no problem institutions being 0, the other stages ranging from 1 "early warning" to 4 "not viable/insolvency imminent"). Elevation from stage 0 to stage 1 results in more intense oversight by OSFI. It also results in a higher OSFI assessment fee and in an increase in their deposit insurance premiums charged by the Canada Deposit Insurance Corporation. Further increases in stage ratings attract additional deposit insurance premiums.

1046. If OSFI determines that directors or senior management of a FRFI have, or are about to, fail to comply with or properly implement AML/CFT requirements in a manner that amounts to the commission of an unsafe or unsound practice in conducting the business of the FRFI, or that would constitute a course of conduct that is an unsafe or unsound practice in conducting the business of the FRFI, the Superintendent has authority to issue unilateral instructions called Directions of Compliance under the FRFI's governing statute. For example subsection 645(1) of the Bank Act provides as follows: "*(1) where, in the opinion of the Superintendent, a bank, or a person with respect to a bank,*

---

amendments to the PCMLTFA that were enacted on 14 December 2006 and in a new set of regulations, the PCMLTF Administrative Monetary Penalties Regulation, enacted on 26 December 2007. These provisions will come into force in December 2008.

is committing, or is about to commit, an act that is an unsafe or unsound practice in conducting the business of the bank, or is pursuing or is about to pursue any course of conduct that is an unsafe or unsound practice in conducting the business of the bank, the Superintendent may direct the bank or person to (a) cease or refrain from committing the act or pursuing the course of conduct; and (b) perform such acts as in the opinion of the Superintendent are necessary to remedy the situation."

1047. The failure of a FRFI to comply with a Direction of Compliance is an offence under the financial institution's governing statute and is sanctionable under the OSFI Act.

1048. The Superintendent of OSFI also has the power to enter into a Prudential Agreement with a FRFI. For example section 644.1 of the Bank Act provides as follows: "*the Superintendent may enter into an agreement, called a "prudential agreement", with a bank for the purposes of implementing any measure designed to maintain or improve its safety and soundness."*

1049. In extreme cases, OSFI can remove directors or officers from office and take control of a financial institution. In addition, OSFI can require external auditors to extend the scope of their audit and request that the board of directors meet with the Superintendent.

1050. In summary, these measures constitute a progressively more intrusive array of supervisory measures that can be utilized to change undesirable behaviour by financial institutions in order to meet ongoing regulatory requirements and expectations.

1051. Concerning AML/CFT issues, the usual way of intervention is via written communication: the 78 assessments between 2002 and the end of the first quarter 2007 resulted in supervisory letters containing 247 required actions on compliance issues with PCMLTFA/PCMLTFR and 381 recommended actions to strengthen risk management controls.

1052. No measure of direction of compliance, terms or conditions imposed or prudential agreement was ever taken on AML/CFT issues. However, in the period 2004 – 2006 inclusive OSFI staged four financial institutions primarily for AML/CFT control deficiencies (one in 2004, 2 more in 2005 and the fourth in 2006). Further, a fifth assessment conducted in 2005 led to the institution, already at Stage 1, remaining there for an extended period of time. These stagings (to stage 1) led to OSFI and/or CDIC surcharges ranging from CAD 45 000 up to CAD 500 000.

1053. In addition, OSFI brings matters related to non-compliance with the PCMLTFA to the attention of FINTRAC immediately following each on-site assessment.

1054. Thus, OSFI has a wider range of possible enforcement actions or sanctions than FINTRAC. Nevertheless, even if these tools exist, sanctions remain rarely used which may be due to the fact that the "sound and safe business practice" principle on which OSFI's intervention is based, imposes a higher threshold than simple non compliance.

1055. It is worth mentioning that, when the proposed PCMLTF Regulations comes into force, the Administrative & Monetary Penalties scheme for non compliance with PCMLTFA will be administered only by FINTRAC and will not be accessible to OSFI or other regulators.

Securities regulators

1056. SRAs have a range of measures they can choose from to rectify circumstances where a market intermediary fails to meet ongoing requirements and protect the public. They include suspending or terminating the intermediary's license, imposing terms and conditions on the intermediary requiring for instance restrictions on the type or amount of business that the intermediary may conduct or the number of salespersons or advisers a firm may hire.

1057. Additionally, the SRAs may order that exemptions contained in the securities laws in the jurisdiction do not apply to the intermediary. This order is often made if an intermediary has been suspended or terminated in order to prevent the intermediary from conducting business based on registration and prospectus exemptions. In Ontario and Quebec, the SRAs also may order a registrant to submit to a review of practices and procedures and institute such changes as recommended by the SRA where the SRA has concerns about the practices and procedures of the intermediary.

1058. In certain other provinces, the SRA can appoint a person to review the business and conduct of a registrant or former registrant to determine whether the registrant is complying, or has complied, with the legislation in the jurisdiction, any decision made under that legislation or any requirement of an exchange or SRO to which the registrant belongs. An SRA also may order that a document be produced by a registrant if the SRA is satisfied that securities laws have not been complied with. Additionally, most SRAs may reprimand a registrant or issue a caution letter when the SRA determines that the behaviour of the registrant merits a reprimand or caution, for example, where the behaviour of the registrant is contrary to the public interest.

1059. Compliance officers and branch managers can be sanctioned for contravening a specific requirement to supervise conduct within the firm. In addition, pursuant to this power, an SRA can make an order against a person or company whose behaviour or inaction contributed to the violation, for example, a director, officer or partner of the registrant or parent company of the registrant, if the SRA concludes that it is in the public interest to do so. Certain SRAs have the authority to impose a financial penalty on a registrant for contraventions of securities laws. These SRAs and the other SRAs also have the authority to apply to the court for such an order, for example, where the court finds that there has been a violation of securities laws.

1060. Similarly, the IDA and MFDA may suspend a member's membership rights and privileges, suspend the approval of an individual and/or impose conditions on the continued membership of a member or approval of an individual if, for example, the member or individual fails to meet ongoing requirements, contravenes Canadian securities laws, or engages in any business conduct or practice that the SRO concludes is unbecoming or contrary to the public interest.

1061. The SROs can also impose sanctions against their members (and registered employees of members) for contraventions of SRO requirements, including AML and supervision requirements.

1062. The IDA and MFDA have the power to impose financial penalties on their members and approved individuals if the SRO determines that, for example, the member or individual fails to meet ongoing requirements, contravenes Canadian securities laws or engages in any business conduct or practice that the SRA concludes is unbecoming or contrary to the public interest.

1063. The IDA can discipline its member firms and their employees using a broad range of sanctions that are proportionate to the severity of the situation. For instance, IDA penalties can include fines, up to a maximum of the greater of CAD 1 million per contravention or an amount equal to three times the profit made or loss avoided by reason of the contravention for registered employees or fines up to a maximum of the greater of CAD 5 million per contravention or an amount equal to three times the profit made or loss avoided by reason of the contravention for member firms. The IDA can also suspend or ban individuals for life from registration as a broker, or suspend and expel firms from membership. The latter has the effect of closing down firms from operating in the securities industry.

1064. The IDA's Enforcement Process is an essential element in assuring investors that the IDA's member firms are effectively regulated and that each adheres to the highest standards of conduct. It is comprised of three stages that ensure that sanctions are proportionate to the severity of the situation. All matters presented to the Association are initially considered during the Complaint Review process. If this initial review indicates that further investigation is warranted, the matter is referred to Investigations staff. If the investigation finds sufficient evidence of a regulatory breach, the matter is subsequently referred to Enforcement Counsel for disciplinary action. The IDA's Enforcement

Counsel reviews the investigation file and, if appropriate, prepares charges, penalty recommendations and a settlement offer for the respondent. If Enforcement Counsel is successful in negotiating a settlement with the respondent, the settlement agreement is put before the Hearing Panel, which may accept or reject the settlement agreement. If a settlement offer is not successfully negotiated between Enforcement Counsel and the respondent, a Notice of Hearing and Particulars is issued and a contested hearing is held. Hearing Panels are comprised of two industry representatives and a member of the public who acts as Chair. The public members are not associated with any investment dealer and have legal training, usually as an experienced securities lawyer or retired judge.

1065. IDA hearings are generally open to the public. Notice is provided to the public in advance of any hearing and the IDA subsequently makes information on its disciplinary decisions public.

1066. In general, it has to be noted that, except for IDA which has effectively applied in a number of cases heavy sanctions to its members for non compliance with AML/CFT standards (for instance, CAD 600 000 fine and revocation of the firms membership along fines and suspensions applied to the firms directors for violation of IDA Regulation 1300.1 (a) which requires each member to use due diligence to learn and remain informed of the essential facts relative to every customer and to every order or account accepted and subsequent violation of the PCMLTFA requirements for verifying client identity), it has emerged from the meetings that the assessment team has had with professionals during its on-site visit, that these powers of sanction have generally not been used by SRAs or SROs in that area, as they have rarely issued specific rules or regulations related to AML/CFT and consider it to be mainly FINTRAC's responsibility.

Other regulators

1067. The other regulators are not entrusted with the responsibility of ensuring compliance with the PCMLTFA but, as already stated, some of them include controls related to AML/CFT requirements in their compliance programs, based on their various statutory powers: their intervention in that area is based either on the "safety and soundness" principle, or on the mandate given to them to ensure compliance with any federal law or regulation or still on codes of conduct or mandatory guidance that they have developed at their level for their regulated entities.

Recommendation 23 – Market entry and ongoing supervision

1068. The number of regulators, both federal and provincial, as well various SROs makes this a complex regulatory system.

1069. Although there is no systematic harmonization of the requirements in terms of market entry among the federal and provincial levels and among the different provinces, the information that the assessment team could obtain shows that the measures aimed at preventing criminals or their associates from holding a significant or controlling interest or holding a management function in a financial institution, as well as the "fit and proper" principle are widespread. However, provinces have variations in their supervisory treatment. For instance, for finance companies, not all provinces have adopted such a requirement in their respective Acts regulating the sector.

1070. Currently, MSBs are supervised by FINTRAC for AML/CFT purposes while not subject to registration or licensing.

1071. The following section will further elaborate on the requirements imposed by the main regulators or in the main sectors but they cannot be considered as exhaustive.

Financial institutions supervised by OSFI

1072. All applications to incorporate or register FRFIs must be approved by the Minister of Finance (who issues the letters patent) and Licences To Commence And Carry On Business must be approved by the Superintendent. Such approvals are required by the federal statutes governing the specific financial institution.

1073. Each application is subject to the proposed financial institution meeting a number of criteria, and submitting detailed information in support of the application.

1074. The suitability and integrity of individuals responsible for the oversight and management are important prudential concerns for OSFI. The integrity and suitability of owners, directors and senior managers are verified upon incorporation or authorisation of a FRFI. The Minister of Finance considers an applicant's character, integrity, business record and experience and the competence and experience of the directors and senior officers. To incorporate a FRFI in Canada, the major direct and indirect (*i.e.* all beneficial) shareholders (detaining above 10 % of the shares), and the directors and senior officers of the applicant, must submit personal information on themselves including place and date of birth, current address, curriculum vitae, etc. This information is used by OSFI to evaluate whether they have the required qualifications and expertise to manage or direct a financial institution's business and affairs. They must also submit a completed OSFI Security Information Form so that the RCMP and CSIS can conduct security assessments. There are similar requirements in respect of the senior officers of foreign financial institutions that make applications to establish branches in Canada.

1075. Whenever there is a change in ownership through the acquisition of significant interest of a federally regulated financial institution, it has to be submitted to the approval of the Minister who will rely on the same type of controls as those performed at the time of the initial incorporation.

1076. However, there is no specific legal obligation in federal financial institutions legislation for FRFIs to implement screening procedures for those who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. In May 2007 OSFI issued a draft Guideline E-17: Assessment of Responsible Persons by FREs[131]. The purpose of the Guideline is to ensure that FRFIs implement policies and procedures to ensure that those individuals responsible for the oversight and management of financial institutions (defined in the Guideline as "Responsible Persons") are evaluated, both initially and on a regular basis, with respect to suitability and integrity (*i.e.* Fit and Proper).

Securities dealers

1077. The SRAs and SROs regulate the activities of securities dealers and other intermediaries from both a prudential and market conduct basis, including registering qualified member firms and employees. Participants in this sector must meet stringent capital requirements, demonstrate an ability and willingness to conduct its business in a manner consistent with securities legislation, and SRO rule books and are subject to ongoing supervision.

1078. Canadian securities laws contain various fundamental provisions regarding the licensing of market intermediaries. They set out: (1) the requirements to be registered, (2) exemptions from the registration requirements and (3) certain basic standards and requirements for registrants (for example, the duty to deal fairly, honestly and in good faith with clients), as well as rights of registrants. These fundamental provisions generally are incorporated into securities statutes.

1079. Canadian securities laws also contain more detailed requirements respecting registration. These more detailed requirements generally are incorporated into subordinate instruments such as regulations and rules. These more detailed provisions also may establish additional exemptions from the registration requirements. In addition to the requirements in Canadian securities laws, the IDA and the MFDA rulebooks contain complementary requirements which apply to their members as a matter of contract.

1080. The Canadian Securities Administrators (CSA), the coordinating body of Canadian SRAs, has undertaken a project to modernize the regulation of securities registrants. The CSA's Registration

131 This includes FRFIs.

Reform Project is intended to update, streamline and harmonize the categories of registration and the regulation of securities registrants in Canada, effective July 2008.

1081. There are three important general criteria to the fit and proper standard that applicants for registration must meet to be considered acceptable for registration: (1) proficiency; (2) financial stability; and (3) suitability, a concept that encompasses but is not limited to integrity. The core principles and most of the detailed provisions for registration are set out in Canadian securities laws. If an SRO has been authorised by an SRA to carry out certain registration functions, additional requirements may be set out in the SRO's rules.

1082. To be registered, a securities intermediary must demonstrate: (1) the appropriate financial resources to carry on the proposed business, such as the minimum capital requirements are met; and there are additional capital resources available to meet the continuing demands of the business; (2) adequate operational systems and controls for the businesses it proposes to carry on, such as proper books and records, internal controls, risk management, and supervisory systems; (3) senior management, with the appropriate knowledge, resources, skills and ethical attitude (including a consideration of past conduct) necessary to perform their proposed roles; (4) directors with the appropriate knowledge, resources, skills and ethical attitude (including a consideration of past conduct) necessary to perform their proposed roles; and (5) substantial owners/shareholders with the appropriate resources and ethical attitude (including a consideration of past conduct) necessary to perform their proposed roles.

1083. While Canadian securities laws do not provide detailed minimum criteria of suitability for registration, a general fit and proper requirement applies. Canadian securities laws authorise the SRAs to refuse to register a person or company if the applicant is not suitable for registration or the proposed registration is objectionable. An SRA will examine the applicant's past conduct, including the applicant's criminal record, employment history, history with the SRA and other regulators, civil actions against the applicant making allegations relating to the applicant's integrity and any other information that the SRA believes may reflect upon the applicant's suitability. The IDA and MFDA consider criteria similar to those considered by the SRAs in deciding whether to grant membership status to a firm or to approve an individual.

Provincially supervised insurance companies, agents and brokers

1084. A number of life insurance companies (about 10 %), representing a limited share of the sector in terms of premiums, are provincially registered and regulated. The requirements applying to them could not be examined and assessed in detail but it may be generally assumed that the registration process is subject to a similar scheme to OSFI's one, relying on a complete review of the business case and of the individuals' files. It is worth mentioning that the Canadian Council of Insurance Regulators has engaged a process aiming at harmonizing practices among the different provinces.

1085. Insurance agents are licensed and registered provincially in Canada. For example, FSCO issues licences authorizing persons to conduct business as insurance agents. There are three classes of agent licences: Life Insurance (including accident & sickness), Accident & Sickness, General. Agents listed may hold a combination of the insurance licences listed above. An insurance licence is issued by FSCO for a two-year term. Any person who acts as an insurance agent without being licensed is guilty of an offence under the Insurance Act, and may be prosecuted for such violation.

Licensing or registration of money or value transfer services

1086. The current legislation does not provide for a registration regime for persons or entities that are engaged in the business of money service business or foreign exchange dealing, that is persons and entities engaged in the business of foreign exchange dealing, of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments.

1087. The PCMLTFA currently requires these entities to abide by reporting, client identification, record-keeping and internal compliance requirements. FINTRAC has conducted significant outreach to identify MSBs, including presentations to community groups that use remittance services, searches of telephone records, reviews of ethnic newspapers, and advertising. The objective is to inform MSBs of their obligations and ensure they are included within the compliance program (i.e., Compliance Questionnaires, examinations, etc.).

1088. The sector is diverse, ranging from large multinational firms with many agents, which have developed strict checks before accepting their agents and oversight functions upon them, to individuals "operating in relative obscurity"[132], making the sector highly attractive to money launderers.

1089. In these conditions and in order to comply with FATF recommendations, Canada decided to create a registration regime in force in June 2008[133].

1090. To date, FINTRAC has been able to identify some 700 MSBs and foreign exchange dealers in Canada, largely located in major urban areas.

1091. FINTRAC has focused its examination resources in the MSBs sector with over 50% of all examinations over the last three years covering this sector. This reflects, in part, the risks associated with the MSB sector, as well as the absence of a flow of information from a primary regulator.

Ongoing supervision and monitoring – Recommendation 23

FINTRAC

1092. In order to effectively fulfill its role, FINTRAC has developed a National Compliance Program to ensure that reporting entities are complying with their obligations under the PCMLTFA. FINTRAC's compliance program makes use of risk management strategies to identify those sectors and reporting entities most in need of improving compliance. Efforts are focused on areas where there is the greatest risk of non-compliance and in which the failure to comply could have significant impact on FINTRAC's ability to detect and deter money laundering and terrorist financing.

1093. FINTRAC has developed the FINTRAC Risk Assessment Tool (FRAT) to assist compliance officers in assessing the risk of non-compliance by reporting entities and to centralize compliance information. When assessing the level of risk for reporting entities, FINTRAC looks at a range of factors, including such elements as open source information, reporting volumes, observations gleaned from outreach activities, voluntary information which FINTRAC has received on non-compliance, results from compliance questionnaires completed by reporting entities (see below), other database checks, information received from regulators, quality and quantity assurance reviews, and the results of compliance examinations.

---

[132] See "Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime" Consultation Paper, of June 2005.

[133] The PCMLTFA requires that all money service businesses register and creates a criminal penalty for operating an unregistered business. The application of the registration requirement includes informal money remitters commonly known as Hawala and is also applicable to departments and agencies of Her Majesty in Right of Canada, for example, postal orders. Section 11.11 of the PCMLTFA specifies persons or entities that are ineligible for registration, such those that have been previously convicted of a money laundering offence, a terrorist financing offence, an organized crime offence, any other criminal offence under the PCMLTFA and certain serious offences under the Controlled Drugs and Substances Act such as drug trafficking. FINTRAC is designated by the PCMLTFA to function as the Registrar and is responsible for accepting, denying, revoking and verifying applications for registration, maintaining the information contained in the registry and verifying compliance with the registration requirement. Registrants will have to inform FINTRAC of any material changes to their information within 30 days and renewal of registration will have to take place every 2 years or longer if prescribed by regulation

1094. Based on these risk factors, FINTRAC has assigned a general risk level to each reporting entity sector. This guides FINTRAC's overall compliance work (outreach, examinations, etc.) as in general, FINTRAC focuses more of its compliance resources on entities in higher risk sectors. FINTRAC also conducts assessments to rate the relative risk of non-compliance of entities and individuals within each sector. 26 000 entities are currently rated, which represents all big players and firms as well as some individuals.

1095. Compliance Questionnaires (CQs) are also used by FINTRAC to help focus examination resources, primarily for those entities at highest risk for non-compliance. FINTRAC developed the CQ as a tool to support its risk assessment and examination function. CQs are particularly useful as they can assist in assessing compliance levels in a large number of entities using relatively few resources.

1096. While the exact content of a CQ varies by sector, the CQ assists FINTRAC's Compliance team in assessing the risk of non-compliance within a particular entity by asking questions related to the size and scope of the reporting entity's operation, the institution where the entity does its banking (this information allows FINTRAC to cross-reference this entity with any reports that may have been filed by the bank), the entity's business lines, the implementation of a compliance regime, compliance policies and procedures, review of compliance policies and procedures and ongoing compliance training. CQs have proven to be an effective supervisory tool for FINTRAC.

1097. FINTRAC has sent over 3 000 CQs to financial institutions as of March 31, 2006. In 2006-07, FINTRAC is disseminating an additional 4 000 CQs to reporting entities (including DNFBPs) and 1 500 of these will be to the life insurance sector. The average response rate among financial institutions to CQs sent by FINTRAC is 89%: It should increase in the future since responding to these CQs is now mandatory as the amendment to the PCMLTFA, under section 63.1, which came into force in February 2007, requires reporting entities to "provide (…) the documents or other information with respect to the administration of Part 1 that [an] authorized person may reasonably require".

1098. In order to make it easier for reporting entities to respond to a CQ, they are now done electronically. Reporting entities receive a letter informing them that they have been selected to fill out a CQ. They are given a login and password and requested to go to FINTRAC's website to fill out the CQ on-line. In addition to facilitating responses, electronic forms assist FINTRAC Compliance Officers in scoring responses.

1099. Another key element that assists FINTRAC in its assessment of the risks of entities being non-compliant with their AML/CFT obligations is its consultation and coordination with other agencies that have responsibility for regulating entities covered under the PCMLTFA.

1100. The PCMLTFA permits FINTRAC to exchange compliance-related information with regulators at the federal and provincial levels. FINTRAC has signed Memoranda of Understanding to govern these information-sharing relationships (12 to date) with regulators of financial institutions. Under these MOUs, FINTRAC and the regulators on a regular basis exchange statistics, risk assessment information, examination results, and examination plans. FINTRAC also makes presentations and provide training to staff of MOU partners. In 2005-06, FINTRAC staff had 86 meetings with regulators and in 2004-05, 100 meetings of that type took place. The relationship with the regulators is still in its early stages, the first MOU having been signed in mid-2004 and the most recent in February 2007.

1101. As of September 30, 2006, FINTRAC had conducted almost 400 examinations of financial institutions, while its MOU partners had carried out more than 100 further examinations of financial institutions. These figures have to be compared to the total number of financial reporting entities which exceeds 100 000 (this figure includes individuals such as life insurance agents or securities dealers). However, FINTRAC examination may cover a large number of reporting entities (*e.g.* in the case of life insurance companies/agents and securities firms/dealers) and it is difficult to draw

definitive conclusions about supervisory coverage by comparing the reported examinations each year with the total number of reporting entities.

1102. The on-site portion of the examinations conducted by FINTRAC can, in practice, and depending on the size and complexity of the reporting entity, take anywhere from 3-4 hours to more than five days (in the case of a large, national reporting entity) to perform, which is somewhat less than average time spent by OSFI (see below). FINTRAC's examinations include sample testing of customers' transactions and files. The pre-examination stage, which can take weeks of preparation, consists of a review of documentation (including the results of audit reviews by FINTRAC MOU partners, a review of the entity's policies and procedures, etc.) that assists FINTRAC in scoping the on-site portion of the examination.

1103. A FINTRAC compliance examination will determine if the entity is meeting its obligations under the legislation. Areas of review can include:

- *Implementation of a compliance regime*: (1) The FINTRAC compliance officer will determine if a compliance officer has been appointed within the reporting entity and if this person is at the appropriate level and has the appropriate access to senior management; (2) The compliance officer will review the policies and procedures for compliance with the PCMLTFA that the reporting entity has established and assess them to determine if they are appropriate for the scope of the reporting entity's business and obligations under the PCMLTFA; (3) He will assess the entity's policies and procedures to determine their effectiveness. For example, large entities would be expected to have an annual external audit of their policies and procedures; (4) He will assess the on-going compliance training program that the entity has in place for any employees, agents or any other individual authorised to act on behalf of the reporting entity, including a review of such documentation as training materials, schedules, and agendas.
- *Reporting of all required transactions*: the compliance officer, who will have a detailed account of the entity's reporting history, will examine transaction records kept by the reporting entity to determine if a report (suspicious transaction, large cash transaction, electronic funds transfer or terrorist property) should have been filed by the entity.
- *Implementation of client identification requirements*: the compliance officer will examine records to determine if the reporting entity has identified its clients in a manner consistent with the PCMLTFA and regulations
- *Record keeping requirements*: the compliance officer will examine the reporting entity's records to determine if the entity has kept records in accordance with the PCMLTFA and regulations.

1104. So far, FINTRAC has concentrated most of its examination activities in the MSB, real estate, Credit union, *caisses populaires* and securities sectors: 86% of the examinations conducted by FINTRAC took place in these sectors.

1105. With regard to financial institutions, the following table shows the total examinations conducted by FINTRAC in each sector by fiscal year:

FINTRAC Examinations Conducted in Financial Institutions				
Sector	**2004-05**	**2005-06**	**2006-07 (as of end of Q2)**	**Total (by sector)**
Bank	0	1	0	**1**
CU/CP*	8	29	23	**60**
LI**	1	4	3	**8**
Securities	3	29	14	**46**
Trust & Loans	0	1	0	**1**
MSB	164*	56	43	**263***
TOTAL	**176**	**120**	**83**	**379**

**Note*: In fiscal year 2003-04, FINTRAC began to conduct examinations and completed a total of 26 examinations during the latter part of this time period. The focus of these examinations was largely on the MSB sector.

1106. At the end of 2005/06, FINTRAC had identified an average of 2.75 deficiencies, in general evenly spread across all categories: reporting, ascertaining identification, record keeping and compliance regime elements, as a result of its examinations.

OSFI

1107. FRFIs are subject to ongoing supervision by OSFI, based on its Supervisory Framework, a risk-based process to assess the safety and soundness of FRFIs developed in 1997/98, and released in 1999.

1108. The Framework evaluates the risk profiles of FRFIs, their financial condition, risk management processes and legislative compliance. The Framework evaluates inherent risks in the following areas: credit risk; market risk; insurance risk; operational risk; liquidity risk; legal and regulatory risk; and strategic risk. The Framework applies a risk-based supervisory approach to all types and sizes of FRFIs and which is administered on a consolidated basis. FRFIs are informed of OSFI's overall risk assessment, including a consolidated net risk rating. The risk assessment determines the type and extent of prudential supervisory work carried out on financial institutions.

1109. OSFI's AML/CFT methodology is broadly based on the approach taken in the Supervisory Framework. However, inherent risk measurement for AML/CFT purposes is based primarily on the product mix offered by financial institutions, together with the geographical spread of operations. For example, institutions which focus heavily on retail deposits and lending, or which offer correspondent banking services, or where insurance products have large cash values are ranked at higher risk than those that focus primarily on term insurance products or that have little or no deposit taking.

1110. OSFI considers inherent risks associated with money laundering and terrorist financing as a factor of operational risk as well as legal and regulatory risk. Therefore, at the highest level, issues such as weak AML/CFT controls can potentially harm the reputation of FRFIs. Although the Framework does not formally recognize reputation risk as an identified area of risk, OSFI typically treats reputation risk as a composite inherent risk arising from underlying risks, especially operational risk and legal & regulatory risk.

1111. The quality of risk management controls for prudential supervision is viewed from the following perspectives; operational management; financial analysis; compliance; internal audit; risk management; senior management and board oversight. Net risk is defined as inherent risks, mitigated by risk management control functions. Similarly, for AML/CFT purposes, OSFI examines the risk management controls exerted by the Board, senior management, compliance and internal audit when conducting AML/CFT assessments to conclude whether the inherent risks of ML/TF are being managed appropriately. Because this process differs from the analysis of traditional prudential risks to capital and earnings, OSFI has placed AML/CFT assessment into a separate unit (Compliance Division) and not in its Supervision Sector.

1112. OSFI supervises a large number of institutions that deal in a very significant amount of total assets and that offer a broad range of financial sector activities as shown by the following table.

Type of Federally Regulated Financial Institution	No. of federal institutions FRFIs	Total Assets (CAD 000) Q3 2006	%
Six largest Conglomerate Domestic[134] banks and affiliates	9	CAD1 990 039 189	69.4
All other Domestic Banks	13	CAD 37 044 174	1.3
Subsidiaries of Foreign Banks	21	CAD 120 204 087	4.2
Branches of Authorised Foreign Banks	24	CAD 48 262 271	1.7
Trust and Loan Companies	30	CAD 16 852 035	0.6
Trust and Loan Companies subsidiaries of	20	CAD 212 553 043	7.4

[134]. "Domestic " means the entity was incorporated in Canada by Letters Patent under the appropriate governing legislation and is not a subsidiary of a foreign bank.

Type of Federally Regulated Financial Institution	No. of federal institutions FRFIs	Total Assets (CAD 000) Q3 2006	%
Canadian banks			
Cooperative Credit Associations [1]	7	CAD 11 889 712	0.4
Cooperative Retail Associations	1	CAD 3 236 524	0.1
Three largest Conglomerate Domestic Life Insurance Companies and their affiliates	9	CAD 365 692 000	12.8
All other domestic Life Insurance Companies	30	CAD 45 506 966	1.6
Branches of Authorised Foreign Life Insurance Companies	41	CAD 16 291 088	0.5
Total	215	CAD 2 866 584 842	100

[1] 4th quarter 2005.

1113. Since 2002, OSFI has conducted on-site assessments to assess FRFIs AML/CFT programs. These assessments assess both the quality of AML/CFT risk management at such institutions, including their subsidiaries and branches both within and outside Canada, as well as their ability to comply with their obligations under the PCMLTFA and Regulations. The results of these assessments are shared regularly with FINTRAC. Quarterly meetings are also held with FINTRAC to, among other things, review these results.

1114. OSFI's current AML/CFT methodology was developed in 2002 and subsequently refined to reflect its experience in assessing financial institutions. OSFI has instituted a target frequency of about 3 years for institutions presenting higher inherent risk. This includes all conglomerate banks and most conglomerate life insurance companies, and is generally consistent with OSFI's regular prudential examination cycle. Smaller entities will be risk ranked using various ML/TF risk criteria unrelated to financial risk (capital, earnings, liquidity, etc). Smaller entities that present medium to high inherent risk (due to their business profile matched against the AML/CFT criteria) will also be cycled through an assessment approximately every 3 years. The small, low- to no-risk entities will be the subject of regular monitoring with on site work taking place at longer intervals.

1115. On-site assessments typically involve:

- Iinterviews with senior management of risk control functions (AML, Internal Audit, and Risk Management) and selected lines of business.
- Review of systems technology used to support transaction reporting to FINTRAC, including business rules and lines of accountability.
- review of account opening procedures and sample customer files in business lines selected for their exposure to ML and TF.
- Exit meeting to verbally communicate principal findings and recommendations in advance of the written supervisory letter.

1116. Moreover, OSFI also administers a program to support implementation of, and ensure compliance with, section 83 of the Criminal Code, section 7 of the PCMLTFA, FINTRAC Guideline 5, the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), United Nations Al-Qaida and Taliban Regulations (UNAQTR), the United Nations Democratic People's Republic of Korea Regulations and the regulations to implement the United Nations Security Council Resolution 1737 on Iran. Under this program OSFI includes in its AML/CFT assessment methodology a review of the policies and procedures in place at FRFIs to assure compliance with their obligations to search for terrorist and terrorist entities and freeze their assets and report thereon to the RCMP, CSIS and OSFI. OSFI has emphasised to all federal financial institutions that the terrorist name searches must be done on a regular basis to comply with the "continuous" search requirement in the UN regulations and the Criminal Code regulations. Generally, deposit taking institutions and large conglomerate life insurance companies are expected to perform a full search for listed persons' names at least weekly, with larger institutions, including the five largest conglomerate banks, scrubbing customer name databases as frequently as daily.

1117. The examination of a conglomerate bank takes on average 2 to 3 weeks of preparation and 3 weeks of on-site work involving a team of about six persons. On-site work comprises a review of AML/CFT policies and procedures and reports generated by or for risk management control functions, interviews with senior management of risk control functions and selected lines of business, review of system technology used to support transaction reporting to FINTRAC and review of account opening procedures and sample customer files in business lines selected for their exposure to ML and TF.

1118. OSFI supervises financial institutions on a consolidated basis. It regularly reviews the operations of conglomerate banking and insurance companies with significant operations outside Canada, and the AML/CFT assessment program is included in this approach. Since the inception of the AML/CFT assessment program OSFI has reviewed selected financial institutions' offshore operations to test the effectiveness of their enterprise-wide AML/CFT standards. From 2002 to date OSFI has conducted reviews, of varying scope, in subsidiary and/or branches of FRFIs located in the UK, Jamaica, Mexico, Cayman Islands, Jersey, and Guernsey.

1119. In recent assessments of conglomerate financial institutions with securities subsidiaries, and as part of its consolidated supervision responsibilities, OSFI has also tested the effectiveness of these standards in securities dealer subsidiaries of a number of banks. Such securities dealers are regulated by the IDA.

1120. OSFI conducted 73 AML/CFT assessments from November 2002 to December 2006, including 6 follow-up assessments on institutions identified as having significant weaknesses in AML/CFT controls. OSFI has also conducted 5 projects consisting of thematic work associated with cross-sector activity, or assessments of selected Canadian Bank subsidiary operations located outside Canada. In 2006, OSFI upgraded the quality of its assessment work and focused primarily on more labour intensive second generation AML/CFT assessments at Canada's 6 largest banks. These banks had previously been assessed in either 2003 or 2004. Although the total number of assessments conducted by OSFI in 2006 (13) was lower than in 2005 as a result, each assessment was far more significant in scope. Five of the 13 assessments conducted by OSFI in 2006 therefore covered a grand total of 40 FRFIs (comprising 12 banks, 5 life insurance companies and 23 trust and loan companies).

1121. In summary, the 2006 AML/CFT assessment program covered a total of 40 FRFIs, which in turn comprised 87% of the assets of all federally regulated deposit-taking institutions and about 75% of the assets of all FRFIs, gave both FINTRAC and OSFI quite a thorough view of the state of AML/CFT compliance and risk management controls in the federally regulated sector in Canada.

1122. In 2004, OSFI entered into a Memorandum of Understanding with FINTRAC under which OSFI and FINTRAC agreed to share information related to federal financial institutions' compliance with Part 1 of the PCMLTFA. The MOU was authorised under the Public Safety Act, which removed previous restrictions in the PCMLTFA on the ability of FINTRAC to share such information with financial regulators. It also removed similar restrictions under the Office of the Superintendent of Financial Institutions Act, which had prevented OSFI from sharing compliance information with FINTRAC. As a result of the MOU, the PCMLTFA and its Regulations, when combined with FINTRAC Guidelines and OSFI Guideline B-8 represent the primary instruments for reviewing the implementation of AML/CFT requirements in the federally regulated financial sector in Canada. FINTRAC now receives each examination findings letter sent to a FRFI and discusses each in detail at regularly scheduled quarterly meetings with OSFI, unless more urgent discussions are required. FINTRAC also sees all of the action plans.

1123. The following table summarizes the number of OSFI on-site AML/CFT assessments and projects from 2002 to 2006:

Type of actions	2002	2003	2004	2005	2006	Total
Assessments undertaken	5	12	11	29	10	67
Follow-up Assessments	0	0	1	2	3	6
Sub Total	**5**	**12**	**12**	**31**	**13**	**73**
Thematic Projects	0	0	2	2	1	5
Total Assessments and Projects	**5**	**12**	**14**	**33**	**14**	**78**
Required Actions	5	29	31	128	29	222
Recommended Actions	21	66	49	185	62	383
Total Actions	**26**	**95**	**80**	**313**	**91**	**605**

1. The following table summarizes the reasons for intervention that OSFI has made at FRFIs.

Subject	Required Action	Recommended Action	Total
AML/CFT Policy Development & Implementation	17	69	86
Self-Assessment Program Implementation	14	57	71
Independent Procedures Testing & Reporting	11	47	58
Role of the CAMLO	6	43	49
Total Oversight Recommendations	**48**	**216**	**264**
Training	16	26	42
Large cash transactions, Suspicious transactions and Electronic fund transfers	7	43	50
Customer Identification Issues	69	65	134
Other Business Line Specific Issues	26	18	44
Retention of records	2	2	4
Outsourcing	1	3	4
Terrorist Searching and Freezing	55	8	63
Total Operational Recommendations	**176**	**165**	**341**
Grand Total	**224**	**381**	**605**

1124. In 2005 OSFI improved the scope of AML/CFT assessments by including more detailed assessments of the various lines of businesses at the conglomerate banks (including lines believed to have a higher vulnerability to ML/TF) and a consistent focus on customer record keeping. The conglomerate reviews post-2005 are referred to as "second generation assessments".

IDA

1125. The IDA's Sales Compliance Department ensures that member firms implement policies and procedures to comply with all non-financial regulatory requirements, including those of the IDA, provincial securities acts and federal legislation including the PCMLTFA. The IDA's Sales Compliance staff conducts regular reviews and on-site examinations of member firms, focusing on issues of compliance, anti-money laundering due diligence, supervision, corporate finance and research, employee activities and internal controls; 70% of staff time is spent directly on member firm reviews.

1126. The Sales Compliance Risk Assessment Model helps identify, define, assess and weigh risks in respect to IDA member business activities and behaviour patterns to assist in determining the frequency, scope and principal focus of the individual Sales Compliance Reviews to be conducted for each firm. The objective of the Risk Assessment Model is to identify member firms having a higher than average probability of being found to be non-compliant. To achieve this, the Association runs both qualitative and quantitative evaluations for every dealer and combines their respective outcomes into a single Net Residual Risk score. With this information, the IDA ensures that its regulatory focus is placed on higher risk firms. These objectives are enhanced by the model's ability to indicate the comparable risk assessed for each member firm relative to all other firms under the jurisdiction of the IDA – and to subsets, or "peer groups," of firms engaged in comparable activities.

1127. Providing best practice guidance and rule interpretations is also part of Sales Compliance's work, as well as providing feedback on policy development to the Regulatory Policy Department.

1128. The IDA uses its sales compliance risk assessment model to assist in assigning firms to examination cycles. The cycles are: annual for high risk firms; every 18 months for large, integrated firms; 2 years for low risk firms; a five-year cycle is assigned to minimal risk firms, such as dealers of Alternative Trading Systems (which provide facilities through which other dealers and large institutions trade) and proprietary-trading only firms that have no clients and therefore do not present any risk to IDA rules.

1129. In other respects, the Enforcement Department of the IDA may undertake investigations into the conduct, business or affairs of its members and their employees. Investigations can also be undertaken on the basis of: a complaint received from a member of the public; a directive from the IDA's Board of Directors; a request from an SRA; or any information obtained or received by the IDA.

1130. The Investigator reviews the findings of the investigation and makes a recommendation as to whether there appears to be sustainable evidence that a breach of the Association's By-laws, Regulations or Policies has occurred. Files with insufficient evidence are closed and files with sufficient evidence are sent to the Association's Enforcement Counsel for prosecution.

1131. The IDA provides AML/CFT findings to FINTRAC under an MOU, and had previously provided such information voluntarily. The IDA provides FINTRAC with its review schedule, periodic compendia of deficiency findings involving AML/CFT issues and the remedial action taken by firms. The IDA also provides information to FINTRAC to assist it in the risk assessments it uses to determine what reporting entities it will audit.

1132. From 2001 to 2005 the IDA conducted 526 head office and 100 branch office reviews. Some separate reviews of large branches were also conducted, however, the IDA generally conducts branch reviews in conjunction with a head office reviews to understand how compliance controls are operating at all levels.

MFDA

1133. The activities of the MFDA's Enforcement Department are integral in providing firm, fair and transparent regulatory processes in enforcing the MFDA requirements that enhance investor protection. The activities of the Enforcement Department also directly support the MFDA's goal of participating in the Canadian securities regulatory framework, by developing and maintaining collaborative working relationships with other securities regulatory authorities and law enforcement agencies. The MFDA's Enforcement Department investigates when MFDA member firms and their registered persons breach its rules.

1134. The Enforcement Department receives referrals of the results of sales compliance examinations done by the MFDA Compliance Department, where the nature or extent of the examination results exceeds a threshold that the MFDA has established to identify areas where Enforcement action is required in addition to resolution through normal Compliance follow-up process. The MFDA has committed by letter to FINTRAC that it will report any such referrals that identify situations of non-compliance with AML detected during MFDA Sales Compliance examinations. To date, there have been no findings of conduct exceeding the threshold that would require reporting to FINTRAC under this arrangement.

OSC

1135. The OSC, in its reviews of registrant firms, assesses firms according to an internally developed risk management tool to help focus its resources on the relatively higher risk firms. A regular field review includes a review of the operations of the firm including, for example, detailed testing of portfolio management functions, trading functions, conflicts of interest, financial condition, money laundering, etc. Know your client and suitability reviews are done as part of testing of the portfolio management and trading functions. The review of money laundering is limited to ensuring there are policies and procedures in place to comply with money laundering legislation, and testing of client

identification procedures as part of know your client and suitability reviews. The OSC does not publicly disclose its review cycles.

DICO

1136. DICO conducts inspections of its members' compliance with AML/CFT legislation during its regularly scheduled on-site verifications and reviews. DICO inspects all member institutions on a regular basis with frequency determined by size, complexity and risk. At a minimum, each institution is reviewed at least once every three years. Inspections of the money laundering policy and anti-terrorism aspect of the inspection module is rather marginal and the controls in that area remain limited to a rapid examination of procedures and policies (2 hours on average), without sample testing of transactions or files but can take a longer timeframe should major deficiencies were noted. A copy of the report is also provided to FINTRAC.

1137. During the course of the review, should it come to the attention of the inspector that the member has failed to comply with the requirements of the Money Laundering Legislation review, DICO requires the member to provide an Action Plan to address the identified issue. The Action Plan is also provided to FINTRAC for their agreement. DICO will follow to ensure the Action Plan is implemented as set out.

AMF

1138. Under the AML Act, the Desjardins federation, the joint supervisor of the *caisses populaires* with the AMF, must inspect the internal affairs of each *caisse populaire*, including that AML/CFT requirements are being followed, at least once every 18 months and must transmit to the AMF its findings. AMF relies mainly on these reports and performs seldom on-site reviews at Desjardins *caisses populaires*, favouring a "second level" control on this sector.

FSCO

1139. FSCO licenses and regulates insurers that sell life and health insurance in the province of Ontario to ensure they comply with the provincial market conduct legislation. In Ontario, life and health insurance products are sold to consumers directly by companies or through insurance agents. All agents (as defined in the Insurance Act of Ontario) are required to be licensed with FSCO.

1140. FSCO monitors, investigates and takes appropriate regulatory action when there is non-compliance with legislation and regulations that relate to the regulated sectors. Non-compliance may result in enforcement action.

Comments from the assessment team in relation to Recommendations 29 & 17

1141. The previous developments illustrate the unequal degrees of regulation and supervision, depending on the sectors and provinces although OSFI is responsible for regulating well over 80% of the financial sector, by total assets.

1142. The number of examinations performed by FINTRAC appears to be small compared with the total number of reporting financial entities (more than 100, 000) although FINTRAC examination may cover a large number of reporting entities (*e.g.* in the case of life insurance companies/agents and securities firms/dealers). Even including examinations conducted by FINTRAC's MOU partners, which except for OSFI's are not always as detailed as FINTRAC's (see in this respect DICO's assessments which are generally made in 2 hours), the figures remain rather low, except for the banking and federally regulated trust and loan companies sectors which have a good supervisory coverage by OSFI.

1143. The securities sector seems to be regularly controlled, though on a lesser extent, as non IDA or MFDA members are regulated by provincial SRAs which do generally review policies and procedures but do not perform a thorough testing of AML controls in their on-site reviews.

1144. The on-site AML/CFT assessments conducted by OSFI since 2003 at the major life insurance companies have represented 90% of the industry measured by its assets but less than 10% of the supervised population. The supervision appears to be weak for life insurance agents as AML/CFT controls relies mainly upon FINTRAC's actions. In addition, despite the focus put on that sector, FINTRAC had managed to perform controls on only 60 credit unions and *caisses populaires* up to mid-2007, out of a total population of 1 250 reporting entities.

1145. It should also be noted that except for the main sectors like FRFIs, FINTRAC does not take into account the quality of the supervision by the primary regulators in its risk assessment tool, and the assessment tool is focussed significantly on the risk of non-compliance with the legislative and other requirements, as compared to the risk of money laundering and terrorist financing.

Statistics

1146. Canada provided statistics regarding the on-site examinations conducted by FINTRAC and its MOU partners relating to or including AML/CFT during the last three fiscal years. On the other hand, there was no statistics centrally available concerning the involvement of supervisors which have not signed an MOU with FINTRAC in AML/CFT compliance oversight (number of on-site reviews, sanctions taken). Such information would certainly be useful to help FINTRAC implement an effective risk-based compliance supervision program.

Guidelines – R.25 (Guidance for financial institutions other than on STRs)

FINTRAC

1147. FINTRAC provides Guidelines on its website for reporting entities and the general. Cumulatively, these Guidelines provide reporting entities with an understanding of all of their requirements and obligations under the PCMLTFA. Furthermore, these Guidelines all include a section on how to contact FINTRAC for more information if it is required.

1148. Aside from the Guidelines themselves, FINTRAC's website also contains information tailored specifically to the needs of the various reporting sectors. The information on the website for each of the sectors covers what needs to be reported, record keeping, ascertaining identification, third-party determination, and information on the compliance regime requirements and compliance questionnaires. For each reporting sector, the information can be found on FINTRAC's website.

1149. In addition, FINTRAC launched, in March 2005, an additional type of guidance in its FINTRAC Interpretation Notices (FINs), which are documents developed by FINTRAC to provide explanations and clarifications regarding certain provisions contained in the PCMLTFA and its Regulations. FINs are primarily used by FINTRAC staff, reporting entities and their legal counsel, and other individuals who have an interest in having clear interpretations of some key aspects of the PCMLTFA. To date, four FINs, have been developed, dealing with specific topics concerning money services businesses/foreign exchange dealers, accountants, securities dealers and banks. The following FINs are available on FINTRAC's website: (1) Criteria for determining if an entity is "Engaged in the Business of Money Services Business or Foreign Exchange Dealer" (Annex B10); (2) Accountants - Giving Instructions Versus Providing Advice (Annex B11); (3) Opening an Account for a Person or Entity Engaged in the Business of Dealing in Securities Only Outside of Canada (Annex B12); and (4) Large Cash Transaction and Electronic Funds Transfer Reporting Requirements: Two or More Transactions in a 24-Hour Period (The '24-Hour Rule') (Annex B13).

1150. FINTRAC is currently in the process of updating the guidelines and FINs to take into account amendments to the PCMLTFA and regulations.

1151. FINTRAC also undertakes an extensive outreach and assistance program for reporting entities that includes information sessions, presentations at industry conferences (in 2004-05 and 2005-06, FINTRAC participated in nearly 1 300 presentations involving more than 27,000 participants), articles

in trade magazines, and has developed and published sector-specific information sheets and pamphlets for distribution to reporting entities. FINTRAC provides these publications to reporting entities free of charge, and they are also available on FINTRAC's website. In addition, FINTRAC operates a call centre that is open 12 hours a day from Monday to Friday, to answer general inquiries about FINTRAC's operations, as well as more specific questions about reporting requirements and systems. In 2005-2006, FINTRAC received 3,253 inquiries through the call centre, mostly from reporting entities.

1152. In general, FINTRAC guidance is aimed at explaining and detailing the obligations that different sectors have under the PCMLTFA and its regulations. The Guidelines are supplemented by significant outreach activity undertaken by FINTRAC through regular meetings and presentations at conferences and meetings of industry associations. However, they give few indications on how tailoring them and putting them effectively into practice in the various financial sectors. Further guidance to assist their respective financial institutions in complying with AML/CFT requirements that may be detailed in various statutes may be provided by prudential regulators but it is not yet generalised (see life insurance sector, for example).

OSFI

1153. In early 1990, in support of the initiatives resulting from the 1989 G-7 Paris Summit, OSFI implemented for adoption by federal deposit-taking institutions, a Best Practices Paper to Deter and Detect Money Laundering. The key best practices contained in the paper focused on the following areas: (1) designating an officer within the financial institution to be responsible for compliance with the procedures; (2) implementing a system of formal internal controls procedures to deter and detect money laundering that included a source of funds declaration; (3) implementing a system of independent procedures testing; (4) implementing a record retention policy; (5) developing and providing appropriate training to financial institution staff on AML.

1154. In 1996, the Best Practices paper was converted to a formal OSFI guideline and revised to reflect changes implemented as a result of the promulgation of the Proceeds of Crime (money laundering) Act and Regulations. It also added further insights into deterring and detecting money laundering, such as the adoption of an annual Self Assessment Program, as well as a program of (voluntary) suspicious transaction disclosure to law enforcement.

1155. In addition the application of the guidance was extended to federal life insurers in 2001. In 2002 the guideline was further amended to add CFT requirements. Further changes are contemplated in the near future for the OSFI Guideline B-8, Deterring and Detecting Money Laundering and Terrorist Financing, which was last revised in November 2004. In addition, OSFI commenced offering information sessions to the industry in 2005 and continued to do so in 2006.

1156. It may be noted that this Guideline is more specifically suited to the banking sector than to life insurance companies The life insurance industry trade association (CLHIA) has developed in consultation with FINTRAC a guidance Manual intended for helping life insurance agents and brokers across Canada meet their AML obligations. CLHIA and LIMRA (Life Insurance Marketing and Research Association) have also developed jointly supporting on-line training lessons for Canada's life insurance agents and brokers. At the time of the evaluation the guidance Manual and the training lessons were not yet available. Representatives from OSFI have also spoken at a number of sessions on money laundering at various life insurance and banking sector industry educational events.

IDA

1157. The IDA provides regular notices to its members on developments in regulations, including the PCMLTFA, along with information on risks and trends. The IDA developed a guide, Deterring Money Laundering Activity: A Guide for Investment Dealers to help members effectively develop effective anti-money laundering programs in compliance with anti-money laundering and anti-terrorist financing obligations. In general, the guide discusses requirements under the PCMLTFA and refers to

guidance available from FINTRAC, know your client procedures, suspicious transaction reporting, monitoring of account activity, anti-money laundering training, audit program and relationship between introducing and carrying brokers.

1158. Representatives from the IDA have also spoken at a number of sessions on money laundering at various industry educational events.

3.10.2 Recommendations and Comments

1159. The Canadian AML/CFT supervisory structure has several significant weaknesses:

- The exclusion from the AML regime of a number of categories of financial institutions without proper and formalized prior risk assessments or without adequate justifications of low AML risks.
- Heterogeneous levels of AML compliance oversight in the different financial sectors, which is due to an insufficient level of compliance staff resources in FINTRAC compared to the number of reporting entities, and to variable levels of involvement by the various primary regulators (MSBs, life insurance intermediaries, some provincial credit unions and *caisses populaires*, etc.).
- The lack of adequate sanctions provided to FINTRAC under the PCMLTFA which is not compensated by the sanctions administered under their own statute by the other primary regulators (since the regime of administrative monetary penalties is not in force yet).
- The current absence of a registration regime for money service businesses and foreign exchange dealers (since the registration regime adopted in June 2007 will only be in force in June 2008).

1160. Canada could consider allowing FINTRAC to delegate formally its authority to examine financial institutions for AML/CFT compliance to its MOU partners and other primary regulators, so that the basis for their intervention in that area is sound and clear and in order to leverage existing examination resources and to avoid possible duplication of compliance inspections. Such a measure would also ensure a better knowledge by the AML compliance supervisor of the specifics of the sector. Such a delegation should go together with the settling by FINTRAC of objectives (frequency, coverage of risks) and common rules and standards for the conduct of examinations and inspections on its behalf by its partners.

1161. More generally, Canada should encourage the development of specific AML/CFT guidance by the various primary provincial regulators and a more active involvement in AML/CFT supervision. It could also envisage encouraging the creation of SROs in sectors which are less regulated, such as life insurance brokers or MSBs. It is essential too that sufficient resources be dedicated to the supervisory authorities responsible for AML/CFT oversight.

1162. The strengthening of the sanctions regime with the introduction of administrative and monetary penalties, as included in the amended PCMLTFA, should be a crucial enhancement for the effectiveness of the Canadian AML/CFT system. The delegation of the administration of these sanctions to the MOU partners could also be envisaged.

1163. Canada should ensure that market entry rules among the different provinces and sectors are compliant with FATF requirements.

1164. Finally, the creation of a registration regime for the MSBs will be an essential step in the necessary strengthening of the AML supervision of this highly risky sector.

3.10.3 Compliance with Recommendations 17, 23, 25, 29 & 30

Rec.	Rating	Summary of factors underlying ratings
Rec.17	PC	• With the exceptions of OSFI and IDA regulated institutions, only criminal sanctions are available to FINTRAC under the PCMLTFA for all other types of financial institutions and these are only applicable for the most serious failures, and need to be proved to the criminal standard. • OSFI only uses a limited range of actions/sanctions in the AML/CFT context (namely supervisory letters and in a limited number of cases, staging). • The lack of effective sanctions applied in cases of major deficiencies raises real concern in terms of effectiveness of the sanction regime, particularly taking into account that only one criminal sanction and a very limited number of administrative sanctions have been applied.
Rec.23	PC	• Exclusion from the AML/CFT regime of certain financial sectors (such as financial leasing, factoring, finance companies, etc.) without proper risk assessments. • For the financial institutions subject to the PCMLTFA, there is a very unequal level of supervision of AML/CFT compliance, with certain categories of financial institution appearing to be insufficiently controlled (MSBs, certain credit unions/*caisses populaires*, life insurance intermediaries…). This is due to the limited staff resources of FINTRAC dedicated to on-site assessments compared to the high number of reporting entities, which has not always been compensated by the involvement of the primary prudential regulators in AML/CFT issues. • "Fit and proper" requirements are not comprehensive. • At the time of the on-site visit, there was no specific obligation for FRFIs to implement screening procedures for persons who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. • There is currently no registration regime for MSBs.
Rec.25	LC	• There is a lack of specific guidelines intended for sectors such as life insurance companies and intermediaries.
Rec.29	LC	• FINTRAC has no power to impose administrative sanctions.

3.11 Money or value transfer services (SR. VI)

3.11.1 Description and Analysis

1165. *Definition*. Under the PCMLTF Regulations, "*money services business*" means a person or entity that is engaged in the business of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments. It includes a financial entity when it carries out one of those activities with a person or entity that is not an account holder.

1166. To assist the private sector, FINTRAC Interpretative Note March 1, 2005 provides guidance on what it means to be "engaged in the business".

1167. A business is considered to be a MSB if any of the following applies: (1) the business issues or redeems money orders, traveller's cheques or other similar negotiable instruments for more than CAD1 000 with the same person on the same day; (2) the individuals running the business advertise (by means of newspaper, television, yellow pages, Internet, any other media, or by an interior or exterior sign) the fact that they engage in the activity; (3) the business holds a permit or licence related to the activity; (4) the business is registered as someone carrying on the activity; or reports the income of that activity as income from a separate business for tax purposes". Money services businesses include alternative money remittance systems, such as Hawala, Hundi, Chitti, etc.

1168. *Issue of registration/licensing*. At the time of the assessment, there were no federal licensing requirements in place for MSBs. Under the Canadian constitution, licensing of these types of businesses falls within the powers of the provincial governments. However, given that Canada's

AML/CFT legislation is a federal Act and after consultation with the provinces, Canada has moved to create a federal registration regime[135]. At the time of the on-site visit, some provinces regulated the sector, but only in relation to "payday" lending services and in respect of customer protection rules.

1169. FINTRAC has made use of different techniques in identifying MSBs and raising awareness in this sector, including: (1) searching telephone and business directories; (2) field research (walk/drive through neighbourhoods looking for commercial signs); (3) awarded contracts to conduct searches for advertisements in ethnic newspapers; and (4) held regional open house workshops on legislative obligations (all MSBs were sent an invitation). Generally speaking, FINTRAC's outreach activities with the MSB sector include overview presentations about FINTRAC, and presentations concerning reporting entities' obligations under the PCMLTFA and its associated regulations.

1170. With these measures, FINTRAC has been able to identify some 700 MSBs in Canada, largely located in major urban areas. The market is dominated by a few large firms but is also composed of a vast number of relatively small entities compared to other types of reporting entities in the financial sector. However, it has been very difficult to build a complete inventory of the sector since many money services are a part of other businesses such as travel agencies, small grocery stores and gas stations; and they might not advertise. Complicating the task further, these services go in and out of business at a high turnover rate.

1171. The MSB sector has generated more STRs than banks since 2001, with almost one third of all STRs received by FINTRAC coming from this sector. Nevertheless, detailed statistics show that only a limited number of MSBs (mostly the largest players) report STRs to FINTRAC. The following table shows the MSB sector compared with all reporting entities from 2002 to 2006:

	MSB	Total reporting entities	% of Total
Number of reporting entities	about 700	Over 300 000	0.2
Suspicious Transaction Reports	33 426	102 835	33
Large Cash Transaction Reports	214 247	15 800 939	1.4
Electronic Fund Transfer Reports	96 790	29 328 058	0.3

1172. One of the key challenges the larger players currently face is the selection of agents in which some of the bigger MSBs will conduct extensive checks on individual companies and criminal records checks on individuals but this does not apply in all cases. The key players met by the assessment team indicated that they would like the sector to be licensed as it would build market confidence and image.

1173. *Application of the FATF Recommendation*s. The MSB sector is subject to client identification, record keeping and reporting requirements under the PCMLTFA. However, the preventive measures currently applicable to financial institutions including MSBs in Canada (especially in relation to CDD, reporting of suspicious transactions or SRVII) present very serious weaknesses (see in particular Sections 3.2, 3.5 and 3.7 of the report). The MSB sector is therefore subject to a limited range of preventive measures that are not in compliance with international standards.

1174. *Monitoring.* FINTRAC is responsible for supervising the MSB sector for AML/CFT purposes[136]. *In order to* fulfill its responsibilities effectively under section 62 of the PCMLTFA, FINTRAC has established a compliance program. In particular, FINTRAC has made use of Compliance Questionnaires (CQs) (see Section 3.10 of the report). As part of its outreach activities,

[135] A registration system is due to come into force on 23 June 2008. Individuals and entities that engage in MVT services will be required to register with FINTRAC. The registration regime is designed to facilitate compliance with existing obligations under the PCMLTFA and to help FINTRAC supervise an otherwise unregulated sector. It will also create a new criminal offence for operating an unregistered MSB.

[136] Under regulations enacted in June 2007 and in force in June 2008, FINTRAC is responsible for accepting, denying, revoking and verifying applications for registration, maintaining the information contained in the registry and verifying compliance with the registration requirement.

FINTRAC has also had 149 meetings with entities in that sector since 2004-05, which involved over 400 participants (12% of FINTRAC outreach activities (presentations and meetings) over the last three years have been targeted at entities from that sector and 29% of all CQs having been sent to entities in the sector).

1175. The following table illustrates the percentage of positive responses to questions in the CQ about key compliance elements (as of the end of 2005-06):

AREA OF COMPLIANCE	MSB
Implemented Compliance Regime	85%
Designated Compliance Officer	75%
Implemented Compliance Policies & Procedures	91%
Review of Policies & Procedures	77%
Ongoing Compliance Training	71%

1176. The following table indicates the number of FINTRAC examinations conducted in the MSB sector:

Sector	2004-05	2005-06	2006-07 (as of end 09/06)	Total (by sector)
MSB	164	56	43	263*
All Other Financial Institutions	12	64	40	116
Total	176	120	83	379

Note: In fiscal year 2003-04, FINTRAC began to conduct examinations and completed a total of 26 examinations. The focus of these examinations was largely on the MSB sector.

1177. FINTRAC has, to a significant degree, focused its examination resources in the MSB sector, especially in the early years, with 69% of all its examinations of financial institutions having been conducted in that sector over the last 2.5 fiscal years (about 40% of the identified MSBs have been examined by FINTRAC) but clearly there is scope for further progress in this area although it should be noted that a single FINTRAC examination covers the parent entity and potentially may cover many agents of the MSB.

1178. *List of agents*. There is currently no legal requirement for each MSB to maintain a list of agents[137].

1179. *Sanctions applicable to MSBs failing to apply the AML/CFT requirements*. At the time of the on-site visit, under the PCMLTFA, FINTRAC could not impose penalties to MSBs failing to apply the PCMLTFA and its Regulations but only had the option of referring a case of non-compliance to law enforcement for investigation and prosecution (see Section 3.10 of the report)[138]. To date, FINTRAC has disclosed seven such cases of non-compliance to law enforcement agencies and one MSB operator has been convicted for non-compliance with the PCMLTFA and for money laundering. However, at the time of the on-site visit, the sanction regime available to FINTRAC was not effective, proportionate and dissuasive.

1180. *Additional element*. The Best Practices Paper for SRVI outlines five areas in which preventative measures should be considered, namely: licensing/registration; identification and awareness raising; AML Regulations; compliance monitoring and sanctions. In terms of compliance monitoring, a substantial body of work has already been conducted in this field by FINTRAC, along the

[137] The registration regime enacted in June 2007 and coming into force in June 2008 requires the MSBs to submit a list of agents to FINTRAC as part of the registration process (see Schedule 1 Part C of the PCMLTF Registration Regulations).

[138] The PCMLTFA enacted measures in December 2006 that come into force in December 2008 and introduce a new regime of sanctions.

recommended lines in the Best Practice Paper. Other elements were very partially in place at the time of the on-site visit although the overall implementation of the Best Practices Paper should significantly improve after the introduction of the regulatory changes under the PCMLTFA.

3.11.2 Recommendations and Comments

1181. Canada should ensure effective implementation of the registration system for MSBs in force in June 2008 and ensure that the requirements applicable to MSBs fully meet the FATF requirements.

3.11.3 Compliance with Special Recommendation VI

Rec.	Rating	Summary of factors underlying ratings
SR. VI	NC	• There is no registration regime for MSBs as contemplated by SR VI. • Overall, requirements and implementation of Recommendations 4-11, 21-23 and SR. VII is inadequate which has a significant negative impact on the effectiveness of AML/CFT measures for money transmission services.. • MSBs are not required to maintain a list of their agents. • The sanction regime available to FINTRAC and applicable to MSBs is not effective, proportionate and dissuasive.

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

4.1 Customer due diligence and record-keeping (R.12) (applying R.5, 6 & 8-11)

4.1.1 Description and Analysis

Definitions and scope

1182. The PCMLTF Regulations currently cover casinos, real estate brokers and sales representatives, and accountants/accountant firms as reporting entities to FINTRAC. The AML/CFT preventive measures do not currently apply to lawyers, Quebec Notaries, BC Notaries nor to dealers in precious metals and stones[139].

1183. "*Casinos*" means a person or entity that is licensed, registered, permitted or otherwise authorised to do business under any of paragraphs 207(1)(a) to (g) of the Criminal Code and that conducts its business activities in a permanent establishment (i) that the person or entity holds out to be a casino and in which roulette or card games are carried on; or (ii) where there is a slot machine, which, for the purposes of this definition, does not include a video lottery terminal. It does not include a person or entity that is a registered charity as defined in subsection 248(1) of the Income Tax Act and is licensed, registered or otherwise authorised to carry on business temporarily for charitable purposes, if the business is carried out in the establishment of the casino for not more than two consecutive days at the time under the supervision of the casino.

1184. Gambling is permitted pursuant to the Criminal Code of Canada and regulated through provincial gaming legislation (along with its regulations, rules, directives, terms and conditions, and policies). Part VII of the *Criminal Code* makes it an offence to operate a commercial gaming enterprise. The two main exceptions to this prohibition are gambling activities conducted and managed by the province, or pursuant to a licence issued by the province. The *Criminal Code* does not contain any exceptions from the broad prohibition that would allow for the establishment of an Internet casino.

[139] The regulations enacted on 26 December 2007 extend coverage of the Act to these new sectors as of December 2008: legal counsel and legal firms, BC notaries public and notary corporations and dealers in precious metals and stones. See http://www.fin.gc.ca/news07/07-105e.html.

1185. Yet despite prohibitions against non-governmental Internet gambling, there are signs that the online gaming industry is growing in Canada and for some years now, a community in Quebec is hosting servers and has been selling "licences" for the operation of Internet gaming businesses. Interestingly, the RCMP advised it has limited capacity for handling illegal activity related to Internet casinos. Having tried previously to tackle the issue, they found they did not have the resources as the criminals were tracking investigations online and moving their servers off-shore. Internet casinos do not fall within the scope of the PCMLTFA.

1186. *Cruise ships*. Cruise ships operate out of Canadian waters and do offer casino facilities. As indicated by the Department of Transport, after the Caribbean and the Mediterranean, Alaska cruises through British Columbia's Inside Passage are the third most popular in the world. Large cruise vessels calling at Canada's ports are owned by foreign-based companies. Sailing under foreign flags, these vessels offer two basic types of extended cruises: the luxury cruise and the "pocket cruise", distinguished by vessel capacity of more or less than 150 passengers. Vancouver is the main hub in the Canadian cruise ship industry although Vancouver's share of this traffic is decreasing since 2001 to reach some 830 000 passengers in 2006.

1187. In March 1999, amendments to Canada's Criminal Code came into effect, easing restrictions on casino gambling aboard cruise ships. International cruise lines are now able to operate on-board casinos until they are within five nautical miles of a Canadian port of call (as compared to the 12 nautical mile limit for Canadian territorial waters). Previously, vessels had to close casinos as soon as they reached Canadian territorial waters. Some limitations exist: voyages must be at least 48 hours in length to offer gaming services, and passengers embarking in Canada cannot be scheduled to disembark without first calling at one or more non-Canadian ports. Cruise ships are not covered under the PCMLTFA as Canada believes that there is a limited capacity to misuse the casino facilities.

1188. **"***Accountant*" means a chartered accountant, a certified general accountant or a certified management accountant. Accountants and accountant firms are subject to the PCMLTFA when they:

a) Engage in any of the following activities *on behalf of* a person or entity:

- Receiving or paying funds.
- Purchasing or selling securities, real property or business assets or entities. Or
- Transferring funds or securities by any means.

b) Give instructions on behalf of any person or entity in respect of above activities.

c) Receive professional fees in respect of any activity referred to in a) or b).

1189. The Canadian Institute of Chartered Accountants (CICA) believes the accountant must be acting on behalf of a third party, i.e. to be an intermediary or a facilitator in the transaction. This means that the accountant has to be actually involved in the transaction, representing either the client or some third party.

1190. **"***Real estate broker or sales representative***"** means a person or entity that is registered or licensed under provincial legislation. Real estate agents are subject to the PCMLTFA when they engage in any of the following activities on behalf of any person or entity in the course of a real estate transaction:

- Receiving or paying funds.
- Depositing or withdrawing funds. Or
- Transferring funds by any means.

1191. *Real estate developers*. Home builders and real estate developers are two more sectors which the Government proposes to bring within the ambit of the PCMLTFA since they can carry out much the same role and activities as licensed real estate agents by selling homes directly to the public.

1192. *Lawyers and Quebec notaries* (who provide legal advice under the Quebec civil code) were exempted from complying with the provisions of the PCMLTFA in March 2003 when the Government revoked the regulatory provisions as they applied to legal counsel. This followed a legal challenge by the profession when the Government had initially proceeded to require mandatory suspicious and prescribed reporting, client identification, record keeping and internal compliance requirements of legal counsel when engaged in the following activities on behalf of a person or entity including the giving of instructions on behalf of any person or entity in respect of:

- Receiving or paying funds, other than those received or paid in respect of professional fees, disbursements, expenses or bail.
- Purchasing or selling securities, real properties or business assets or entities. Or
- Transferring funds or securities by any means.

1193. The professional legal bodies had argued that requiring lawyers to report information on their clients to the state is contrary to the right to solicitor-client privilege and the principle of an independent bar and judiciary.

1194. During the on-site visit, the legal profession acknowledged that there is a risk of money laundering in the "layering" stage in the business they conduct but seemed to imply money laundering was primarily a cash-based activity and that the Government was not explaining adequately where the risks lie in their discussions with the profession. The profession expressed willingness to the assessors to conduct identification and record keeping, while at the same time protecting access to that information but reporting remains an issue for them.

1195. The assessors were familiar with lawyer-client legal privilege argument but noted with interest that lawyers remain exempted when involved in the more routine purchase and sale of real property while real estate agents, engaged in exactly the same type of transaction, are required to report. The assessors were told that as a matter of business practice, the banking sector asks mortgage brokers and the legal profession to identify mortgage borrowers in accordance with the PCMLTFA at the closing of a real estate transaction.

1196. The amendments to the PCMLTF Regulations pre-published on June 30, 2007 propose to subject legal counsel and legal firms to Part I of the PCMLTFA when they engage in any of the following activities on behalf of any person or entity: (a) receiving or paying funds, other than those received or paid in respect of professional fees, disbursements, expenses or bail or (b) giving instructions in respect of any activity referred to in paragraph (a)[140].

1197. *BC Notaries* were not included in the PCMLTFA in 2001. They do not provide legal advice, undertake limited activities but they are allowed to hold trust accounts to carry out their duties and carry out real estate activities. While the number of BC Notaries is limited by statute to 332, they are at risk of being used for ML/TF. Regulations pre-published on June 30, 2007 extend coverage of the PCMLTFA to them when they act as financial intermediaries[141].

1198. *Trust and company service providers*. TCSPs are not separately recognised nor regulated as a separate business category operating in Canada although there was some acknowledgement during the on-site visit that there are businesses other than lawyers, accountants and trust companies that offer such services[142]. They do not fall under the scope of the PCMLTFA if they are not an entity or person otherwise covered by the legislation (trust and loan companies).

---

140 The PCMLTF Regulations were enacted in December 2007.

141 The PCMLTF Regulations were enacted in December 2007.

142 See for example businesses listed at:
http://ca.dir.yahoo.com/business_and_economy/business_to_business/corporate_services/incorporation_services

1199. *Dealers in precious metals and stones*. Dealers in precious metals and stones are not covered by the PCMLTFA. The profession has met with the Department of Finance to discuss their coverage by the AML/CFT regime. The proposed amendments to the PCMLTF Regulations pre-published on June 30, 2007 extend such coverage to them[143]. The assessors were told that the record keeping requirement is generally perceived as the most challenging issue due to the PIPEDA potential restrictions on customer's information retention and the very small size of the large majority of the retail businesses dealing precious metals and stones. The assessors were told that the industry would not oppose to any reporting requirement, in particular LCTRs since cash transactions are quite a limited practice in this sector (90% of the transactions seem to occur using a credit card).

Applying Recommendation 5

1200. No CDD requirements as set out in Recommendation 5 apply to Internet casinos, ship based casinos, lawyers and Quebec notaries, BC Notaries, trust and company service providers (except trust companies and accountants that may provide that type of services) and dealers in precious metals and stones.

1201. *Casinos*. Casinos are subject to special measures to identify the following individuals or entities (Section 60(b) of the PCMLTF Regulations):

- Any individual who signs a signature card in respect of an account that the casinos opens.
- Any individual who conducts a transaction with the casino for which a large cash disbursement record is required to be kept.
- Any individual carrying out foreign exchange transactions of CAD 3 000 or more or equivalent in foreign currency.
- Any individual conducting a large cash transaction.
- Any individual who conducts a transaction of CAD 3 000 or more for which an extension of credit needs to be kept.
- Any corporation or entity which opens an account.

1202. There is no requirement to carry out CDD measures when there is a suspicion of ML or TF and when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. There is no obligation to carry out customer identification for occasional transactions that are wire transfers[144]. The requirement to identify any individual for large cash transactions (above CAD10 000 which is a too high threshold) does not cover non-cash occasional transactions[145].

1203. Section 64 of the PCMLTF Regulations requires casinos to ascertain customer's identification by referring to the person's birth certificate, driver's licence, provincial health insurance card, passport or any similar record. FINTRAC Guidance 6F provides further indications on the type of documents to use (see Section 3.2 of the report for further developments).

1204. Casinos are subject to equivalent customer identification requirements as financial entities in relation to the identification of:

- Individual not physically present (Section 64(1(a)(ii) of the PCMLTF Regulations).
- Corporation or entity other than corporation (Sections 65 & 66of the PCMLTF Regulations).

143 The PCMLTF Regulations were enacted in December 2007.

144 Regulations enacted in June 2007 and which come into force in June 2008 will require that casinos identify clients in respect of these situations (see Section 60(b)(iv) of the amended PCMLTF Regulations).

145 Regulations pre-published in October 2007 will require casinos to identify clients, keep records and make reports with respect to all large disbursements regardless of the form of payment (e.g. chips, wire transfers, cash, etc.) (see Sections 42, 43(g), 44, 60(b)(i) and Schedule 8 of the PCMLTF Regulations, as amended by the regulations published in October 2007).

- Individuals acting on behalf of the customer (third party determination, Section 8 of the PCMLTF Regulations).

1205. Exceptions to ascertaining identity apply also to casinos: (1) if the customer has already an account (Section 62(2)(a) the PCMLTF Regulations); (2) if there are reasonable grounds to believe that the account holder is a public body or a corporation that has minimum net assets of CAD 75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange that is prescribed by section 3201 of the Income Tax Regulations and operates in a country that is a member of the FATF (Section 62(2)(a) the PCMLTF Regulations) or (3) for the opening of a business account for which the casino has already ascertained the identity of at least three persons who are authorised to give instructions in respect of the account (Section 60(a) of the PCMLTF Regulations).

1206. Casinos are not required to carry out customer identification in relation to: beneficial ownership; ongoing due diligence for accounts that the casinos open and higher risk categories of customers. Casinos are not required to collect information on the purpose and intended nature of the business relationship and on existing customers. There is no specific provision in the case casinos fail to complete CDD[146].

1207. The customer identification (natural or legal person) must be carried out before any transaction other than an initial deposit is carried out on an account.

1208. *Real estate agents and sales representatives.* Real estate agents and sales representatives are subject to customer identity verification (see Article 6.1 of the PCMLTFA) when they engage in any of the following activities on behalf of any person or entity in the course of a real estate transaction (Section 37 of the PCMLTF Regulations):

- Receiving or paying funds.
- Depositing or withdrawing funds. Or
- Transferring funds by any means.

1209. The PCMLTF Regulations also requires real estate brokers and sales representatives to ascertain the identity of their client when they receive §10,000 or more from the client in the course of a single transaction or two or more transactions carried out within a 24-hour period.

1210. In determining the identity of individuals, the PCMLTFA requires that brokers and sales representatives refer to a government issued identification document, such as a birth certificate, driver's license, passport, record of landing, permanent resident card or other similar record, and a provincial health card in certain provinces (see FINTRAC Guideline 6B of June 2005).

1211. When dealing with a corporation or any other entity, there is no specific requirement applicable to real estate agents and sales representatives to ascertain the identity of legal persons[147].

1212. The circumstances in which real estate agents and sales representatives have to carry out customer identification is too restrictive since they should be required to do so when they are involved

[146] Regulations which were enacted in June 2007 and come into force in June 2008, will close some of those gaps by requiring that casinos take reasonable measures to conduct ongoing monitoring; keep client information up-to-date in higher risk situations; and prohibiting casinos from opening an account if the identity of the client cannot be established (see Sections 71.1 and 53.2 of the amended PCMLTF Regulations).

[147] Section 59.2 of the PCMLTF Regulations enacted on 27 June 2007 and entering into force on 23 June 2008 requires real estate agents and sales representatives to confirm the existence and ascertain the name and address of every corporation/entity on whose behalf a transactions is conducted and the names of directors.

in transactions for a client concerning the buying and selling of real estate (see FATF Recommendation 12)[148].

1213. The CDD requirements applicable to real estate agents and sales representatives are substantially very basic and limited. They do not meet the FATF standards set out in Recommendation 5. Only Section 8 of the PCMLTF Regulations on third party determination (see Section 3.2 of the report "*Third party determination*" for a complete description of the provision) - that is applicable to every person or entity that is required to keep a large cash transaction report - applies to real estate agents and sales representatives. FINTRAC Guideline 6B for real estate agents and sales representatives states that what constitutes reasonable measures in making a third party determination will vary in accordance with the context in which they occur, and therefore could differ from one situation to the next. However, reasonable measures would include retrieving the information already contained in the agent's files or elsewhere within the business environment, or obtaining the information directly from the client.

1214. *Accountants and accountant firms*. Accountants are required to carry out customer identification when they (Section 34 of the PCMLTF Regulations):

a) engage in any of the following activities *on behalf of* a person or entity:
- Receiving or paying funds.
- Purchasing or selling securities, real property or business assets or entities. Or
- Transferring funds or securities by any means.

b) give instructions on behalf of any person or entity in respect of above activities

c) receive professional fees in respect of any activity referred to in a) or b).

1215. Accountants and accountant firms are subject to client identification obligations when they receive professional fees to engage in any of the activities listed above. This means that they would be subject to the client identification requirements when they engage in any of the activities mentioned above even if they were doing them on a volunteer basis. Activities of accountants or accounting firms other than those listed above, such as audit, review or compilation engagements carried out according to the recommendations in the Canadian Institute of Chartered Accountants (CICA) Handbook, do not trigger record keeping or client identification obligations. Giving advice to a client, in the context of your accountant-client relationship, is not considered providing instructions (FINTRAC Guidelines 6B of June 2005).

1216. The PCMLTF Regulations also requires accountants and accountant firms to ascertain the identity of their client when they receive CAD 10 000 or more from the client in the course of a single transaction or two or more transactions carried out within a 24-hour period.

1217. In determining the identity of individuals, the PCMLTFA requires that accountants refer to a government issued identification document, such as a birth certificate, driver's license, passport, record of landing, permanent resident card or other similar record, and a provincial health card in certain provinces (see FINTRAC Guideline 6B).

1218. When dealing with a corporation or any other entity, there is no specific requirement applicable to accountants/accountants firms to ascertain the identity of legal persons[149].

---

[148] This issue is addressed in the PCMLTF Regulations enacted on 27 June 2007 that will enter into force on 23 June 2008 (see Section 59.2 of the amended PCMLTF Regulations that must be read in conjunction with section 39 of the same regulations).

[149] Section 59.1 of the PCMLTF Regulations enacted on 27 June 2007 and entering into force on 23 June 2008 requires accountants and accountant firms to confirm the existence and ascertain the name and address of every corporation/entity on whose behalf a transactions is conducted and the names of directors.

1219. The circumstances in which accountants have to carry out customer identification are too restrictive since they should also be required to do so in the following circumstances (see FATF Recommendation 12):

- Management of bank, savings or securities accounts.
- Management of client money, securities and other assets (and not only purchasing or selling of these).
- Organisation of contributions for the creation, operation or management of companies.
- Creation, operation or management of legal persons or arrangements.

1220. The current CDD requirements applicable to accountants are substantially very basic and extremely limited. They meet a very limited range of requirements under Recommendation 5.

1221. Accountants and real estate agents and sales representatives must inform individuals concerning the collection of personal information about them. However, they do not have to inform individuals when they include personal information about them in any reports that they are required to make to FINTRAC (see FINTRAC Guideline 6B).

Applying Recommendation 6

1222. Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs and discussions with the private sector representatives met by the assessment team suggest that this is not perceived as an area of high priority.

Applying Recommendation 8

1223. There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes[150].

1224. The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions[151].

Applying Recommendation 9

1225. There are currently no provisions for DNFBPs that address the issue of relying on intermediaries or third parties to perform elements of the CDD process (see Section 3.3 of the report). FINTRAC's current Guideline 6 indicates that DNFBPs may choose to use an agent/introducer or third party for customer identification purposes and, should they chose to do so, they need to enter into a written agreement with the agent/introducer which specifies what is expected from the agent/introducer. Where the DNFBP chooses to enter into such an agreement, it is ultimately responsible for ensuring that the identification requirements are met. This covers an outsourcing type of scenario that falls outside the scope of Recommendation 9.

---

150 The Regulations enacted in June 2007 and coming into force in June 2008 will require all reporting entities to conduct ongoing monitoring and keep client information up-to-date in higher risk situations, such as when new technologies are used to delivers products and services (see Sections 71 and 71.1 of the amended PCMLTF Regulations).

151 Section 64 of the PCMLTF Regulations enacted on 27 June 2007 (and due to enter into force on 23 June 2008) requires real estate agents and sales representatives, casinos and accountants/accountant firms to take specific customer identification steps if the person is not physically present at the time the business relationship is established.

Applying Recommendation 10

1226. No record keeping as described in Section 6 of the PCMLTFA apply to Internet casinos, ship based casinos, lawyers and Quebec notaries, BC Notaries, trust and company service providers (except trust companies) and dealers in precious metals and stones.

1227. *Casinos*. The record keeping requirements in relation to casinos are comprehensive. Casinos have to keep the following records: (1) large cash transaction records; (2) large cash disbursement records; (3) certain records about client accounts; (4) extension of credit records; and (5) foreign currency exchange transaction tickets. The record keeping requirements for the large cash transaction reports as well as the large cash disbursement records (Section 41 & 42 of the PCMLTF Regulations) are as follows:

	Large cash transaction reports	**Large cash disbursement records**
Type of transactions for which a record has to be kept	▪ The sale of chips, tokens or plaques. ▪ Front cash deposits. ▪ Safekeeping deposits. ▪ The repayment of any form of credit, including repayment by markers or counter cheques. ▪ Bets of currency. ▪ Sales of your casino's cheques.	▪ The redemption of chips, tokens or plaques. ▪ Front cash withdrawals. ▪ Safekeeping withdrawals. ▪ Advances on any form of credit, including advances by markers or counter cheques. ▪ Payments on bets, including slot jackpots. ▪ Payments to clients of funds received for credit to that client or any other client. ▪ Cashing of cheques or other negotiable instruments. ▪ Reimbursements to clients of travel and entertainment expenses.
Record keeping exemption	If the cash is received from a financial entity. (bank, credit union or caisse populaire; trust and loan company; or an agent of the Crown that accepts deposit liabilities)	-
Contents of the record[152]	▪ The amount and currency of the cash received. ▪ The name of the individual from whom you received the cash and that individual's address and principal business or occupation. ▪ The date of the transaction. ▪ The purpose, details and type of transaction (for example, the cash was used to buy chips, etc.), including whether any other individuals or entities were involved in the transaction. ▪ How the cash was received (for example, in person, by mail, by armoured car, or any other way). ▪ If an account was affected by the transaction, include the following: the number and type of any such account; the full name of the client that holds the account; and the currency in which the account's transactions are conducted.	▪ The name of the individual to whom the disbursement is made. ▪ That individual's address and principal business or occupation. ▪ The date and what kind of disbursement it is.
Extra record to keep for client identification	▪ The individual's date of birth. ▪ The type of document used to confirm the individual's identity, the document's reference number and its place of issue.	▪ The individual's date of birth. ▪ The type of document used to confirm the individual's identity, the document's reference number and its place of issue.

[152] Information on individual's date of birth will have to be kept from June 2008 (see the definition of "large cash transaction record" in 1(2) and paragraph 42(2)(d) of the amended PCMLTF Regulations. Please note that once the large disbursement reporting requirement comes into force (as introduced in the regulations that were published in October 2007), casinos will be required to keep a copy of the large disbursement report instead of a large cash disbursement record. However, the report also contains the date of birth of the person requesting the disbursement (see new Schedule 8, Part D, item 8 under PCMLTF Regulations).

1228. The record keeping requirements for client accounts are as follows (Section 43 of the PCMLT Regulations):

- *Account operating agreements*: an account operating agreement is any document that is received or created in the normal course of business and outlines the agreement between the casino and its client about the account's operation. If the casino has to identify the individual, the account operating agreement for that individual also has to contain the following information: (1) the individual's date of birth; and (2) the type of document used to identify the individual, its reference number and its place of issue. If the casino has identified the individual based on a cleared cheque, the account operating agreement has to contain the financial entity and account number of the account on which the cheque was drawn.
- *Deposit slips:* casinos have to keep a deposit slip for every deposit made to an account. A deposit slip means a record that sets out the date of a deposit, the amount of the deposit, and any part of it that was made in cash. A deposit slip also sets out the holder of the account in whose name the deposit is made and the number of the account.
- *Debit or credit memos*: casinos have to keep any debit or credit memo that they create or receive regarding an account in the normal course of business.
- *Accounts for corporations*: if the account is opened for a corporation, casinos have to keep a copy of the part of the official corporate records showing the provisions that relate to the power to bind the corporation regarding the account. This could be the articles of incorporation that set out those duly authorised to sign on behalf of the corporation, such as an officer, the comptroller, etc. If there were changes subsequent to the articles, then the board resolution stating the change would be included in this type of record.
- *Accounts for an individuals or entities other than corporations*: if the account is opened for an individual or any entity that is not a corporation, the casinos have to keep a record of the name, address and principal business or occupation of that individual or entity.
- *A signature card in respect of every account holder*: casinos have to keep a signature card in respect of any account they open, which must include the date of birth of the person, the type and number of the identification document used to identify the individual and its place of issue.

1229. Casinos have also to keep an extension of credit record for every extension of credit to a client of CAD 3 000 or more. This record has to indicate the following information: (1) the name of the client; (2) the client's address and principal business or occupation; (3) the terms and conditions of the extension of credit; and (4) the date and amount of the extension of credit (Section 43(d) of the PCMLTF Regulations).

1230. Third party record requirements in relation to third party determination are equivalent to these applicable to financial entities (see Section 3.5 of the report).

1231. Casinos are recommended to maintain an effective record keeping system to enable FINTRAC to have access to the records in a timely fashion. Such records have to be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them (Section 69 of the PCMLTF Regulations and FINTRAC Guideline 6F).

1232. *Real estate agents and sales representatives and accountants*. Real estate agents and sales representatives and accountants have record keeping obligations when they engage in one of the activities described above (see this section of the report in relation to "Applying Recommendation 5") as well as for large cash transactions and third party determination (see Section 3.5 of the report that sets out the details of the record keeping requirements in the case of large cash transactions and third party determination). However, the circumstances in which real estate agents and sales representatives

and accountants have to keep record are not satisfactory since the list of activities covered is too restrictive (see this section of the report in relation to "*Applying Recommendation 5")*[153].

1233. Large cash transactions records must be kept for a period of at least five years following the date they were created. The records' retention rules are otherwise described in Section 69 of the PCMLTF Regulations and are equivalent to those applicable to financial entities (see Section 3.5 of the report). FINTRAC Guideline 6B recommend real estate agents and sales representatives and accountants to maintain an effective record keeping system to enable FINTRAC to have access to the records in a timely fashion. Such records have to be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them. Records must be in a machine-readable or electronic form, as long as a paper copy can be readily produced. Also, for records that are kept electronically, an electronic signature of the individual who must sign the record has to be retained.

Applying Recommendation 11

1234. There is currently no explicit provision requiring that DNFBPs pay special attention to all complex, unusual large transactions that have no apparent or visible economic or lawful purpose. Similar to financial institutions, such a requirement may only be indirectly deduced from the requirement to report to FINTRAC suspicious transactions that may be related to money laundering or terrorist financing, as well as the obligation to report large international electronic funds transfer reports involving CAD 10 000 or more (EFTRs) and large cash transaction reports of CAD 10 000 or more (LCTRs).

4.1.2 Recommendations and Comments

1235. *Scope issues*. The assessors noted that Canada is working on addressing the outstanding scope issues and such an effort should continue in order to bring all DNFBPs in line with FATF Recommendations[154]. The participation of lawyers in the AML/CFT effort is essential since their current exemption leaves a very significant gap in coverage. The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification and keep records should be extended to be in line with the types of activities targeted under Recommendation 12[155].

1236. *Recommendation 5*. Canada should ensure that the entire set of requirements under Recommendation 5 apply to all non-financial professions.

1237. *Recommendations 6, 8, 9 and 11*. Canada should require the non-financial professions to implement requirements in relation to Recommendations 6, 8, 9 and 11.

1238. *Recommendation 10.* Canada should ensure that all types of transactions carried out by the non-financial professions are subject to proper record keeping requirement that permits their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. Canada should ensure that all customer and transactions records and information collected by the non-financial professions are available on a timely basis to domestic competent authorities.

---

153 These circumstances are expanded in regulations enacted in June 2007 and coming into force in June 2008 (see Section 39 of the amended PCMLTF Regulations).

154 Canada enacted regulations on December 2007 to extend coverage of the PCMLTFA to the following sectors as of December 2008: legal counsel and legal firms, BC notaries public and notary corporations and dealers in precious metals and stones.

155 Canada indicates that the regulations coming into force in June 2008 will resolve this issue.

4.1.3 Compliance with Recommendation 12

Rec.	Rating	Summary of factors underlying ratings
R.12	NC	*Scope issue* • Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the requirements under Recommendations 5, 6 and 8-11. *Application of Recommendation 5 to casinos* • The requirements applicable to casinos are insufficient in relation to: (1) when CDD is required; (2) required CDD measures; (3) identification of persons acting on behalf of the customer; (4) third party determination and identification of beneficial owners ; (5) purpose & intended nature of the business relationship ; (6) ongoing Due Diligence; (7) ML/FT risks and (8) failure to satisfactorily complete CDD. *Application of Recommendation 5 to real estate brokers and sales representatives and accountants* • The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification are too limitative. • The CDD requirements that real estate agents and sales representatives and accountants are subject to are substantially very basic and extremely limited. *Application of Recommendation 6 to casinos, real estate brokers and sales representatives and accountants* • Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs. *Application of Recommendation 8 to casinos, real estate brokers and sales representatives, accountants* • There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes. • The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. *Application of Recommendation 9 to casinos, real estate brokers and sales representatives and accountants* • There are currently no provisions for DNFBPs that address the issue of relying on intermediaries or third parties to perform elements of the CDD process outside the outsourcing type of scenario. *Application of Recommendation 10 to casinos, real estate brokers and sales representatives and accountants* • The circumstances in which real estate agents and sales representatives and accountants have to keep records are too limitative. • Real estate agents and sales representatives, casinos and accountants institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which is not in line with the FATF requirement to make CDD records available on a timely basis to competent authorities. *Application of Recommendation 11 to casinos, real estate brokers and sales representatives and accountants* • There is currently no explicit provision requiring that DNFBPs pay special attention to all complex, unusual large transactions that have no apparent or visible economic or lawful purpose (the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11). The other requirements under Recommendation 11 are not met either.

4.2 Monitoring transactions and other issues (R.16) (applying R.13-15, 17 & 21)

4.2.1 Description and Analysis

Applying Recommendation 13

1239. Every person or entity subject to Part I of the PCMLTFA is required to report to FINTRAC financial transactions for which there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering or a terrorist financing offence (Section 7 of the PCMLTFA). Since 2002, reporting persons or entities have to send a terrorist property report to FINTRAC if they have property in their possession or control that they know is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about any transaction or proposed transaction relating to that property. In addition to making a terrorist property report to FINTRAC about this type of property, there is also a requirement under the Criminal Code that applies to anyone in Canada and any Canadian outside Canada. Whether or not they are a reporting person or entity, they must disclose to the RCMP and CSIS, the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist or a terrorist group. Reporting entities are also required to report all cash transactions of CAD 10 000 or more.

1240. No suspicious transaction reporting requirement applies to Internet casinos, ship based casinos, lawyers and Quebec notaries, BC Notaries, trust and company service providers (except trust companies and accountants that may provide that type of services) and dealers in precious metals and stones.

1241. The PCMLTFA explicitly excludes, under Section 10.1, legal counsel and legal firms from STR and LCTR requirements "when they are providing legal services", which seems to be interpreted widely, as the profession considers that legal services cannot be in practice distinguished from financial services. It is worth mentioning that the Federation of Law societies is preparing a model rule on Client identification and verification requirements, which will be incorporated in the regulatory instruments of each law Society. It would apply when a lawyer acts as financial intermediary for a client and would include a provision stating that if a lawyer reasonably suspects that he might be assisting a client in dishonesty, fraud, crime or illegal conduct, he must withdraw from representation of the client and record the results of his reasonable suspicions.

1242. *Suspicious transactions reporting for casinos*. Under Article 5 of the PCMLTFA, casinos as defined in the regulations (see Section 4.1 of the report, "*definitions and scope*") are subject to the suspicious transactions reporting requirement. FINTRAC has elaborated indicators (Guideline 2 "*Suspicious Transactions*" of March 2003) for casinos to detect suspicious transactions.

1243. Under Section 40 of the PCMLTF Regulations, casinos are required to report to FINTRAC the receipt of an amount of cash of CAD 10 000 or more in the course of a single transaction unless the amount is received by a financial entity.

1244. *Suspicious transactions reporting for real estate agents and sales representatives*. Real estate agents and sales representatives have to submit STRs to FINTRAC according to Section 7 of the PCMLTF Suspicious Transaction Reporting Regulations when they engage in any of the following activities on behalf of any person or entity in the course of a real estate transaction: (1) receiving or paying funds; (2) depositing or withdrawing funds; or (3) transferring funds by any means. However, the circumstances in which they have to report suspicious transactions are not satisfactory since the list of activities covered is too restrictive (see comments in Section 4.1 of the report).[156]

[156] Canada indicated that the amendments to the PCMLTF Suspicious Transaction Reporting Regulations enacted in June 2007 and coming into force on 23 June 2008 extend these circumstances to any situation where real estate agents and sales representatives act as an agent in respect of the purchase or sale of real estate.

1245. *Suspicious transactions reporting for accountants and accountant firms*. Accountants and accountant firms are required to submit STRs to FINTRAC when they (Section 34 of the PCMLTF Regulations):

a) Engage in any of the following activities *on behalf of* a person or entity:
- Receiving or paying funds.
- Purchasing or selling securities, real property or business assets or entities. Or
- Transferring funds or securities by any means.

b) give instructions on behalf of any person or entity in respect of above activities
c) receive professional fees in respect of any activity referred to in a) or b).

1246. However, the circumstances in which accountants have to carry out customer identification are too restrictive (see comments in Section 4.1 "*definitions and scope*").

1247. The CICA has been active in developing comprehensive guidelines for compliance with the PCMLTFA (the guidelines were published in November 2004). These guidelines provide the CGAs with an overview of the obligations under the legislation and assist them developing a "knowledge base" from which the accountants can exercise their judgement in carrying out their obligation to report suspicious transactions. The assessors believe that such guidelines provide useful information to the profession.

1248. In practice, professionals face some difficulties to clearly determine which firms or individuals are subject to the requirement and what should be reported.

1249. With regard to accountants and real estate agents, it is worth noting that the effective implementation of the STR requirement is limited by the fact that these professions are only required to identify and ascertain identity of their clients in the case of large cash transactions.[157]

1250. *Provisions in relation to Recommendation 16 applicable to casinos, real estate agents and sales representatives and accountants/accountant firms*. The PCMLTFA requires the reporting of all completed transactions, where there are reasonable grounds to suspect that they relate to the commission of a money laundering or a terrorist financing offence, regardless of the involvement in tax matters. Attempted suspicious transactions are not yet covered by the Suspicious Transaction Reporting requirement[158].

1251. Casinos, real estate agents and sales representatives and accountants/accountant firms have to submit suspicious transaction reports to FINTRAC, containing specific information (see FINTRAC Guideline 3A). Once they have determined that there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering or terrorist financing offence, their report, including all required and applicable information, must be sent within 30 calendar days. This 30-day reporting time limit begins when their employees first detect a fact about a transaction that constitutes reasonable grounds to suspect that it is related to the commission of a money laundering or terrorist financing offence. If such a fact is detected at the time of the transaction, the reporting timeline begins at the time of the transaction. However, if the fact is not detected at the time of the transaction, the 30-day time limit could begin at some time after.

---

157 Canada indicated that the amendments to the PCMLTF regulations enacted on 27 June 2007 and coming into force on 23 June 2008 require that all reporting entities identify their clients in respect of a suspicious transaction or a suspicious attempted transaction.

158 The PCMLTF Suspicious Transaction Reporting Regulations enacted on 27 June 2007 introduces an obligation to report attempted transactions as of 23 June 2008 (the requirement is in section 7 of the PCMLTFA. The PCMLTF Suspicious Transaction Reporting Regulations provide more details on the person or entities subject to the reporting requirement and on the information that must be reported).

1252. FINTRAC has elaborated indicators (Guideline 2 "*Suspicious Transactions*" of March 2003) for casinos to detect suspicious transactions including: (1) any casino transaction of CAD 3 000 or more when an individual receives payment in casino cheques made out to third parties or without a specified payee; (2) client requests a winnings cheque in a third party's name; (3) acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party; (4) client attempts to avoid the filing of a report for cash by breaking up the transaction; (5) client requests cheques that are not for gaming winnings; (6) client enquires about opening an account with the casino and the ability to transfer the funds to other locations when you do not know the client as a regular, frequent or large volume player; (7) client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque; (8) client exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or cheques; (9) client is known to use multiple names or (10) client requests the transfer of winnings to the bank account of a third party or a known drug source country or to a country where there is no effective anti-money-laundering system.

1253. Equivalent guidelines have been published by FINTRAC for the real estate agents and sales representatives as well as for accountants.

1254. *Statistics*. The following table indicates the number of STRs per fiscal year and by DNFBPs:

	2001/2002	2002/2003	2003/2004	2004/2005	2005/2006	2006/2007	**Total**
Accountants	7	20	20	40	20	12	**119**
Casinos	143	498	360	390	420	223	**2 034**
Legal counsel[159]	5	2	3	0	0	0	**10**
Real estate agents/sales representatives	2	8	6	6	12	1	**35**

1255. Some concern raised by the current STR requirement applicable to DNFBPs is the relatively low number of reports actually sent to FINTRAC by certain DNFBPs, in particular accountants and real estate brokers and sales representatives in spite of the outreach they have benefited from FINTRAC.

Applying Recommendation 14

1256. Section 10 of the PCMLTFA provides immunity provisions for reporting entities. No criminal or civil proceeding lie against a person or entity for making a suspicious transaction report, a terrorist property report, a large cash transaction report or an electronic funds transfer in good faith or for providing FINTRAC with information about suspicions of money laundering or the financing of terrorist activities.

1257. In addition to the immunity provision, Section 8 of the PCMLTFA specifies that no person or entity can disclose that they have made a suspicious transaction report, or disclose the contents of a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. Failure to comply with these requirements could lead to up to two years imprisonment.

Applying Recommendation 15

1258. Every person or entity subject to the Part I of the PCMLTFA, including DNFBPs, has to implement a compliance regime, *as far as practicable*, which means that, depending on the various size and activities of the reporting entities, a regime may be adapted. This includes the appointment of a person responsible for its implementation, the development and application of policies and procedures, a review of those procedures and policies to test their effectiveness by an internal or

[159] Legal counsel was removed from reporting obligations to FINTRAC in 2003.

external auditor or by the person or entity itself, *as often as necessary* and an ongoing compliance training program for the employees or agents (Section 71 of the PCMLTF Regulations, see Section 3.8 of the report)[160].

1259. Apart from the specific scope issues related to DNFBPs, the main deficiencies applicable to financial institutions apply also to DNFBPs, since the core obligations for both DNFBPs and financial institutions are based on the same general AML/CFT regime contained in the PCMLTF Regulations. The requirements to keep up to date internal procedures, that the policies include the detection of unusual and suspicious transactions and ensuring that the AML/CFT compliance officer has timely access to customer identification data and other CDD information, transactions records and other relevant information are only implicit. There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance, even if certain provincial gambling Acts include such requirements. Measures exist in the casino industry to ensure the screening of key employees and employees with direct access to gaming facilities, so as to prevent criminals owning or controlling casinos. For some other categories of DNFBPs, there are entry requirements for the business or profession, but these do not amount to screening of employees as contemplated by R.15.

Applying Recommendation 21

1260. All reporting parties, including DNFBPs, received information from FINTRAC in relation to the NCCT process when that process was still under way (including the need to enhance the level of scrutiny in the case of counter-measures). However, there is no enforceable requirement to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations, no effective measures in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems, and no requirement to examine the background and purpose of these transactions and to document the related findings.

4.2.2 Recommendations and Comments

1261. *Recommendation 13*. All DNFBPs as defined by the FATF should be subject in Canada to the suspicious transactions reporting requirement in all circumstances defined in Recommendation 16. The current incomplete coverage of certain DNFBPs has an impact on the effective implementation of the suspicious transactions report requirement. FINTRAC should address the issues raised by the low number of STRs provided by some non-financial professions (especially real estate agents and sales representatives and accountants).

1262. *Recommendation 15*. The current requirements should be expanded, specified and enforced, especially:

- The policies and procedures should be required to be written and their minimum mandatory content should include the detection of unusual and suspicious transactions for all DNFBPs.[161]
- There should be a requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information.
- The requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened.
- Canada should impose screening procedures when hiring employees to DNFBPs.

[160] The compliance regime requirements were expanded in regulations enacted in June 2007 which will come into force in June 23, 2008 (see Section 71 of the amended PCMLTF Regulations).

[161] Canada indicated thar the compliance regime requirements were expanded in regulations enacted in June 2007 which will come into force in June 23, 2008.

1263. *Recommendation 21*. The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to DNFBPs. Effective measures should be put in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. Finally a provision should be introduced requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

4.2.3 Compliance with Recommendation 16

Rec.	Rating	Summary of factors underlying ratings
Rec.16	NC	*Scope issue* • Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the suspicious transactions reporting requirements. *Application of Recommendation 13 to casinos, real estate brokers and sales representatives and accountants/accountant firms* • The circumstances in which real estate agents and sales representatives and accountants have to report suspicious transactions under the PCMLTFA are too limited. • Attempted transactions are not yet covered by the Suspicious Transaction Reporting requirement. • The relatively low numbers of STRs sent by real estate agents/sales representatives and accountants raise significant concerns in relation to the effectiveness of the reporting system in these sectors. *Application of Recommendation 15 to casinos, real estate brokers and sales representatives and accountants/accountant firms* • There is no explicit requirement to: (1) keep up to date internal procedures, (2) have policies to monitor for and detect unusual and suspicious transactions and (3) ensure that the AML/CFT compliance officer has timely access to customer identification data and other CDD information, transactions records and other relevant information. • There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance. • Except for casinos, there are no requirements concerning screening procedures when hiring employees. *Application of Recommendation 21 to casinos, real estate brokers and sales representatives and accountants/accountant firms* • There is no general enforceable requirement for DNFBPs to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations but only through general guidance or advisories sent on a case by case basis. • There are no effective measures in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. • There is no requirement to examine the background and purpose of these transactions and to document the related findings.

4.3 Regulation, supervision and monitoring (R. 24-25)

4.3.1 Description and Analysis

Recommendation 24

1264. FINTRAC is responsible for ensuring that DNFBPs comply with their obligations under the PCMLTFA. In order to effectively use its powers to ensure compliance, FINTRAC has developed a comprehensive Compliance Program using a risk-based approach to ensuring compliance includes the development of comprehensive sector profiles and the active gathering of information on individual

reporting entities (see Section 3.10 of the report). However, given the very high number of persons or entities likely to be subject to the PCMLTFA as non-financial professions and the limited staff resources of FINTRAC dedicated to compliance, the assessment team is of view that FINTRAC is not in a position to ensure on its own an efficient monitoring of the effective application of AML/CFT legislation in these sectors. In these conditions, regulators and SROs have an important role to play to assist FINTRAC in ensuring compliance with the AML/CFT requirements.

1265. As already stated under Section 3.10 of the report, Subsections 65(2) and 65(3) of the PCMLTFA permit FINTRAC to exchange information with regulators for compliance purposes. As a result, FINTRAC works with regulators who, under their own powers, examine entities that are covered under the PCMLTFA. Information provided by these regulators to FINTRAC feeds into FINTRAC's risk assessment and assists FINTRAC to target the highest proportion of its compliance resources to the sectors and entities at highest risk for non-compliance. Where entities are covered by a regulator with a robust compliance program which includes examinations for issues related to compliance with the PCMLTFA (reporting, record-keeping, client identification, existence of a compliance regime), FINTRAC may decide to allocate fewer resources to examinations in that sector than in a sector that is not well regulated.

1266. Regarding DNFPBs, FINTRAC has currently entered only into 5 agreements with regulators of the gaming sector (see below). FINTRAC always reserves the right to examine the reporting entities covered by an MOU. For some regulators, if significant non-compliance is detected, they could issue sanctions under their respective legislation. In the case of other regulators, they will advise FINTRAC of the results and FINTRAC may complete an on-site examination of the reporting entity and take the appropriate action as necessary.

Casinos

General

1267. Under Section 207 of the Criminal Code, provinces have the responsibility to license, operate, and regulate legal forms of gaming, including the rules for gaming products and financial services available within the casinos. Gaming products include a wide variety of card games, roulette and slot machines. There are also a wide variety of financial services available at casinos, including some that resemble services provided by financial institutions. Depending on the province, casinos can open customer deposit or credit accounts, have facilities for transmitting and receiving funds transfers directly from other institutions, and offer cheque cashing and currency exchange services. These services are ancillary to their core activities, which is the sale and redemption of chips.

1268. Provinces permit the delivery of gaming services through one or a combination of the following operational models:

- *Commercial Casinos* – the province through a crown corporation or through service contracts with private corporations delivers gaming services at the casinos;
- *Charity casinos* – charities participate directly in the provision of the gaming activities at designated "charity" casinos or they are provided a direct grant from a fund generated from casino revenues;
- *First Nation Casinos* – based on either the charity or commercial casino models, First Nations operate casinos on First Nation land.

1269. The table below shows the distribution of casinos among categories and provinces.

Province	Commercial Casinos	Slots	Charity	First Nation	Seasonal	Total
Alberta	0	3	18	1	1	**23**
British Columbia	19	2	0	0	1	**22**
Manitoba	2	0	0	2	0	**4**
Nova Scotia	2	0	0	0	0	**2**
Ontario	4	17	5	1	2	**29**
Quebec	3	0	0	0	0	**3**
Saskatchewan	3	0	0	4	0	7
Yukon	1	0	0	0	0	1
TOTAL	**34**	**22**	**23**	**8**	**4**	**91**

1270. *Internet casinos*. Part VII of the *Criminal Code* makes it an offence to operate a commercial gaming enterprise. The two main exceptions to this prohibition are gambling activities conducted and managed by the province, or pursuant to a licence issued by the province. The *Criminal Code* does not contain any exceptions from the broad prohibition that would allow for the establishment of an Internet casino.

1271. Despite the legal prohibitions against online gaming, for a number of years the "Gaming Commission" of the Mohawk Territory of Kahnawake (Quebec) is hosting servers and has been issuing "licenses" for the operation of Internet gaming businesses. Licenses cost from CAD 5 000 to CAD 25 000 and it appears that there are now more than 400 "permit holders" operating Internet casino and gambling sites, with some reports suggesting that up to 60% of on-line casino gaming is passing through the Kahnawake based servers. In Canada, courts have explicitly rejected First Nations' claims to an inherent right to conduct gaming activities. The Quebec Minister of Public Security has spoken out against the operation of these online casinos, and in late 2007 one of the "licensees" that had offices in Montreal pled guilty to a charge of illegal gambling. However, no action has been taken against other "licensees". Despite this decision the Mohawks of Kahnawake continue to assert that they have jurisdiction to issue gaming licenses for gaming operations, and continue to host Internet casinos on their reserve.

1272. Having recognized the need to create a regulatory environment designed specifically for the interactive gaming industry, the Kahnawake community created the Kahnawake Gaming Commission which in turn enacted a "regulatory" framework for online gaming, under the "the Kahnawake Gaming Law" and the "Kahnawake Regulations Concerning Interactive Gaming". The measures were designed to ensure that all interactive gaming and gaming related activities conducted within, or from the Mohawk Territory of Kahnawake, satisfy three basic principles: (1) that only suitable persons and entities are permitted to operate within Kahnawake; (2) that the games offered are fair to the player; and (3) that winners are paid.

1273. However, these activities are not subject to AML/CFT regulations and Canada's federal and provincial governments are faced with substantial challenges in determining the appropriate course of action to be taken concerning Internet gambling. The industry has grown rapidly and huge revenues are generated. Canada must either enforce its prohibition effectively or introduce comprehensive AML/CFT regulation for the industry.

1274. *Cruise ships*. Cruise ships operate out of Canadian waters and do offer casino facilities (except within five nautical miles of a Canadian port). No AML/CFT measures apply to such casino gambling.

1275. Regarding the legal forms of casinos, the methods of licensing and registration depend on the operational model used. The measures in place to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino are comprehensive (with the exception of Internet and ship based casinos).

Commercial Casinos

1276. Under section 207(1)(a) of the Criminal Code, provinces have the authority to operate gaming facilities or authorise a commission to operate gaming on their behalf. In practice, six provinces (British Columbia, Manitoba, Nova Scotia, Ontario, Québec, and Saskatchewan) have authorised casinos (including slot facilities) under section 207(1)(a) of the Criminal Code. Each has established a provincial gaming corporation to operate gaming within the province as described in the following table.

Province	Provincial Gaming Corporation
British Columbia	BC Lottery Corporation
Manitoba	Manitoba Lotteries Corporation
Nova Scotia	Nova Scotia Gaming Corporation
Ontario	Ontario Lottery and Gaming Corporation
Québec	Loto Québec
Saskatchewan	Saskatchewan Gaming Corporation

1277. In British Columbia, Nova Scotia and Ontario, the gaming corporations have contracted to private corporations to provide at least some of the day-to-day casino operations[162]. The contracts do not alleviate the crown corporations of their legal role of operator, as they are required to monitor the activities of the private corporations with whom they enter into contracts.

1278. To ensure the sound running of the casino industry, private gaming service providers must also disclose detailed corporate information to the provincial gaming regulator, including the structure, business relationships, and finances (including tax returns), as well as a documented history of criminal charges, civil proceedings, insolvency, gaming permits, and taxes.

1279. To ensure that criminals and their associates are unable to become involved in the casino industry, regulations under the provincial gaming legislation require that the following groups register with the regulator before becoming involved in gaming operations:

- The casino operator (private corporation).
- Executive members and key employees (*e.g.* the Chief Executive, Chief Financial, and Chief Operating Officers, floor managers, directors of security or any position that has direct gaming-related decision making responsibilities within the casino).
- And all other gaming employees (*e.g.* employees that have access to the casino floor or restricted areas of the casino as part of their regulator or continuing employment functions).

1280. An application for registration will be refused where there are reasonable grounds to believe that the applicant will not act as a supplier or gaming assistant in accordance with the law or with honesty and integrity. Suppliers are also required to meet high standards of financial responsibility.

1281. In assessing whether an applicant meets the requisite standards of honesty, integrity and financial responsibility, the applicant must disclose detailed information describing their past conduct, including work history, finances, criminal and civil proceedings, bankruptcies / insolvencies, as well as personal investments. In addition, information is required on interested persons of the applicant, including business partners, persons who have or may have a beneficial interest in the applicant's business, persons who exercise or may exercise direct or indirect control over the applicant's business, or persons who have or may have given direct or indirect financing to the applicant.

[162] The 17 slot facilities at racetracks (“racinos”) and 5 charity casinos in Ontario are operated by Ontario Lottery and Gaming Corporation while private corporations operate the four commercial casinos.

1282. On an ongoing basis, regulators must be notified if there is any change to the facility licensee's executive or key employees at the casino. Failure to disclose any changes to the regulator can result in sanctions, including the cancellation of registration and fine.

1283. The assessors were told that investigators from the provincial regulators undertake civil, criminal and credit history checks of individual registrants and conduct interviews with associates to ensure the information provided by a registrant is accurate. In cooperation with the RCMP, regulators query the Canadian Police Information Centre database for the disposition of charges for which a person had been fingerprinted (indicating they have a criminal record) and all outstanding charges currently before the courts. Local infraction checking is also conducted through any source that regulators deem appropriate.

1284. For corporations, investigators review the application information and evaluate the financial, business and criminal history of the corporation using information from international, national, provincial, state, county or municipal law enforcement or security agencies; police services and sheriff's offices; government ministries or regulatory agencies; banks, trust companies, brokerage houses, credit bureaus; professional or industry associations, licensing bodies or regulators; and former or current customers.

1285. The Provincial Gaming Corporations have developed corporate governance policies. For instance, the BC Lottery Corporation has corporate governance that refers to clearly defined processes with respect to the selection and composition of the board and senior management and the division of responsibilities, decision making and accountability among the Board, Senior Management and the Shareholder (Government of BC) to ensure the organization's short- and long-term success is consistent with its mandate and mission. The British Columbia Lottery Corporation practices and policies meet the Best Practice Guidelines on Governance and Disclosure for public sector organizations, which was issued by government in February 2005. The corporation has developed a Code of Conduct and Conflict of Interest Guidelines applicable to casinos' directors.

1286. In Manitoba, Québec and Saskatchewan, the crown corporations directly operate the commercial gaming facilities according to government and corporation standards, policies and procedures, including the establishment of new casino operations. Because they have been established to run the gaming in the provinces, they do not require gaming registrations or licenses. However, key gaming employees and gaming employees are required to register and must undergo a similar process as employees of private corporations. As well, Officers and Directors of the crown corporations are required to file a personal disclosure and are subject to a full background investigation prior to their involvement in gaming activities.

Charitable Casinos

1287. Under section 207(1)(b) of the Criminal Code, provinces have the authority to issue charitable gaming licenses to registered charities and religious organizations. Gaming takes place in established charity casinos operated by a private corporation in cooperation with the charity. Charity casinos are not allowed to operate without a participating charity.

1288. Of the 23 charity casinos operating in Canada, 17 are in Alberta. Religious and charity groups apply to the Alberta Gaming and Liquor Commission (AGLC) for 2-day[163] charitable gaming licences that allow the charity to assist in the operation of gaming at a casino. In return for their participation, charities receive a portion of the gaming proceeds to be used for an identified purpose.

1289. Private corporations own the charity casinos in Alberta. Each has a casino facility license with the AGLC that allows it to operate a gaming facility in conjunction with religious or charity group.

[163] Because licenses are only available for two-day events, compliance with the AML/CFT requirements under the PCMLTFA is the responsibility of the casino operator, not the charity.

The private corporation provides key operating personal including gaming employees, security and surveillance.

1290. Prior to obtaining a casino facility license, a corporation must undergo a multi-step screening process. The first step is providing the AGLC with an overview of the proposed casino. The AGLC then publicly advertises the proposal and solicits expressions of interest from other potential applicants to encourage the best possible proposal for a casino in a given market area. The ALGC evaluates the applications based on several factors, including financial footing of the applicant, proposed physical attributes and security features of the casino, and the applicant's understanding and compliance with relevant federal, provincial and municipal legislation and requirements.

1291. Once the market assessment is complete and the successful applicant is chosen, the AGLC will undertake a thorough due diligence investigation into the applicant and any other key persons associated with the applicant. According to the ALGC Casino Terms and Conditions and Operating Guidelines, the investigation is to ensure criminal interests, or those who otherwise would be a detriment to the integrity or lawful conduct of gaming in the province, are prevented from operating, having a financial interest in or having an association with a casino facility license. The ALGC can refuse to issue a casino facility license if they are not satisfied with the integrity of the applicants, individuals involved in the operation of the casino, or business associates, including the officers and directors of corporations controlled by the applicant, and their families. Part of the due diligence investigation on an applicant is a records check to determine whether anyone associated with the application has been charged or convicted with an offence under the Criminal Code, the Excise Act, the Food and Drugs Act or the Controlled Drugs and Substances Act.

1292. The Yukon uses a charity model similar to Alberta's and imposes the same stringent conditions. In Ontario's five "charity casinos", charities do not participate in the operation of casinos but are eligible to receive a percentage of the gaming proceeds from the designated casinos. The Ontario Lottery and Gaming Corporation, a crown corporation established by the province, owns and operates the charity casinos. Although considered charity casinos because of the fund raising component, Ontario's charity casinos are authorised under section 207(1)(a) of the Criminal Code.

First Nations Casinos

1293. First Nations casinos and slot facilities operate in Alberta, Manitoba, Ontario and Saskatchewan[164]. Subsection 35(1) of the Constitution Act, 1982, affirms and recognizes aboriginal rights in Canada. The Supreme Court of Canada in one ruling covering two cases R. v. Pamajewon and R. v. Gardiner Pitchenese and Gardiner (1996), 138 D.L.R. (4th) 204, ruled that gaming (or the regulation of gaming) was not integral to the cultures of the two First Nations claimants at the time of first European contact, which is the test for a claimed aboriginal right. As a result, the First Nations involved in the cases did not have the inherent right to regulate gambling on Indian reserves. Provincial legislation governs the operation of casinos on First Nation land. All First Nations casinos operate under either the charity model or the commercial model and are required to comply with the registration requirements of these models.

Compliance Risk Assessment and Examinations

1294. As of September 30, 2006, FINTRAC had conducted a total of 12 examinations in the commercial casino sector as follows:

[164] In Saskatchewan, First Nation gaming is conducted through an agreement between the provincial government and the Federation of Saskatchewan Indian Nations (FSIN). FSIN formed the Saskatchewan Indian Gaming Authority (SIGA) to operate the casino on its behalf.

FINTRAC Examinations Conducted in Casinos

	2004-05	2005-06	2006-07 (as of end Q2)	Total
Casinos	5	5	2	**12**

1295. As of the end of 2005-2006, the assessors were told that it had also sent 83 questionnaires regarding the implementation of an AML/CFT compliance regime (CQs) to reporting entities in the casino sector, all of which were returned, with globally high rates of positive responses to questions about key compliance elements.

1296. Moreover, to date, FINTRAC has signed five agreements with regulators having supervisory authority over casinos (see table below). Under these MOUs, the assessors were told that FINTRAC and these regulators regularly exchange statistics, risk assessment information, examination results, and examination plans.

Signed MOUs with Casino Regulators (to date)		
1	British Columbia Gaming Policy and Enforcement Branch (GPEB)	July 9, 2004
2	Saskatchewan Liquor and Gaming Authority (SLGA)	November 16, 2004
3	Alberta Gaming and Liquor Commission (AGLC)	December 20, 2004
4	Alcohol and Gaming Commission of Ontario (AGCO)	December 21, 2004
5	Nova Scotia Alcohol and Gaming Authority (NSAGA)	May 6, 2005

1297. These MOU partners had conducted additional 38 examinations in reporting entities for the fiscal years 2005-2006 and 2006-2007 (as of September 30, 2006). These examinations were not systematically dedicated to audit compliance with the PCMLTFA requirements.

Role of Provincial Regulators

1298. In addition to requirements under the PCMLTFA, casinos must comply with the provincial gaming legislation and regulations.

1299. Provincial gaming legislation imposes requirements on gaming service providers and gaming employees to ensure the integrity of the industry. These requirements include mandatory registration, internal control systems, and security and surveillance systems, gaming rules and permitted financial transaction. The legislation also identifies the regulator responsible for the administration of the legislation. The following table identifies the provincial regulator and the key gaming legislation within each province.

Province	Regulator	Primary Gaming Legislation
Alberta	Alberta Gaming and Liquor Commission	*Gaming and Liquor Act*
British Columbia	Gaming Policy and Enforcement Branch,	*Gaming Control Act*
Manitoba	Manitoba Gaming Control Commission	*Gaming Control Act*
Nova Scotia	Nova Scotia Alcohol and Gaming Authority	*Gaming Control Act*
Ontario	Alcohol and Gaming Commission of Ontario	*Gaming Control Act*
Québec	Loto Québec	*An Act Respecting Lotteries, Publicity Contests And Amusement Machines*
Saskatchewan	Saskatchewan Liquor and Gaming Authority	*The Alcohol and Gaming Regulation Act*

1300. Beyond the requirements in the PCMLTFA, most provinces have adopted AML/CFT measures into internal control procedures or provincial gaming legislation, which then become the responsibility of the provincial regulator to enforce, including:

Alberta

• Reporting large, suspicious, and large currency exchange transactions to FINTRAC; • Record-keeping of large cash and suspicious transactions; • Implementation of a compliance regime.	Section 5.9 of Alberta Casino Terms and Conditions and Operating Guidelines

British Columbia

• Reporting *Criminal Code* violations to the provincial regulator (which includes money laundering, possession of proceeds of crime and terrorist financing).	Section 86 of *BC Gaming Control Act*

Nova Scotia

• ID and record-keeping requirements for large cash transactions.	Section 248 of NS Casino Regulations

Ontario

• ID and record-keeping requirements for large cash transactions. • Record-keeping requirement for tracking multiple transactions of CAD 2 500 to an aggregate of CAD 10 000. • Compliance regime • Internal controls for AML/CFT requirements	Section 24, 27 and 28, Ontario Regulation 385/99 under the *Ontario Gaming Control Act*.

Saskatchewan

• Requirement for the Saskatchewan Gaming Corporation to maintain written procedures on recording large cash transactions.	Section 17 of the Saskatchewan Gaming Corporation Casino Regulations

1301. To ensure that casinos are complying with provincial gaming legislation, terms and conditions of registrations and internal control policies, regulators conduct regular and unscheduled audits, compliance reviews and investigate any alleged offences.

1302. The assessors were told that regulators perform audits at least annually to review the financial and reporting records, operating procedures and security systems in place. In addition, regulators conduct interviews with gaming employees to ensure they are familiar with all relevant legislation. Some provinces audit specifically for compliance with PCMLTFA. For example, British Columbia and Ontario have developed a module through which it determines compliance with all of the requirements for casinos under the PCMLTFA.

1303. When minor non-compliance issues are identified, the regulator will work with the casino to resolve the issue. However, when more significant non-compliance issues such as violations to a provincial gaming act are discovered, the regulator undertakes an investigation.

1304. Each province has established an investigative unit within its regulator. These units usually include former or active law enforcement officers with significant expertise in gaming and proceeds of crime investigations. Investigators work cooperatively with the gaming industry, other gaming agencies, law enforcement and other regulatory bodies to identify unlawful activity, and conduct timely and thorough investigations.

1305. Investigators are responsible for the investigation of gaming related complaints and allegations of illegal behaviour and will recommend charges relating to provincial gaming legislation. Law enforcement officials (either RCMP or municipal police forces), in cooperation and with the assistance of the investigative unit, will investigate and lay charges relating to offences found in the Criminal Code.

1306. In Ontario, for instance, the Casino Enforcement Unit provides 24-hour Ontario Provincial Police coverage in the casinos, and is responsible for conducting criminal investigations in relation to gaming inside the casino. The members of this unit liaise with casino security and surveillance staff and with the local police service according to formal protocol agreements. In addition, there are

Compliance Inspectors on-site at the casinos, who are responsible for monitoring the casino for compliance with the approved policies, procedures and internal controls.

1307. If an investigation concludes that there was a violation of the condition of licence or registration, regulators have the authority to impose administrative sanctions and prosecution.

1308. Administrative sanctions may include a warning; refusal to issue or renew a license; suspension or cancellation of a license; imposition of conditions on a license; the imposition of a fine; or other administrative settlements. Regulators can apply additional monetary or other penalties for offences that are contrary to provincial gaming legislation or the Criminal Code. Regulatory or criminal infractions may also result in administrative sanctions, including the cancellation of registration.

1309. In conclusion, casinos in Canada, except for Internet and ship based casinos, are globally subject to a reasonably comprehensive regulatory and supervisory regime. However, it is difficult to express a global opinion regarding the adequacy and effectiveness of the AML/CFT compliance supervision as it may vary a lot from one province to another. While FINTRAC is in principle the sole regulator of casinos for AML/CFT, based on a risk-based approach, the quality of supervision may nevertheless vary from one casino to another depending on whether its provincial supervisor has signed an MOU or not with FINTRAC and whether it performs or not controls in that area. As the provincial regulators are not directly responsible for ensuring compliance with PCMLTFA, their involvement in AML/CFT activities is unequal: some of them, like Alberta or Ontario have incorporated in their own regulatory framework detailed AML/CFT rules, covering most or all of the PCMLTFA requirements, while others, like Manitoba have not included such rules in their compliance program. The methodology and the frequency of examinations may also differ: Saskatchewan Liquor and Gaming Authority, for instance, has no AML/CFT compliance assessment methodology, while Alberta Gaming, Liquor Commission and Alcohol and Gaming Commission of Ontario perform regular and detailed audits. Moreover, the assessment team was not provided with any data or statistics regarding possible sanctions taken by these regulators on the ground of AML/CFT non-compliance issues.

Other DNFBPs covered by the PCMLTFA

1310. Due to the large number of potential entities within the accountants and real estate sectors (in total, about 146 000 accountants and accounting firms and 100,000 licensed real estate agents could be covered under the PCMLTFA if they perform certain activities), FINTRAC is not in a position to monitor closely their compliance with PCMLTFA requirements, even if a large majority of these persons or entities are not actually concerned (as they are not engaged in the specific activities covered by the requirements) and despite the risk-based approach for compliance adopted by FINTRAC.

1311. FINTRAC's compliance program makes use of risk management strategies to identify those reporting entities most in need of improving compliance (see comments below). In order to assist FINTRAC's Compliance team in assessing the risk of non-compliance within particular entities, almost 3 000 CQ had been sent, as of the end of 2005-06, to reporting entities in the accountants and real estate sectors. A further 1 500 have been forwarded to the accountants sector in early fiscal 2006/07, and an additional 1 500 are planned for the real estate sector later in the fiscal year.

1312. Due to the potentially large number of entities within the accountants and real estate sectors and high turnover, continued awareness raising campaigns/outreach are required to ensure obligations are understood. It should be noted that FINTRAC is committed to ongoing outreach with these sectors. As of the end of September 2006 FINTRAC had conducted 139 outreach meetings/presentations with the accounting sector with nearly 2200 participants and 272 meetings/presentations with the real estate sector, with more than 15 000 participants). However, the response rates to Compliance Questionnaires remains relatively low for accountants (75%) and real estate brokers (63%), compared to 89% for financial institutions and 100% for casinos.

1313. The results measured by the positive responses regarding compliance regime are somewhat lower than those for financial institutions or casinos: for instance, only 58% of responding accountants have declared having implemented a compliance regime and 34% an ongoing compliance training program in their entity. This can be partially explained by the fact that, for example, a number of accountants receiving a CQ are not engaged in any of the activities covered under the PCMLTFA (such as receiving or paying funds; purchasing or selling securities, real estate, business assets or entities; or, transferring funds or securities).

1314. As of September 30, 2006, FINTRAC had conducted a total of 26 examinations in the accounting sector, and a total of 95 examinations in the real estate sector. The assessment team was not given any detailed information about the results of these examinations.

	2004-05	2005-06	2006-07 (as of end Q2)	Total
Accountants	0	19	7	26
Real Estate	9	52	34	95

1315. Quite obviously, such a limited number of on-site examinations made by FINTRAC compared with the number of potential reporting entities cannot be considered as sufficient to ensure an effective monitoring of compliance even if FINTRAC targets its examinations based on a comprehensive risk assessment. It should be completed by interventions of provincial regulators or SROs. However, these institutions are not in charge of ensuring AML/CFT compliance and, as for the other sectors examined above, their level of involvement in that area, the regulatory basis on which they rely and the methodology adopted may strongly differ from one province or sector to another.

Provincial Regulation of DNFBPs

Accountants

1316. As mentioned earlier in the report, there are three designations of accountants, all of whom are represented by a national association: Canadian Institute of Chartered Accountants (CICA), Certified General Accountants Association of Canada (CGA) and the Society of Management Accountants of Canada (CMA). It is the role of the provincial institutes and associations to ensure that accountants are complying with the rules of professional conduct and corresponding by-laws to ensure that accountants are protecting the public interest.

1317. *Canadian Institute of Chartered Accountants*. For the purpose of outlining the monitoring and supervisory regime, focus will be placed on CICA, the group of accountants with the most likelihood of undertaking the types of financial transactions covered by the PCMLTFA.

1318. The CICA has developed a Guide (originally published in 2002 and updated in 2004) to assist CAs and CA firms in understanding the obligations imposed by the PCMLTFA. It indicates that CAs should be mindful of the possibility of money laundering and risks of becoming a party to the offence by failing to take the appropriate action. Early in 2006, the CICA established an Anti-money laundering advisory Committee whose objectives are to provide advice to Department of Finance on proposed changes to AML regime and to provide advice to CICA staff for updating the 2004 Guide. It is currently elaborating detailed guidance regarding the activities which should be considered as covered by the AML/CFT regime. Rules of professional conduct specifically address “unlawful activity” and establish the minimum level of ethical conduct for accountants.

1319. Provincial institutes of Chartered Accountants work in partnership to develop and enforce national standards, which are not relating specifically to money laundering but are designed to protect the public interest and maintain the good reputation and integrity of the CA profession. To help ensure that accountants are complying with the rules of professional conduct, provincial institutes undertake inspections of all members in public practice.

1320. Each year, approximately 25% of all firms in private practice are inspected. The selection of firms is made on an ongoing, cyclical, basis. New firms are selected within the first year of operation while other offices are normally selected every four years from the date of their last inspection. The inspection primarily focuses on the firm's quality control system and a review of current engagement files and related financial statements in order to assess adherence to professional standards. If inspection reveals significant shortcomings, the matter is referred to the professional conduct committee.

1321. After assessment, the committee may conclude that a breach of the rules of professional conduct has taken place and a charge or charges should be laid. In this event a formal hearing is held before the CICA discipline committee. The discipline committee has the authority to summon witnesses and require the production of evidence relevant to the case. The discipline committee has the power to impose administrative fines; suspend or expel a member; restrict a firm's practice; and publicize the decision of the committee. All cases that result in a finding of guilty of professional misconduct are made publicly available on provincial institutes' websites. Details of cases are made available to law enforcement authorities to assist in their investigation. No further information was provided to the assessment team on actions taken in relation to non-compliance with AML/CFT obligations.

1322. In addition to the role of the provincial accounting institutes and associations, the Canadian Public Accountability Board (CPAB) plays an oversight role of its member firms to ensure the integrity of financial reporting of publicly listed companies by promoting high quality, independent auditing. CPAB conducts inspections of public accounting firms that audit publicly listed companies to ensure compliance with professional standards and participation requirements. Firms with 50 or more clients that are publicly listed companies are inspected annually while those with less than 50 will be inspected on a three-year cycle. CPAB has entered into MOUs with the provincial accounting oversight bodies under which those institutes will inspect the smaller firms on behalf of CPAB. Where appropriate, CPAB imposes sanctions and restrictions on public accounting firms that publicly listed companies and, where necessary require remedial action, including referring matters to provincial accounting organizations for discipline purposes or to securities regulators.

1323. *General Accountants Association of Canada*. The Certified General Accountants Association of Canada has developed a Code of ethical principles and rules of conduct designed to protect the public and ensure that CGAs maintain the highest ethical standards. Specific provisions prohibit members from participating in or providing services to any activity that the member knows or which a reasonably prudent person would believe to be unlawful.

1324. Provincial associations have adopted the Canadian Association's standards of conduct contained in the Code of ethical principles and rules of conduct. In the case of breach of professional conduct as defined by the Code, members are subject to disciplinary action through the member's Provincial association or Ordre professionnel. Every registered public practitioner is required to have a peer review or audit at least every three years and to have a Policies and procedures Manual.

Real Estate Agents

1325. *General*. In addition to AML/CFT compliance supervision by FINTRAC, real estate agents are subject to monitoring by provincial regulators to ensure compliance with the provincial real estate legislation. In addition, real estate agents have industry associations that represent them at the local, provincial and federal levels. The associations also provide awareness and information on AML/CFT requirements for the real estate industry through training and workshops. The following section describes the compliance and oversight activities of the provincial regulators and the industry associations in the real estate industry.

1326. *Regulators*. Provinces are responsible for the regulation of real estate industry professionals. Provincial real estate legislation establishes the regulatory function within an agency or council in seven provinces (Alberta, British Columbia, Newfoundland and Labrador, Nova Scotia, Ontario,

Québec and Saskatchewan). In the other six provinces and territories (Manitoba, New Brunswick, Prince Edward Island, Northwest Territories, Yukon Territories and Nunavut), the government performs these activities directly.

1327. The responsibility of the regulator includes licensing of professionals (including admission exams and education requirements); setting and enforcing standards of conduct and business practices; and administering the provincial real estate acts and the bylaws and rules that have been established by the provincial regulating body.

1328. *Audit and investigation*. To ensure that real estate agents are complying with their requirements under provincial real estate legislation, regulators in Alberta, British Columbia, Nova Scotia, Ontario, Québec and Saskatchewan use a risk-based approach to determine which firms are selected for audit. In determining risk provinces include factors such as the size and location of the firm, deficiencies in accountant reports and previous audits and the amount of trust monies held. In addition, the regulator chooses some firms on a random basis for audit.

1329. Regulators provide courtesy audits to new brokers. A courtesy audit is an educational resource to ensure that new brokers are aware of the provisions of provincial real estate legislation as it applies to brokerage accounting. During the process, an auditor reviews the agent's books and records and provides assistance to make appropriate changes.

1330. During the audit, the auditor may review books and records, policies and procedures, trust and other account details and samples of open and closed files. Firms are required to keep records for a minimum of three years. Serious concerns discovered during an audit are forwarded to an investigation unit. Investigators determine whether there has been conduct that deserves sanction. Investigators have the power to collect all evidence relevant to the investigation, including interviews with the complainant and the industry member. The investigator has the authority to inspect or examine the books, documents and accounts (including the trust accounts) of any broker. In addition, industry members are required by the provincial real estate acts to cooperate with investigations, including responding to questions and providing requested documentation. If evidence of criminal activity is obtained during an investigation, it can be forwarded to law enforcement for a criminal investigation.

1331. Following an investigation, the regulator has the power to impose sanctions, including administrative penalties; suspension of the license to practice; and prosecution in the courts. It is worth noting that in provinces where the regulator does not conduct regular audits, each firm is required to submit reports from a public accountant verifying that transactions and accounts are being managed in accordance with provincial legislations.

1332. The assessment team did no get evidences that such audits and investigations are dedicated to check compliance with the AML/CFT requirements.

Dealers in Precious Metals and Stones

1333. Dealers in precious metals and stones do not have an established regulator. The Jewellers Vigilance Canada (JVC) has established a code of ethics and standards of practice to guide the professional behaviour of jewellers. Although it does not play an enforcement function, Jewellers Vigilance Canada provides members information and training on AML/CFT issues and has developed a crime prevention training package for members of the jewellery industry. In addition, Jewellers Vigilance Canada works closely with the RCMP to provide them educational support on the jewellery industry and information pertaining to specific crime. JVC also works closely with the Department of Finance on the new regulations covering the sector.

Lawyers and BC Notaries

Legal Counsel

1334. *General.* As described in Section 1.3, access to the profession and professional conduct for legal counsel is regulated and supervised at the provincial/territorial level of government through self-regulatory organizations (SRO). Each SRO is empowered through provincial/territorial legislation to regulate the profession to ensure a competent and ethical bar and authorises the SRO to educate, license and regulate the conduct, capacity and competence of legal counsel. Only members of an SRO can practice law in a given jurisdiction.

1335. There are nine provinces and three territories governed by the common law tradition and each jurisdiction has separately empowered SROs (law societies). The province of Québec follows the civil law tradition and has two separate SROs for the legal profession, the Barreau du Québec and the Chambres des notaires du Québec.

1336. Due to the differences between the civil and common law traditions, only notaries in Québec provide legal advice and are thus considered legal counsel. In the common law provinces, except British Columbia, licensed legal counsel only provide notary services. In British Columbia, a separate self-regulatory organization licenses 332 individuals to provide notary services and supervises the profession. These notaries are not considered legal counsel and the protections afforded under solicitor-client privilege do not apply.

1337. Legal counsel in Canada can be a member of multiple jurisdictions. In doing so, they must abide by the rules and conditions placed on them by the law society of that province/territory. In addition, each law society is a member of the Federation of Law Societies of Canada, the national coordinating body. In total the 14 SROs regulate Canada's lawyers and notaries.

1338. SRO by-laws and Rules of Professional Conduct set out the professional and ethical obligations for their members, including conduct and procedures relating to trust accounts and cash prohibition. Members failing to meet these obligations are subject to the SRO's disciplinary process. Each SRO has procedures and resources for dealing with professional misconduct and for taking action when appropriate. The SROs have the authority to impose fines, suspend the member from practicing, impose conditions on the member's practice and in serious cases, disbar the member.

1339. Each provincial and territorial law society, including both SROs in Québec, have implemented rules of professional conduct that prohibit legal counsel from accepting CAD 7 500 or more in cash in connection with a single client file or matter. This in essence limits the ability of criminals to place cash into the financial system through legal counsel. These rules are binding on the profession and enforceable by each provincial/territorial SRO. The SROs have incorporated the compliance examination of the cash prohibition rule into their standard compliance procedures pertaining to trust accounts. The standard compliance procedures include the use of an annual attestation by members indicating that they have not accepted cash of CAD 7 500 or more as well as spot and random audits of members' files and trust account statements. While the frequency of full audit varies amongst SROs, generally, each legal counsel undergoes an audit of their practice every three years, with every legal counsel being required to file annual reports to the appropriate law society. The cash prohibition rule has only been fully implemented in all jurisdictions since March 20006 and thus at the time of publication of the MEQ has not yet been subject to an annual report in all jurisdictions.

1340. There is no AML/CFT supervision *per se* as far as legal counsel is concerned.

British Columbia Notaries

1341. As indicated above, notaries in the province of British Columbia are supervised and regulated by a separate SRO. They are not considered legal counsel. The profession is governed by the British

Columbia Notaries Act, however, for the purposes of AML/CFT requirements, there is no authority for monitoring and ensuring compliance of BC notaries[165].

Recommendation 25 (Guidance for DNFBPs other than guidance on STRs)

1342. Guidance available to casinos, real estate agents/sale representatives and accountants is generally comprehensive and rather detailed.

1343. *Guidance for casinos, real estate agents/sale representatives and accountants*. FINTRAC provides casinos, real estate brokers and sales representatives, and accountants with specific guidance concerning the implementation of a compliance regime (Guideline 4), and record keeping and client identification (Guideline 6).

1344. FINTRAC has also developed a number of other resources to assist reporting entities in understanding their obligations under the PCMLTFA. These include Sector Specific Information Sheets and various pamphlets, which can be found on FINTRAC's website. Furthermore, a nine-minute video was produced to inform reporting entities of their legal obligations and helps explain FINTRAC's role. The video is accessible on FINTRAC's website and has also been distributed to reporting entities on DVD.

1345. Finally, FINTRAC also directs the operations of a call centre and a toll-free telephone line to serve the public and reporting entities. The service is available for 12 hours each day, from Monday to Friday.

1346. In addition to the guidance provided by FINTRAC, the industry associations and regulators in some provinces also provide AML/CFT guidance to their members.

1347. *Guidance for accountants*. As described above, CICA has developed a guidance document to assist CAs in their understanding of the requirements under the PCMLTFA and to outline the responsibilities of CAs flowing from those requirements. Ongoing money laundering information is provided through the CICA monthly magazine sent to all members called the CA Magazine. Articles inform members of ongoing changes to legislation, report on recent money laundering conferences and training, and inform on trends and cases.

1348. *Guidance for real estate agents*. Real estate industry associations at the local, provincial and federal levels provide members with significant guidance on their AML/CFT requirements under the PCMLTFA. The Canadian Real Estate Association (CREA) is comprised of provincial real estate associations and local boards throughout the country and is concerned with improving real estate practices across Canada. A key focus of CREA's activities is to educate members on federal issues, including providing awareness and requirements of real estate professionals on AML/CFT issues.

1349. In addressing this, CREA has developed an AML/CFT Internet site for members of the real estate industry called "*the Canadian Real Estate Money Laundering Compliance Centre*". Through this site, real estate agents (brokers and sales representatives) have access to online training, the procedures that real estate agents must have in place to be compliant with the PCMLTFA, as well as direct access to FINTRAC large cash, suspicious and terrorist property reporting forms.

1350. Continuous learning is a requirement of maintaining a real estate license in most provinces. To meet this requirement, provincial real estate associations have made available courses on money laundering that give real estate agents an awareness of the susceptibilities of the industry and their requirements under the PCMLTFA. In addition, a component of the required course to obtain a real estate license focuses on money laundering. Local boards work closely with local agents and promote the training available from the federal and provincial associations. In addition, local boards organize

[165] Canada indicated that BC Notaries are covered by regulations enacted in December 2007 and coming into force in December 2008.

discussions and presentations on topics of interest to their members. For example, the Ottawa Real Estate Board arranged for the RCMP and FINTRAC to give presentations to better inform members of their requirements under the PCMLTFA.

1351. *Other initiatives*. In order to provide advice and assistance to, as well as maintain relationships with the 91 casinos, FINTRAC has had 73 meetings with the majority of the reporting entities from that sector since 2004/2005. These meetings, in a number of cases, would have involved more than one reporting entity. These meetings and presentations are with, or are attended by, all levels of the organization in question. A total of 542 casinos' employees attended these meetings.

1352. In order to provide advice and assistance and maintain relationships with accountants and real estate brokers, FINTRAC had 411 meetings with these sectors since 2004/2005. 2 186 accountants and 15 316 real estate agents attended these meetings.

4.3.2 Recommendations and Comments

1353. *Recommendation 24*. Canada should ensure that supervisory action (especially on-site examinations) vis-à-vis casinos, but more importantly with respect to all other DNFBPs is strongly reinforced. The role, functions and monitoring powers of other regulators and SROs in ensuring compliance of DNFBPs with the AML/CFT requirements should be clarified. Canada should consider revisiting the supervision issue as a whole and give further consideration on whether FINTRAC should be the only authority in charge of ensuring compliance with the AML/CFT requirements (see conclusions in Section 3.10 of the report). The Department of Finance or FINTRAC should collect detailed information about the AML/CFT regulation and supervision role and action of all the provincial regulators/SROs in order to get a complete overview of the current situation.

1354. The sanction regimes applicable to DNFBPs, including casinos, should be reinforced and Canada should ensure that the sanctions available for failures to apply AML/CFT requirements are effective, proportionate and dissuasive.

4.3.3 Compliance with Recommendations 24 & 25

Rec.	Rating	Summary of factors underlying ratings
Rec.24	NC	*Scope issue* • Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and not subject to FINTRAC supervision. *Supervision of casinos* • The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the grounds of AML/CFT non-compliance issues have been made available to the assessment team. *Supervision of other DNFBPs* • Limited staff resources deprives FINTRAC from closely and efficiently monitoring DNFBPs' compliance with the PCMLTFA requirements especially in sectors/provinces where the primary regulators or SROs are not or insufficiently involved in AML/CFT compliance supervision. • The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the ground of AML/CFT non-compliance issues have been made available to the assessment team.
Rec.25	LC	• Lack of sufficiently sector-tailored guidance - see factors in Sections 3.7 & 3.10 of the report.

4.4 Other non-financial businesses and professions – Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

Considering applying AML regime to other non-financial businesses and professions at risk of being misused for ML

1355. As part of the development of the amendments to the PCMLTFA and in preparation of the Government of Canada June 2005 Consultation Paper, research and analysis was conducted on the domestic money laundering and terrorist financing risks and the operational feasibility of expanding the coverage of the Act to other non-financial businesses and professionals that are not explicitly subject to the FATF Recommendations.

1356. A number of new sectors were discussed, including auto dealers and auction houses. They have been targeted for further examination and ongoing monitoring. A lack of perceived risk led the Government to conclude that the application of PCMLTFA measures to these sectors was not warranted at this time.

"White label" automated banking machines

1357. White label ATMs in Canada provide alternative source of cash dispensing vis-à-vis traditional ATMs owned and operated by banks, other financial institutions and cash back debit services offered by retailers at the point of sale. In Canada, most deposit taking financial institutions have their own branded ATMs located throughout the country. These ATMs prominently display the logo of the financial institutions. A "white label" or no name ATM, which are usually located in non-traditional places (bars, shops, etc.), while branded, display no major financial institution labels on the actual ATM. After 1997, independent operators were allowed to operate ATMs, not owned by major financial institutions. In 2006, a little more than half of the 51 000 ATMs in operation in Canada were "white label".

1358. White-label ATMs are owned and operated by non-financial institutions. They are not under federal jurisdiction because they are not considered as financial institutions. However, concerns have been raised due to the unregulated nature of the business and the fact that the white label owner or operator can load these machines himself, thus creating an opportunity to "place" illicit cash into the financial system.

1359. Interac is the organization responsible for the development and operation of a national network of two shared electronic financial services: Shared Cash Dispensing at automated banking machines and Interac Direct Payment ("IDP"), Canada's national debit service. In June 1996, the Competition Tribunal ordered that Interac must broaden its membership to non-financial institutions and allow these non-financial corporations to deploy automated teller machines (ATMs).

1360. The Government's approach to date has been to rely on safeguards put in place by the Interac Association and on financial institutions holding the settlement account of the owner of the ATMs. When a small or unknown corporation applies for membership, Interac carries out corporate and other searches (*e.g.* background and bankruptcy checks). In 2003, Interac amended its regulations in order to enhance the safety and soundness of the network and assure the integrity of its system. The regulations increased due diligence requirements for all financial and non-financial organisations involved in the delivery of Interac services and strengthened inventory control procedures for ATMs and point-of-sale terminals. The regulations emphasized Interac members' accountability and responsibility for all their downstream business partners in order to address fraudulent attacks against their systems. Interac has developed new measures in the following areas:

- *New member process*: changes to the new member process to include an enhanced review of the business plans and enhanced background searches.
- *Regulations governing acquirers*: acquirers provide access to the Interac network and process ATM transactions for White Labels. Acquirers are required to conduct due diligence tests on business partners with whom they have a direct business relationship, such as independent sales organizations. Acquirers will have to actively monitor ATMs for fraudulent activity.

1361. However, there is currently no supervision of the acquirers themselves: the Shared Cash Dispensing service is built on a decentralized model with the individual members wholly responsible for their own business and their performance. Regulation and requirements regarding the monitoring of transactions by a third party (in order, for instance, to detect atypical profiles of transactions on certain ATMs such as withdrawals significantly above the norm in volume or value , or at atypical times, cash replenishments by the owner non consistent with his activity etc.) should be implemented.

1362. The assessors were told that the Department of Finance, the RCMP, FINTRAC and Interac continue to examine the AML/CFT risks created by white label machines and measures to address these risks. Measures could include a prohibition on self-loading and self-servicing of the ATM, and/or requiring a source of funds declaration from machine owners. The industry is committed to addressing any ML related risks and recognises that any gap poses a reputation risk. In addition, there is a clear recognition from the industry that these risks need to be addressed whether by industry or regulatory solutions. Possible measures contemplated include enhanced due diligence requirements on acquirers, including the requirement to obtain more information from the machine owner or operator, such as the source of funds, enhanced record-keeping (bearing in mind that every transaction from every machine is recorded and kept by the acquirer for a minimum of 7 years in order to comply with tax laws) and compliance enforcement.

1363. The legislative framework currently in place provides certain safeguards. For instance, the Minister of Finance has the authority under the Canadian Payments Act to designate and oversee a payment system, if it is in the public interest to do so. When a system is designated, the Canadian Payments Act requires that a copy of every rule be sent to the Minister of Finance and gives the Minister of Finance the power to disallow the whole or a part of a rule, as well as the power to issue guidelines and directives. In determining whether a system should be designated, a number of factors are considered, including the safety, efficiency, competitiveness and the best interests of the financial system. Further work needs to be done to address the risks of ML and TF with the industry. The risk issues are being addressed through further discussions with the industry.

1364. The assessment team believes that the current measures do not adequately address the risks and that it is important that the authorities undertake further action, possibly with the objective of introducing a registration and monitoring system for the owners of the ATMs.

Stored Value Cards

1365. Another new trend that is currently monitored is the use of stored value cards. An increasing number of these cards are put in circulation by certain financial institutions and a growing number of retailers. The assessment team was told that there is anecdotal evidence that stored value cards have been used to carry funds into and out of Canada.

1366. *Requirements of financial services provided via the Internet*

1367. Internet payments are an emerging area in Canada, with the largest industry player being PayPal. Finance is currently involved in discussions with PayPal and other Internet Payment Processors (IPPs) in an effort to better understand their business models and determine where the transactions are domiciled, who their client base are and whether the services offered by IPPs to Canadians carry money laundering and terrorist financing risks. In addition, Finance commissioned a research study by an outside consultant on this issue and is reviewing the findings of that study.

Real estate developers

1368. The sales of new homes or buildings are covered by the PCMLTFA and its regulations to the extent that home builders rely on a real estate broker or sales representative to sell the property. However, many real estate developers use an in-house employee to conduct the same work. The purchase of a new property often involves progress payments over the construction of the house or building, which offers criminals opportunities to place illicit funds in the system[166].

Reducing reliance on cash and secure automated transfer systems

1369. Canada's clearing and settlement system is secure and efficient, enabling consumers and businesses to make and receive payments and transfer funds throughout the country quickly and reliably. This has fostered a greater reliance and early adoption of non-cash payment mechanisms.

1370. The Canadian Payments Association operates national clearing and settlement systems that facilitate this flow of funds and mitigate risk to payment system participants. Its membership consists of financial institutions, which are reporting entities under the PCMLTFA.

1371. The Canadian Payments Act sets out the legal framework for the Canadian Payments Association, including its mandate, the types of organizations that are eligible for membership, the role of the Board of Directors and oversight responsibilities for the Minister of Finance. A key element of the Canadian Payments Association's mandate is facilitating the development of new payment methods and technologies.

1372. On average, some 20.6 million non-cash payment items, representing CAD 164 billion in transactions, were cleared and settled through the Canadian Payments Association's Automated Clearing Settlement System and Large Value Transfer System each business day during 2005. These include cheques, wire transfers, direct deposits, pre-authorised debits, bill payments and point-of-sale debits.

1373. Canadians have been early adopters of new banking technologies. Since the launch in 1986 of the Interac Association, the operator of the national debit card network, Canadians have been one of the highest per capita users worldwide of debit cards. According to the Bank for International Settlements, Canadians made 3.1 billion debit card transactions in 2005, or 95 transactions per person, worth over CAD 137.5 billion.

1374. MasterCard and Visa operate the principal credit card networks in Canada. In 2005, Canadians made 1.9 billion credit card transactions, or 60 transactions per person, worth CAD 209.5 billion according to the Bank for International Settlements. Other credit card networks operating in Canada include American Express, Discovery Card and Dinner's Club.

Discontinuation of the CAD 1 000 note

1375. On May 12, 2000 the Bank of Canada stopped issuing CAD 1 000 bank notes and began to withdraw them from circulation. The announcement followed the federal government's approval of an amendment to the Bank of Canada Notes Regulations to eliminate the CAD 1 000 note as part of the fight against money laundering and organized crime. This decision was recommended by the Department of Finance in consultation with the Bank of Canada, the federal Solicitor General, the Royal Canadian Mounted Police, and other Canadian law enforcement agencies.

1376. At that time, the Bank of Canada indicated that after it stopped issuing CAD 1 000 notes, the notes already in circulation would remain legal tender and would retain their full face value.

[166] The Department of Finance views this situation as a gap and, Canada indicated that, for this reason, Finance pre-published new regulations in October 2007 to subject the sector to the same requirements as real estate brokers and sales representatives.

Individuals are free to hold and use the notes for as long as they want. This is true for all Bank of Canada notes that are no longer issued, such as one- and two-dollar notes.

1377. The CAD 1 000 notes were withdrawn from circulation over time with the help of financial institutions, which return the notes to the Bank of Canada as they are deposited or exchanged by the public. All CAD 1 000 notes returned to the Bank of Canada are destroyed.

1378. The withdrawal of the CAD 1 000 note had little impact on Canada's currency system and its ability to meet the needs of businesses and individuals. The note was rarely used for cash transactions. In 1999, for example, there were about 3.8 million CAD 1 000 notes in circulation, representing less than 0.3% of all notes in circulation. As of October 31, 2006, 1.4 million CAD 1 000 notes were in circulation. The largest note in active circulation is the CAD 100 note.

4.4.2 Recommendations and Comments

1379. The authorities are engaged in considering the need to extend the AML/CFT requirements to a number of key areas, and this work should clearly proceed as quickly as possible. On the basis of comments by law enforcement, the money laundering risk appears to have been appropriately identified; however, insufficient AML/CFT measures have been implemented to address the risk for these businesses and products (especially "White Label" ATMs). Canada should take additional action to address this issue as soon as possible.

4.4.3 Compliance with Recommendation 20

Rec.	Rating	Summary of factors underlying ratings
Rec.20	C	• The Recommendation is fully met.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and Analysis

Transparency concerning the beneficial ownership and control of legal persons

1380. The principal form of legal person in Canada is a company/corporation. Canadian corporate law (both federal and provincial) permits private, public and unlimited liability companies. The principle federal law is the Canada Business Corporations Act (CBCA); however, the laws of Alberta, Saskatchewan, Manitoba, Ontario and New Brunswick reflect most provisions of CBCA. The majority of corporations operating in Canada are incorporated under Ontario business corporation law but a substantial number of companies are incorporated under the laws of Alberta, Quebec and British Columbia and the federal jurisdiction. Given the similarity in systems, the assessment team focused primarily on the federal CBCA.

1381. The CBCA requires the following information on incorporation:

- Name of the corporation and descriptions of the business activities and intended clients.
- Provincial or territorial location and civic address of the registration office.
- Descriptions of the shares, classes of shares and the maximum share capital that the corporation may issue.
- Description of any limits on share transfer (companies will provide this information if they are registering as a private corporation and so will not have to comply with the registration and

prospectus filings requirements and other related procedures set out in the CBCA and provincial/territorial securities law[167]).

- Number of directors of the corporation and the name and residential addresses of the directors of the company.
- Names and addresses of the incorporators, who must be least 18 years of age and not in a state of bankruptcy.
- Additional rules and regulations that will govern the conduct of the company members and directors.

1382. CBCA also requires corporations to file an annual return with details such as the name of the corporation, the date of incorporation and any changes in corporate information, and to file notice of any changes to directors or the address of the registered office within 15 days. Broadly similar requirements exist in Ontario and Quebec.

1383. There is no requirement to list identifying information relating to shareholders when filing incorporation documentation. No information on the beneficial owners (as defined by the FATF) of the company being established is collected. The information provided in the incorporation process is reviewed by staff at the applicable corporate registries to ensure that the entity meets the legal requirements for incorporation, but there is no requirement in legislation for those registries to verify the accuracy of the information provided.

1384. Corporations are also required by the CBCA to prepare and maintain records at their registered office or at any other place in Canada designated by the directors and be available for inspection by directors, shareholders, creditors and incorporation authorities. These records must include a register of directors, officers and shareholders (including a list of the names and addresses of all shareholders by class of shares) and be available to directors, shareholders and creditors. Inspection of these records under the CBCA has to be supported by an affidavit that the information used shall be only in respect of the company's affairs. Also the CBCA requires that in the annual information circular companies should identify the shareholders who hold the largest number of shares. However, it is important to note that there is no requirement that the ultimate beneficial owners of shares be identified in the corporate records of private companies and, moreover, there is no legal requirement to indicate in these records if, or when, a transfer of shareholding has occurred. Public companies are, on the other hand, required to disclose on the company's information circular any shareholder who beneficially owns, directly or indirectly, or controls or directs, voting securities carrying 10% or more of the voting rights attached to any class of shares. This requirement is, however, limited to the persons who are the immediate holders of the beneficial interest and not the ultimate beneficial owners as required by Recommendation 33.

Access by competent authorities to information on the beneficial ownership and control of legal persons

1385. Regulatory, taxation, intelligence agencies, supervisory and law enforcement authorities (including Police, CRA, FINTRAC and securities regulatory authorities) have a variety of powers that enable them to secure information about the control and ownership of legal persons in Canada both from publicly available sources and through a variety of coercive measures. Regulatory and supervisory authorities also maintain records on persons who are the beneficial owners of their regulated/supervised institutions. For example, information is obtained by OSFI on persons that hold 10% of more of the shares in federally regulated banks & insurance companies, and the Director of Corporations Canada and securities regulators obtain information on persons that hold 10% or more of the shares in listed companies.

[167] To qualify as a private company, there must be fewer than 50 shareholders and shares must not be offered to the public.

1386. Coercive measures include production orders, search warrants in justifiable circumstances and court ordered inspections in others. Law enforcement authorities may also take statements from witnesses. Securities regulatory authorities have a wide range of powers to secure information including the authority to compel production of information, compel testimony and evidence, as well as other powers. For publicly available information those authorities may search the appropriate corporate registries in addition to other publicly available data bases relating to corporations for any relevant information.

1387. Through its regulatory reviews, civil audits and investigative actions, and information filed in tax returns, the CRA has access to a large amount of information. However, this does not extend to beneficial shareholder information. In addition, throughout the conduct of its administration, the CRA is bound by its own legislation and policies regarding the disclosure of information. The provision of information is permissible if the sharing of such information can reasonably be regarded as necessary for the administration or enforcement of the applicable Act, specifically the Income Tax Act or Excise Tax Act. This agency is constrained with regards to the information (and the circumstances) in which it can share information uncovered in the course of its administration of the tax statutes. For example, it can only share information with the RCMP when an information/indictment has already been laid. To obtain information via court order, the RCMP must prove that the information will be of substantial value to the case.

1388. As mentioned earlier in this report (see Section 2.5), FINTRAC is limited in the nature of information it is able to provide to law enforcement authorities[168]. In addition, the financial institutions that report to FINTRAC are not required by law to obtain information relating to the beneficial owner of legal arrangements. Under the PCMLTFA, the requirement is to establish the existence of the legal person, but not the ultimate beneficial owner (see Section 3.2 of the report).

1389. Law enforcement has a number of powers to gather information on control and beneficial ownership of legal persons from a variety of sources as outlined in this section, and also may use powers to access further information from non-public sources in the course of investigations. However, these powers are constrained insofar as several entities and persons that ought to be repositories of this type of beneficial owner information (*i.e.* company services providers, financial institutions and registries) do not currently maintain this sort of information. This is likely to affect the ability of the authorities to access accurate and current information on the ultimate beneficial owners and controllers of legal persons on a timely basis.

Bearer shares

1390. While s 24(1) of the CBCA provides that shares of a Canadian corporation must be in registered form and without nominal or par value, ss 48(1) and 187(9) of the CBCA appear to permit bearer shares to be issued by corporations. Similar provisions recognising the use of bearer shares also exist in the Manitoba Corporations Act (though not in Ontario). The CBCA provisions appear to establish that bearer shares remain a legal means of taking an ownership interest in a Canadian company. CBCA section 54 in particular indicates that securities (including shares) are fungible and that delivery may be effected either in bearer form or in registrable form. But there is no legal mechanism to require disclosure of the person or entity which holds, or is the beneficial owner of, bearer shares of any particular corporation incorporated under the CBCA.

1391. The assessment team were advised by Canadian officials, who had in turn been advised by various corporate share registrars, custodians/trustees, and securities participants in general, that they had not seen bearer shares in practice. However, it should be noted that it is most unlikely that bearer shares issued in private corporations would pass through registrars or custodians anyway, and the assessment team is not aware as to how broad a sample of private sector representatives provided

[168] Fintrac can disclose a broader set of information to law enforcement since 30 June 2007.

information. In practice it is likely that the number of bearer shares may be quite limited, but it is important that the right to issue such shares exists, and there are no mitigating measures.

Additional elements

1392. Outside the information contained in the corporate registry documents of corporations, which contains limited information on shareholders as indicated above, there are limited mechanisms to ascertain beneficial ownership information for corporations in the Canada.

5.1.2 Recommendations and Comments

1393. Although the authorities may be able to get some information on legal or beneficial ownership of a limited class of companies, such as public companies or certain classes of financial institution, these only constitute a small percentage of the total number of companies, and also those which appear to be lower risk. Canada's general corporate registry and information collection system does not focus on obtaining information relating to the beneficial owner or controller of bodies corporate in Canada. The information maintained (including changes in information) relates almost solely to persons and other corporations that are the immediate owners or controllers of a company through shareholdings.

1394. The assessors noted that the federal companies registry did not seem to be focussing on the issues relating to money laundering and the financing of terrorism and were not implementing any special measures in this regard. For example, the registry did not cross-reference applications for company formations against the terrorist lists issued by the other agencies of Government. Measures such as these could act to mitigate to some extent the threat that arises through the use of legal persons to perpetrate terrorist financing.

1395. Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis. The current powers of the competent authorities are hampered to the extent that the repositories of information from which the authorities could obtain beneficial ownership information do not maintain beneficial ownership information, and for authorities such as CRA there are statutory barriers to the sharing of the information that is held with law enforcement or other competent authorities.

1396. The Canadian CBCA appears to allow for the ownership of companies through the use of bearer shares (as does the Manitoba legislation, though not Ontario) although it is likely that these shares have limited use in practice. Nonetheless, there do not appear to be any special measures in place, in particular with private corporations, to ensure that disclosure of beneficial owners of these shares so that they cannot be exploited by money launderers or those who would finance terrorism.

5.1.3 Compliance with Recommendation 33

Rec.	Rating	Summary of factors underlying ratings
Rec.33	NC	• There is no requirement to ensure adequate transparency, for instance there is no obligation that information on the beneficial ownership of shares in legal persons is required to be collected by either the corporate registry, within corporate records held by legal persons or by lawyers, accountants or TCSPs. • While law enforcement and other authorities have sufficient powers, those powers are not adequate to ensure the existence of adequate, accurate and timely information on the beneficial ownership of legal persons, which can be accessed or obtained in a timely fashion by competent authorities. • There are no measures to ensure that bearer shares are not misused for ML, particularly for private corporations.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

General

1397. Under the Constitution of Canada, property and civil rights are a matter of provincial legislative jurisdiction. Except for the province of Quebec, all provinces are common law jurisdictions and have trust law which requires three essential components: a settlor, a trustee, and beneficiaries. Essentially, the establishment of a trust results in a transfer of proprietary rights. The trust property can be any form of property whether real or personal, tangible or intangible. In general terms, a settlor transfers legal title of specific property to a trustee but beneficial ownership to specified beneficiaries[169].

1398. In Québec, the fiducie results from an act whereby a person transfers property from his or her patrimony to another patrimony that he or she constitutes; the property is appropriated for a particular purpose and a trustee undertakes to hold and administer it (Article 1260 of the Civil Code). As a legal arrangement, the fiducie in Quebec is similar to the trust as defined above. The assessment team was not provided with information on measures taken to ensure adequate transparency concerning the beneficial ownership and control of fiducie in Québec.

1399. There are a number of different kinds of trusts in Canada with a range of purposes, but there is no general legal requirement that a trust be evidenced in writing. For those trusts that are evidenced in writing a trust instrument, such as a declaration or trust agreement (including a deed), setting out the rights and obligations of the trustees and beneficiaries, and in some cases certain third parties, is usually employed as the appropriate vehicle. Provincial legislation provides for the rules to be followed by trustees. Trusts are not separate legal entities however. Trustees are persons responsible for the trust property; hence, the trustee is liable for the obligations incurred in the name of the trust.

1400. A number of persons offer services to establish and administer trusts on behalf of trustees in Canada and they include: trust companies, lawyers and accountants (for the most part). Other trust and company service providers exist in Canada (which is discussed in Section 4.1 of the report) but limited information was available on the extent of the role of such service providers in the business of establishing or servicing trusts. There is no legal requirement that obliges these trust providers to collect information on the settlor, trustees and beneficiaries notwithstanding that as a matter of practice they would normally collect this information as vital to the establishment of a trust. However, for those entities which fall within the definition of "financial institution" under the PCMLTFA (to a large degree trust companies would be so defined), there are specific provisions requiring the collection of information relating to settlors, trustees and beneficiaries (see Section 3.2 of the report).

1401. Some pooled investment funds, such as mutual funds, or pension plans use trusts as vehicles to administer the funds on behalf of their beneficiaries. These types of trusts are frequently referred to as "pooled funds" or "pension trusts" (usually managed by a trust company or a board of trustees). In Canada, pension trusts are regulated by the federal government or by provincial governments. OSFI supervises federally regulated pension plans. These plans and the other investment plans noted fall within the definition of a "financial entity" within the PCMLTF and are therefore required to collect beneficial owner information. Income trusts are sometimes referred to as publicly-traded flow-through entities because they can flow income and the associated tax liabilities to their investors. These income trusts are registered and regulated by securities exchange commissions.

[169] Although the *Civil Code* in Québec provides for the creation of a "trust", the definition used differs from a common law trust because there is no division of ownership interest.

Prevention of the unlawful use of legal arrangements

1402. There are limited measures in place to prevent the unlawful use of trusts and fiducie in Canada. For instance, there is no system of central registration of trusts and there is no legal requirement for the recording of trusts and for maintaining the trust instrument by the settlor or any other party to the trust. The main situations where a legal obligation arises to maintain relevant information on trusts (i.e information on settlors, trustees, beneficiaries and protectors) are (a) where the trustee is also a "financial entity" such as a trust company under the PCMLTF regulations and (b) where the trust is required to lodge a tax return with the CRA. The examiners noted however that with respect to trust companies, the information requirements under the PCMLTF require the collection of "third party" information. But the term "third party" as defined in those regulations does not extend to cover the full scope of "beneficial owner"as defined in the FATF Recommendations. If a trust receives income, the trust is required to lodge a tax return with the CRA, and the information in that return may contain certain beneficial ownership/control information depending on the nature of the trust in question, but not necessarily.

Access by competent authorities to information on the beneficial ownership and control of legal arrangements

1403. Under certain conditions, trustees on behalf of a trust have to file income tax and information returns with CRA. In these returns, trusts are required to provide specific information on the name of the trust, type of trust, amounts of income and property for tax purposes, including amounts paid or payable to beneficiaries, whether the trust holds foreign property in excess of CAD 100 000 and the name, address and telephone number of trustees, executor, liquidator, or administrator. For the initial return, a trust must attach a copy of the trust document or will, and a list of assets at death (unless filed with the deceased final personal income tax return). The trust document or will contains information on the beneficiaries of the trust.

1404. Throughout the conduct of its investigations, the CRA is bound by the confidentiality provisions outlined within the Income Tax Act and the Excise Tax Act to ensure that tax information is used only for its intended purpose of administering or enforcing the applicable act. However, CRA is able to provide voluntary information reports to FINTRAC on ongoing investigations. These could include information about trusts. However the CRA may only disclose taxpayer information in the case of investigations relating to the administration of the Income Tax Act, the Canada Pension Plan, the Unemployment Insurance Act or the Employment Insurance Act, which then limits its usefulness.

1405. In addition to the information that is proactively disclosed to FINTRAC by federal tax authorities, law enforcement also has the powers to compel production of tax information on trusts held by the CRA in certain circumstances. There are two statutory exceptions that allow the CRA to provide taxpayer information to the RCMP. In both cases, the information being sought must be relevant to the substantive offences being investigated.

1406. First, the CRA will provide tax information to the RCMP where criminal proceedings, either by indictment or on summary conviction, have been commenced by the laying of an information or the preferring of an indictment under an Act of Parliament. Second, the CRA will also provide taxpayer information on trusts to the RCMP pursuant to a judicial order. This section authorises ex parte applications by the RCMP that are supported with a sworn affidavit. The judge must find that the information being sought will be of substantial value to the investigation.

1407. In addition, law enforcement may also approach trustees to ask for the voluntary provision of information on their control, ownership and activities. Law enforcement also has access to powers to compel the production of information from trustees themselves or information about trusts (via production orders or search warrants). There are no specific provisions in trust legislation that protects information from law enforcement apart from the usual confidentiality restrictions that the government imposes upon itself, e.g., the Privacy Act, section 241 of the Income Tax Act or the Personal

Information Protection and Electronic Documents Act for trusts engaged in business activities. Production orders or warrants may also be used by law enforcement to compel the production of information on the formation of a trust from the office of a lawyer that created the trust, provided that the information is not subject to legal professional privilege. Applications of this nature have been very rare. Law enforcement may also conduct interviews with persons connected with the trust as witnesses or suspects.

1408. If additional information from FINTRAC is required, law enforcement may seek a production order against FINTRAC. Law enforcement can obtain information from reporting entities through voluntary cooperation or various court orders described in Section 2.3 of the report (Recommendation 3). However given the fact that the reporting entities do not cover what could potentially be a significant portion of the persons providing trust services (i.e. lawyers and TCSPs), the law enforcement authorities may be handicapped in obtaining leads which can arise from the reporting regimes imposed on reporting entities.

1409. The assessment team believes that the agencies that receive information on legal arrangements (namely the CRA and FINTRAC) have significant limitations on their ability to disclose information. Tax information from certain trusts and law enforcement powers provide the means to access certain information on beneficial ownership and control of certain trusts. However, overall the mechanisms to obtain and have access in a timely manner to beneficial ownership and control of legal arrangements, and in particular the settlor, the trustee, and the beneficiaries of express trusts, are significantly weakened by the lack of legal record-keeping requirements and the limitations on information exchange.

5.2.2 Recommendations and Comments

1410. Canada relies on the investigatory powers of law enforcement to obtain or have access to information concerning the beneficial ownership and control of trusts and fiducie in Québec. These powers are generally sound and widely used. However, the system is only as good as the information that is available to be acquired. In the case of trusts, limited, partial information is available within the jurisdiction, and even where certain information is recorded by agencies such as CRA or FINTRAC, they can only share this information with law enforcement authorities in very limited circumstances, and the information may not be up to date. Canada should implement measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts and fiducie in Québec.

5.2.3 Compliance with Recommendation 34

Rec.	Rating	Summary of factors underlying ratings
Rec.34	PC	• There are limited and indirect legal requirements to obtain, verify, or retain information on the beneficial ownership and control of trusts and fiducie in Québec; • While the investigative powers are generally sound and widely used, there is minimal information that is adequate, accurate and timely concerning the beneficial owners of trusts and fiducie in Québec that can be obtained or accessed by the competent authorities in a timely fashion. Where some information is held, such as by CRA, there are limits on the circumstances in which information on trusts can be shared.

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

General

1411. The NPO sector in Canada is substantial and is comprised of various types of registered charities and corporations in relation to education, health, faith, human rights, social justice, environment, arts and culture, and sports and recreation. There are:

- More than 82 500 registered charities.
- An estimated 63 000 additional NPO corporations operating in Canada.

1412. Registered charities (which receive in excess of USD 5.5 BN annually) represent a significant portion of the financial resources of the NPO sector accounting for approximately 68% of all revenues and 95% of all donations. In addition, they account for a substantial share of the sector's foreign activities: 75% of international organisations in Canada are registered charities. In 2004, over 22 million Canadians made a financial donation to a charitable or other non-profit organisation.

Review of the non-profit sector

1413. Canada has conducted several reviews of the NPO sector, and the potential risks of terrorist financing. First, in 1999 the Senate examined "the international threat environment with particular reference to terrorism as it relates to Canada", including the issue of fundraising and it found that registered charities in Canada were particularly susceptible to abuse in this regard because of the credibility and deniability such status affords. Second, an inter-departmental group reviewed the adequacy of its laws and regulations as they relate to non-profit organizations in considering its anti-terrorism legislation. Lastly, in 2004 a five-year Regulatory Reform Action Plan for the Charities Directorate was announced based on the result of a comprehensive review of the regulatory framework for the non-profit sector in Canada undertaken as a joint voluntary sector and government initiative.

1414. In September 2004 Canada reviewed the adequacy of its laws and regulations in relation to risks of terrorist financing posed within the NPO sector as part of its obligations to the FATF. A report entitled "*A Review of the Canadian Non-Profit Organisation Sector* (A Discussion Paper for the FATF Working Group on Terrorist Financing)" was presented to the FATF WGTYP the following year.

Charitable registration

1415. All charities are required to apply to the CRA for registration and abide by the provisions of the Income Tax Act (IT*A). Charities that fail to meet these legal requirement*s can be de-registered. To qualify for charitable registration, an organisation must be established for charitable purposes and devote its resources to charitable activities. The charity must also be resident in Canada and cannot use its income for the benefit of its members. There are four kinds of recognised charitable purposes: relieving poverty, advancing education, advancing religion and providing certain other community benefits (including, homes for the elderly, hospitals, disaster relief efforts). To qualify for registration a charity must meet a "public benefit" test. An organisation must show that its activities and purposes are legal and (1) provide a tangible benefit to the public, (2) benefit the public or a significant portion of the public, and (3) do not serve a political purpose.

1416. A registered charity can be one of three entities: (1) a charitable organisation (which comprise 90% of registered charities), (2) a public foundation (which comprise 5% of the charities and generally funds the charitable activities of other charities), or (3) a private foundation (comprising the remaining 5% controlled by a group of related persons which can carry out charitable activities or fund the charitable activities of others).

1417. An organisation will not be registered under the Income Tax Act (or its existing registration will be revoked) when there are reasonable grounds to believe it is connected to terrorism. Most often, the regular rules and procedures under the Income Tax Act can be used to deny or revoke registration. To assist in cases where highly classified information must be used to substantiate a charity's links to terrorism, the Charities Registration (Security Information) Act was enacted as part of the Anti-terrorism Act. This legislation establishes a ministerial process whereby sensitive information can be used to determine whether to deny (or revoke) a charitable registration. In reviewing new applications and existing registered charities, the CRA requests information from the RCMP and CSIS when there are concerns an organization may be connected to terrorism.

Supervision, monitoring and data collection

1418. At the federal level, law enforcement and intelligence agencies monitor and investigate charities suspected of providing support for terrorist activities. In addition, the CRA closely monitors registered charities. Organisations seeking registration are required to apply to the CRA's Charities Directorate. Applicants use a standard form, which requires them to provide the organisation's current legal name, a list of the directors or trustees, key financial data and a detailed description of the organisation's programs. This description includes the location of the activities, the identity of the intended beneficiaries and the mechanisms to ensure that the organisation retains control of its resources. Applicants must also include copies of the governing documents under which they operate, such as certificates of incorporation or organisational by-laws.

1419. The Charities Directorate's compliance program is largely based on information from the annual returns, internal analysis of trends in the charitable sector, complaints from the public and tips from informants. The CRA is also authorised by statute to release certain other information regarding registered charities to the public. This includes: (1) the organization's governing documents and other prescribed information provided on applying for registration; (2) the notification of registration issued by the CRA; (3)the names of the persons who at any time were the charity's directors; and (4) any notice of the grounds for revocation of registration issued by the CRA. Certain other information, such as the addresses of trustees and directors, is reported to the CRA but remains subject to confidentiality rules

1420. These supervisory mechanisms appear to be effective for charities even though limited to the latter (and not applicable to other non profit organisations). Existing corporation law mechanisms under the Canada Corporations Act, which are administered or maintained by Industry Canada are utilized such as a mandatory submission of specific corporation information and requirements that compel corporations to maintain corporation records and financial reports available for inspection. If potentially illegal activities are detected by Industry Canada, it is standard practice to refer these matters to law enforcement. Canadian provinces generally have reporting and supervision mechanisms of a similar nature under their corporation laws.

1421. Canada also has a number of "umbrella organizations" that provide guidance and varying degrees of oversight such as the Canadian Council of Christian Charities which offers its members a certification program. Charities, which participate in this program, can display a special "seal of approval". Certification requires that the member organization has an independent board, audited financial statements, and that it has adopted the Council's "Code of Ethical Fundraising and Financial Accountability".

1422. Similarly, the Canadian Centre for Philanthropy encourages its members to adopt its "Ethical Fundraising and Financial Accountability Code". The 500 charities that have adopted this Code are committed to responsibly managing the funds that they receive and reporting their financial affairs accurately and comprehensively. The Association of Fundraising Professionals also encourages its members to adopt a code of ethics, a donor's bill of rights and put in place a mechanism to register complaints. Other charitable organizations with chapters or branches in Canada also play an important role in ensuring that high standards of accountability are observed by their affiliates.

1423. The specialized supervisory and monitoring measures under the CRSIA do not apply to the other parts of the NPO sector. This sector is estimated to be almost of comparable size to the registered charities sector, but the Canadian risk reviews suggest that it is far less significant in terms of risk profile. There is acknowledged coverage as regards outreach and data collection (insofar as the CRA does obtain substantial information as regards the operations of NPOs). However, if an entity does not register under the ITA, then there are no similar supervisory measures.

Sanctions

1424. The ITA provides CRA with the ability to apply a range of interim sanctions against registered charities that are non-compliant. These include financial penalties and/or the temporary suspension of certain privileges such as the ability to issue tax receipts. The scope of activities that can be subject to sanctions range from, but are not limited to, certain business activities, unjustly enriching principals of the organization, gifting resources to non-eligible recipients and furnishing false statements with respect to tax receipts. The severity of the penalty increases with subsequent infractions and may ultimately lead to revocation.

1425. Out of a pool of 82 500, about 2 000 charities have their registrations revoked each year. These are mostly organizations that have ceased operations or have failed to file annual returns. CRA conducts comprehensive field audits of about 800 registered charities each year. Recent experience suggests that, on average, about 10 charities a year lose their registrations as a result of serious non-compliance issues, including dubious fund-raising schemes, political activities, lack of proper books and records, and improper personal benefit. In addition, registered charities that have failed to demonstrate sufficient control over their foreign operations have been de-registered.

1426. Under the CRSIA, a special mechanism has been established to deny an organization's application for registration (or revoke its existing registration) when terrorist connections are suspected. As outlined above, the CRSIA establishes a ministerial process whereby sensitive information can be used to determine whether to deny (or revoke) charitable registration.

Record keeping requirements

1427. In the process of applying for registered status, a charity must provide key financial data to the CRA, including information on the mechanisms to ensure that the organization retains control of its resources. Once registered, a charity must annually provide the CRA with a copy of its financial statements and a return providing information on its board of directors, its sources of revenue, its types of expenditures and its general operations. A charity is required to maintain such records for a period of six years from the date of the last taxation year to which they relate. A revocation of a charity's registration could take place where the record keeping requirements are not met.

Information gathering and domestic co-operation

1428. Cooperation exists between law enforcement and intelligence and security agencies and other key agencies including the CRA, CSIS, RCMP and FINTRAC.

1429. Departments and agencies share information and cooperate in the charitable registration process. In reviewing new applications and assessing compliance, the CRA is able to obtain information held by the RCMP and CSIS that may reveal an organization's ties to terrorist groups.

1430. As part of the CRA, the Charities Directorate is subject to the Income Tax Act's stringent provisions on the confidentiality of taxpayer information. However, the ITA does permit the Directorate to share its information when such disclosures can reasonably be regarded as necessary to

enforce the ITA or the Charitable Registration (Security Information) Act[170]. The CRA can share information about a registered charity or an organization that has applied for such status with law enforcement and intelligence agencies where there are reasonable grounds to suspect that information held by the CRA might be relevant to the investigation of a terrorism offence under the Criminal Code or to threats to the security of Canada[171].

1431. The measures implemented by the CRSIA relate to the reliance on security information with regards to a decision whether to permit an entity to be registered or continue to be registered as a charity. There is no automatic trigger between the decision to issue a certificate under the CRSIA and the process leading to listing and/or freezing procedures. However, the measures implemented by CRSIA are supported by formal liaison agreements between the CRA and authorities responsible for conducting investigations which lead to the commencement of listing and/or freezing procedures (*i.e.* the RCMP and CSIS) and CRA information that is shared for purposes of CRSIA may be used to further investigations that could lead to commencing such procedures.

Access to information

1432. During the course of TF investigations, the RCMP will access the publicly available information as provided by the Canadian government registries and/or regulatory bodies and any additional information that can permissibly be obtained from the CRA. It may also seek information directly from the entity or individual under suspicion using existing law enforcement powers. The RCMP must abide by legislation that dictates the legal process, *i.e.* obtain search warrant or production order, under which information pertinent to a criminal investigation may be obtained. Through these methods, law enforcement is able to access all available information on the administration and management of an NPO in the course of an investigation.

1433. Under section 462.7 of the Criminal Code, and subject to section 241 of the Income Tax Act any person may make a disclosure to the Attorney General or a peace officer where a reasonable suspicion exists that property is the proceeds of crime or that the person has committed or is about to commit a designated offence. Section 241 of the Income Tax Act also provides an avenue for the law enforcement authorities to obtain information from the CRA where it is proven that a terrorism offence is being investigated is underway and that the information sought is likely to be of substantial value to the investigation.

Sharing of information

1434. Intelligence agencies have expertise and capability to examine NPOs that are suspected either being exploited by or actively supporting terrorist activity or terrorist organizations. CSIS investigates NPOs as part of their terrorist investigations and will disclose information to the police or other jurisdiction in the same manner as for any other investigations. Additionally, the CSIS Financial Analysis Unit works closely with the Charities Directorate of CRA in reviewing renewals and applications for charitable status. This unit, as the primary contact, conducts the research related to the requests and formulates the response on behalf of the CSIS.

1435. FINTRAC conducts analysis of the information it receives from reporting entities and other government departments and has made disclosures that have included information about the suspicious activities of NPOs. As of July 2005, FINTRAC had made over 120 case disclosures of suspected terrorist activity financing and other threats to the security of Canada. NPOs, both foreign and domestic, have figured in over one-third of the case disclosures related to suspected terrorist activity financing, with slightly more Canadian NPOs represented in these disclosures than foreign ones.

---

[170] To assist in the administration and enforcement of the CRSIA, an amendment has been made to the PCMLTFA to allow FINTRAC to disclose information to the CRA on suspected cases of terrorist financing involving charities.

[171] Amendments to section 241 of the Income Tax Act brought in force on February 10, 2007.

FINTRAC is however currently unable to make disclosures to the CRA and may only disclose a limited amount of information (see comments on "designated information" in Section 2.5 of the report).

1436. The CRA is constrained under section 241 of the Income Tax Act as regards the circumstances in which it can voluntarily share taxpayer information though there are a number of exceptions to the general rule that confidentiality must be maintained. One such exception is set out in s.241(3.2) which allows the disclosure to any person of certain information related to registered charities such as governing documents, names of directors, financial statements etc. Other information on registered charities or on other tax payers, including other NPOs, can be disclosed as part of criminal proceedings that have commenced (s.241(3)). Equally, defined classes of information relating to registered charities and any other NPO that has sought registration (though not all taxpayer information) can be shared with law enforcement, intelligence agencies and FINTRAC for purposes of investigating terrorism (including terrorist financing) in prescribed circumstances *i.e.* reasonable grounds to suspect the information would be relevant to an investigation of whether a terrorism (including TF) offence may have been committed (s.241(9)). In addition, under s.241(9.1) any information about a registered charity or an NPO that has applied for such status (other than individual Canadian donors information) which the CRA has provided to CSIS or the RCMP for purposes of administering or enforcing the CRSIA can also be used by those agencies for purposes of investigating terrorism. Finally, s.241 allows the release of all taxpayer information, without any restriction, pursuant to a court order or CSIS warrant.

1437. The assessment team believes that the CRA maintains an extensive information collection regime for all NPOs for taxation purposes. The team notes that a broader amount of information can be shared with respect to registered charities and NPOs that have sought registration than other types of taxpayers (including other NPOs). However, except in cases where it is acting under the authority of a court order or a CSIS warrant, the CRA can only share a broad class of tax payer information relating to all NPO with law enforcement when criminal proceedings have commenced, and a more limited class of information with FINTRAC when the requirements of s.241(9) are met. The requirements of s.241 thus impose some limitations on the type of information to be obtained, or the circumstances in which it can be obtained by FINTRAC or law enforcement, which may limit the investigative value of the information..

International requests

1438. Formal and informal mechanisms are used to provide and receive international information regarding the terrorist-support activity in the NPO sector. These are the same channels that are used by law enforcement, intelligence organizations and judicial authorities to share information on terrorist financing and money laundering activities (see Section 6.5 of the report).

Law Enforcement Cooperation

1439. Police forces in Canada regularly provide informal assistance to police forces from other countries. Generally, police are able to provide information or documentation that is publicly available or which may be obtained on a voluntary basis. This usually involves direct communication between police forces and may include transmission of information through Interpol.

Cooperation between Financial Intelligence Units

1440. For its part, FINTRAC also can exchange information relevant to the investigation or prosecution of a money laundering or terrorist financing offence involving non-profit organizations with international counterparts. To provide information, however, FINTRAC must have a memorandum of understanding with the counterpart FIU, which governs how the information will be used and protected. Further information about FINTRAC and its information sharing agreements are available in Sections 2.5 and 6.5.

Judicial Cooperation

1441. The International Assistance Group (IAG) of the Department of Justice is the focal point where all Mutual Legal Assistance Treaties (MLATs) requests are processed. The IAG has received MLAT requests for information related to NPOs suspected of terrorist financing or other forms of terrorist support. The IAG has applied the same process as for any other MLAT requests. The process is explained in Section 6.3 of the report.

5.3.2 Recommendations and Comments

1442. Canada has taken considerable steps to implement SR VIII in relation to registered charities, which it considers to be the sector most at risk, based on the risk assessment studies it has done. A large segment of the NPO population is not covered by the current measures using the risk based approach, but Canada should continue to monitor the risks in these other sectors. Canada should improve the existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications. Again, Canada should review the capacity of CRA and FINTRAC to share information with law enforcement authorities related to the non-profit sector.

5.3.3 Compliance with Special Recommendation VIII

Rec.	Rating	Summary of factors underlying ratings
SR.VIII	LC	• The existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications is insufficient to fully address the risk in some segments of the NPO sector.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and coordination (R.31 & 32)

6.1.1 Description and Analysis

Recommendation 31

1443. The lead for policy and coordination in the AML/CFT area rests with the Department of Finance. The Department of Public Safety and Emergency Preparedness (PSEPC) takes a lead role in coordinating the Government of Canada's response and activities related to terrorist listings.

1444. Canada has developed several structures which are aimed at ensuring proper coordination in AML/CFT matters.

Department of Finance Committee Structures

1445. *Interdepartmental Assistant Deputy Minister (ADM) Steering Committee (ISC) and Working Group*. The ADM Steering Committee has representation from the key departments and agencies within the federal AML/CFT regime – FINTRAC, OSFI, PSEPC, RCMP, CSIS, CBSA, CRA, and the Department of Justice. The ISC meets a minimum of twice a year and serves as a forum for the discussion of policy and operational issues relative to the regime. This ADM Steering committee also serves as a forum for a high level assessment of the effectiveness of the regime and discussion of issues of strategic importance. In addition, there is a working level group that undertakes activities as directed by the committee through regular meetings (about 10 times annually), as required. This working level committee's work includes the development of new policy, legislative and regulatory proposals, the co-ordination of audits and evaluations of the effectiveness the regime, discussion of funding pressures and operational challenges among the partners and their potential impact on results.

1446. *Informal Group*. The Department of Finance originally established the Informal Group in 2002 to facilitate an integrated federal/provincial response to events in financial markets related to investor confidence. Some of the more recent issues that the Informal Group has dealt with include enforcement issues in capital markets, challenges posed by hedge funds and enhancements to Canada's AML/CFT regime.

1447. *Heads of Agencies*. The Governor of the Bank of Canada chairs the Heads of Agencies group, which meets three to four times each year. The group brings together regulators, such as OSFI and the chairs of the provincial securities commissions, as well as the Department of Finance, to exchange information regarding financial market regulatory developments.

1448. *Federal-Provincial-Territorial Financial Sector Policy Officials Meetings*. The Department of Finance chairs meetings of federal, provincial and territorial financial sector policy officials twice each year. The range of issues discussed is very broad and evolves with current developments. Although these meetings are generally focused on information sharing, they also serve to identify areas where coordinated intergovernmental action is required.

PSEPC Committee - Interdepartmental Coordinating Committee (ICC)

1449. The ICC is a working level group created in 2001, to address operational and administrative issues relating to the listing of terrorist entities pursuant to Security Council Resolutions 1267 and 1373, as well as under the Criminal Code. It is currently chaired by the Counter Terrorism Policy and Coordination Division within PSEPC and is attended by representatives of the Department of Finance, RCMP, CSIS, OSFI and DFAIT. The ICC meets on a monthly basis or as needed. The committee provides a forum for departments and agencies to assess operational challenges and requirements to implement the listing regime and the efficiency and effectiveness of that regime.

1450.

Department of Justice Prosecution Coordination Structure

1451. The new Public Prosecution Service of Canada (PPSC) assumes carriage and control of all prosecution functions previously undertaken by the Federal Prosecution Services and the PPSC is tasked with all of the consultation and coordination responsibilities previously undertaken by the Federal Prosecution Service. The PPSC continues the three times a year coordination meeting with the heads of prosecutions in the provinces. In the area of money laundering and proceeds of crime, there are two committees that have been created. The National Liaison Committee, comprised of money laundering prosecutors, meets yearly or more frequently to coordinate common issues relevant to money laundering prosecutions. The second committee is the Coordinating Committee of Senior Officials (CCSO) on Proceeds of Crime. It is also comprised of money laundering prosecutors and criminal law policy lawyers and reports to the Justice Deputy Ministers Committee (Federal, Provincial and Territorial). The PPSC is also a partner in a national memorandum of understanding with the RCMP for the IPOC.

Additional Co-ordination Initiatives

1452. *Canada Drug Strategy (CDS).* The CDS aims to strike a balanced, integrated approach to reducing both the demand for and the supply of drugs through integrated efforts of a number of federal organizations including the RCMP, Correctional Service of Canada, CBSA, Department of Justice, Drug Treatment Courts, Federal Prosecution Service, Foreign Affairs Canada. The programme of work includes law enforcement activities aimed at disrupting activities surrounding the production and supply of illicit substances, as well as substance abuse programs for Federal inmates.

1453. *First Nations Organized Crime Initiative (FNOC).* The First Nations Organized Crime Initiative assists First Nations police services in addressing organized crime and cross-border criminality. It enables sustained participation in multi-agency law enforcement activities. Furthermore, it provides training and opportunities for intelligence gathering and sharing.

1454. *Integrated Border Enforcement Teams (IBETs).* Established after September 11, 2001, the Integrated Border Enforcement Team (IBET) program is an intelligence-led cooperative that supports national security investigations associated to the Canada/US border and investigates cross-border illegal activities, between the Ports of Entry (POE). The RCMP and the Canadian Border Services Agency work with U.S. Customs and Border Protection, the US Bureau of Immigration and Customs Enforcement, and the US Coast Guard to share information and work together daily with other local, state and provincial enforcement agencies on issues relating to national security, organized crime and other criminality transiting the Canada/US border between the POE.

1455. Integrated Proceeds of Crime Initiative (IPOC). See description in Section 2.6 of the report.

1456. *National Coordinating Committee on Organized Crime (NCC).* The NCC, a body composed of federal, provincial and territorial (FPT) government senior officials, prosecutors, and representatives from the law enforcement community, identifies key issues for action and develops national strategies and initiatives to address them. The NCC has three main responsibilities: (1) to identify issues and policy priorities related to the problem of organized crime; (2) to advise FPT Deputy Ministers on the development, coordination and implementation of policies, legislation and programs aimed at combating organized crime; and (3) to encourage coordination of anti-organized crime activities among various players at the regional and local level.

1457. *Governance of Initiatives*. Initiatives such as FNOC, IBET, IMET, IPOC and NCC operate under a similar governance structure, with both a Partners Advisory Committee and a Senior Governance Committee. The Partners Advisory Committee is composed of representatives from each of the partner organizations at the Director and Senior Analyst levels. These committees meet several times a year or more frequently to address urgent issues. These working groups focus on a myriad of issues, including communications, research, evaluation and risk management and emerging issues, and have been established to support decision-making by the ADM Steering Committee.

Additional elements

1458. Finance is the primary lead in terms of consultations with stakeholders, and has a close working relationship with industry regulators and associations that represent the reporting entities. Finance also maintains a list of stakeholders to ensure that they are adequately consulted and informed of any new legislative and regulatory changes. A recent example is the release of Finance's consultation paper, "Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime" in June 2005, which led to over 50 written submissions and nine months of face-to-face consultations with stakeholders throughout the country. These consultations played a significant role in the drafting of the new legislation that was passed in December 2006, and the resulting changes to regulations and industry guidance. FINTRAC and OSFI, in particular, play an essential role with the Department of Finance, in liaising with the private sector to ensure their commitment to and compliance with the AML/CFT regime.

1459. Further, law enforcement maintains its own contacts with the private sector in order to ensure a supportive environment. There is an ongoing dialogue with the Canadian Bankers Association and with specific large banks.

1460. *AML/CFT Advisory Committee (AC).* One of the recommendations coming from domestic assessments of the Canadian regime was the creation of a new AML/CFT Advisory Committee. The AC had its first meeting in November 2007[172].

[172] With the aim of increasing outreach, cooperation and coordination, the new Advisory Committee comprises both public and private sector representatives. The AC consists of members of the key departments and agencies, in addition to representatives from each sector of the reporting entities. It is chaired by the Department of Finance and has high-level representation from approximately 30 members.

1461. Federal partners interact regularly with each other and with external stakeholders in relation to AML/CFT issues. The federal partners primarily use the interdepartmental working group led by the Department of Finance. The group meets regularly and, although no minutes of the meetings are kept, participants acknowledge that it provides an effective means of discussing common issues. However, at more operational level, the assessment team found signs of friction, especially between FINTRAC and the law enforcement authorities. Some signs of reluctance to share information remain which has an impact on the effectiveness of the implementation of the AML/CFT regime.

Recommendation 32

1462. Canada reviews quite extensively the effectiveness of the AML/CFT system on a regular basis and through different authorities and bodies.

1463. Canada's system of government has numerous means by which to ensure that its policies and programs are effectively meeting their intended goals, and Canada's anti-money laundering and counter-terrorist financing regime has been subjected to these checks and audits. This included an in-depth audit by the Office of the Auditor General[173], an independent government agency that ensures that government programs are effectively using public funds for their intended purpose. The AML/CFT regime has also been evaluated by a private research group[174] as a condition for a renewal of funds by the Treasury Board. Lastly, as stipulated under the PCMLTFA, the regime s recently underwent a five year review by a committee of the Senate[175] to review administrative and operational effectiveness and efficiency since the legislation was originally passed. Section 72(1) of the consolidated legislation mandates that such a review take place every five years by a committee of the House of Commons, of the Senate, or of both Houses.

1464. In the first review, the results of the 2004 OAG report were favourable. However, the auditors highlighted three areas for further consideration:

- The PCMLTFA limits the information that FINTRAC can disclose to law enforcement and security agencies as a result of Charter and privacy rights. This inhibits to some degree the usefulness of disclosures in generating new investigations.
- The partners involved in the initiative could enhance coordination through the introduction of an overarching advisory committee to discuss issues of common interest and develop approaches for dealing with emerging issues.
- Accountability mechanisms to monitor the impact and usefulness of the intelligence that FINTRAC provides law enforcement and security agencies could be enhanced.

1465. Overall, the AML/CFT system was viewed positively by EKOS that made the following key recommendations:

- Reporting entities require feedback from FINTRAC concerning the impact of their reports.
- Additional funding should be allocated to meet specific needs, such as IT renewal at FINTRAC and expansion of investigation capacities for the RCMP and CBSA.
- Information in FINTRAC disclosures could be expanded to increase the value to law enforcement and security agencies.

---

173 "Observations and Recommendations." Chapter 2 – Implementation of the National Initiative to Combat Money Laundering. 2004 Report of the Auditor General of Canada at: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20041102ce.html.

174 "Year Five Evaluation of the National Initiative to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing. Final Report" EKOS Research Associates Inc. November 30, 2004. p. iv.

175 "Stemming the Flow of Illicit Money: A Priority for Canada." Parliamentary Review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Standing Senate Committee on Banking, Trade and Commerce. October 2006. p. 27.

- Updating the logic model and evaluation framework should be undertaken, among other things, to ensure outcomes and cost effectiveness of the program.

1466. The Senate Committee tabled a report, "Stemming the Flow of Illicit Money: A Priority for Canada", on October 5, 2006, which highlighted the need for the AML/CFT regime to meet domestic requirements, but also the importance of meeting international obligations in order to ensure that the world is "safer and more secure". The review was conducted with the understanding that there were proposed legislative changes underway stemming from a consultation paper released by the Department of Finance in June 2005. Recommendations and the Government's response included:

- Creating a registration system for money service businesses.
- Require dealers of precious metals and stones to report suspicious transactions and other prescribed reports to FINTRAC.
- Require customer identification in non-face-to-face transactions.
- Use a risk-based approach to determine the level of client-identification and record keeping for reporting entities.
- Oblige lawyers to follow client-identification, record keeping and reporting requirements, while still respecting solicitor-client privilege, the Canadian Charter of Rights and Freedoms, and the Quebec Charter of Human Rights and Freedoms.
- Enable FINTRAC to disclose to law enforcement and intelligence agencies the rationale for the disclosure and any other publicly available information.
- Determine the likelihood and extent of money laundering and terrorist financing activities that could be taking place with emerging modes of financial services delivery, like white label ATMs and Internet banking.
- Require feedback from law enforcement and security agencies to FINTRAC on the value of their disclosures. As well, FINTRAC should provide feedback to reporting entities on the usefulness of their reports in the fight against money laundering and terrorist financing.
- Require the reporting of suspicious attempted transactions.
- Examine whether the reporting threshold of CAD 10 000 is appropriate to activities in Canada and consistent with other countries.
- Ensure that FINTRAC is adequately funded to carry out its mandate under the PCMLTFA.
- Ensure that the RCMP has the required financial resources and expertise to investigate cases of money laundering and terrorist financing.
- Ensure appropriate oversight of FINTRAC.

1467. In response to these evaluations, the responsible government departments and agencies have been working to ensure that the recommendations made in each of these three evaluations were followed-up and that the appropriate changes to the regime were made.

1468. Canada's AML/CTF regime will be subject to a further third party evaluation in fiscal year 2009-2010 in order to secure continued funding. Similarly, Treasury Board also recommended, following the 2006 increase in funding for FINTRAC, the RCMP, CBSA and the Department of Justice in Budget 2006, that the evaluation framework be re-assessed to see if it is capturing the results of the regime appropriately. This new evaluation framework must be completed by October 2007. In addition, an assessment of the impacts of data collection and disclosures provided under Canada's AML/CFT regime on Canadians' privacy will be conducted.

6.1.2 Recommendations and Comments

1469. Canada has developed quite a large number of initiatives to improve co-operation mechanisms among the different stakeholders taking part in the fight against money laundering and terrorist financing. However, from the discussions that took place during the on-site visit, the assessment team believes that interagency cooperation between the FIU and law enforcement authorities is not fully effective and needs to be enhanced, in order to optimise Canada's capacity to investigate ML and TF

cases. Canada should consider encouraging more bilateral (ad-hoc and more formalised) contacts among agencies.

1470. The assessment team welcome the setting up of an AML/CFT Advisory Committee that allows private and public stakeholders to discuss emerging AML/CFT issues and support implementing the existing standards. It is important that private sector and provincial stakeholders are fully involved in the consultation process, including regional and provincial organisations that have important connections with practitioners in their respective sectors.

6.1.3 Compliance with Recommendation 31

Rec.	Rating	Summary of factors underlying ratings
Rec.31	LC	• Interagency cooperation between the FIU and law enforcement authorities is not fully effective and needs to be enhanced.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

Ratification and implementation of conventions

1471. Canada signed the Vienna Convention on December 20, 1988, and ratified the Convention on July 5, 1990. Canada signed the Palermo Convention on December 14, 2000 and ratified the Convention and its Protocols on May 13, 2002. Canada signed the United Nations International Convention for the Suppression of the Financing of Terrorism on February 10, 2000, and ratified the Convention on February 19, 2002.

1472. The provisions of the Palermo and Vienna Conventions relating to the ML offence have been almost entirely implemented; however there are two small deficiencies, the ML offence does not cover all designated categories of predicate offences/all indictable offences since Canada has a threshold approach to criminalising money laundering (including indictable offences such as offences under the Copyright Act which carry a penalty of up to 5 years imprisonment). Also, Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions or Recommendation 1 (see conclusions in Section 2.1). Most of the provisions of the CFT Convention have also been fully implemented. However, Article 18(1)(b) of the Terrorist Financing Convention requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 currently does not include adequate measures to ascertain the identity of beneficial owners through CDD procedures (see discussion in relation to Recommendation 5)[176].

Implementation of the U.N. Security Council Resolutions

1473. Canada implemented UNSCR 1267 (1999) by adopting the United Nations Afghanistan Regulations in November 1999. These regulations, which were renamed the United Nation Al - Qaida and Taliban Regulations in June 2006, incorporate by reference the list of individuals and entities maintained by the 1267 Committee for the purpose of freezing, seizing or confiscating the funds or assets owned or controlled by those listed individuals and entities. They also implement successor resolutions 1333, 1390, 1452, 1526 and 1617. Canada implemented UNSCR 1373 (2001) in October 2001, with the adoption of the Canadian UN Suppression of Terrorism Regulations, which in 2006 were renamed the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.

[176] Canada indicated that shortfalls have been addressed in regulations enacted in June 2007 and coming into force on 23 June 2008. Such regulations have not been assessed by the assessors.

1474. Canada has fully implemented S/RES/1267(199) and its successor resolutions as well as UNSCR 1373(2001).

Additional elements

1475. Canada ratified the Inter-American Convention against Terrorism on December 2, 2002. It appears Canada has implemented the 2002 Inter-American Convention against Terrorism, with the possible exception of Article 4(b) of that Convention.

6.2.2 Recommendations and Comments

1476. Canada should ensure that the ML offence does cover all designated categories of predicate offences and Canada should consider removing the purpose element from Section 462.31 of the CC to be in line with the UN Conventions (see Section 2.1 of the report). Canada should enact stronger measures to customer identification so as to be more compliant with Article 18(1)(b) of the CFT Convention[177].

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

Rec.	Rating	Summary of factors underlying ratings
Rec.35	LC	*Implementation of the Palermo and Vienna Conventions:* • Canada has ratified the Palermo and Vienna Conventions and implemented them with some omissions however (the ML offence does not cover all required categories of predicate offences and Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions); *Implementation of the CFT Convention:* • Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.
SR.I	LC	*Implementation of the CFT Convention:* • Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.

6.3 Mutual Legal Assistance (R.36-38, SR.V, R.30 & 32)

6.3.1 Description and Analysis

Recommendation 36 & Special Recommendation V

Scope of assistance allowed

1477. Canada has extensive formal and limited informal means of providing mutual legal assistance (MLA) to requesting countries. Canadian police, directly or through Interpol, can provide assistance on the basis of a simple request but only where the evidence or information can be obtained without a court order. However, since 2006, the RCMP is more restricted in both the amount and type of informal information they can provide to foreign law enforcement partners without formal arrangements. Often, this forces the requesting law enforcement partners to resort to the much slower

[177] Canada indicated that shortfalls have been addressed in regulations enacted in June 2007 and coming into force on 23 June 2008. Such regulations have not been assessed by the assessors.

and more cumbersome formal legal assistance processes. This may over-burden the formal MLA process.

1478. Where the evidence can only be gathered pursuant to a court order, Canada's Mutual Legal Assistance in Criminal Matters Act ("MLACMA" or "the Act") is the domestic legislation that enables a Canadian court to issue orders compelling the production or authorizing the seizure of evidence at the request of a treaty partner. Canada is a party to 34 bilateral mutual legal assistance treaties, and as mentioned previously in Section 6.2.1 of the MER, Canada is also a party to multilateral treaties such as the Vienna, Palermo and Terrorist Financing Conventions.

1479. Under the MLACMA, the following mechanisms can be used to obtain evidence in compliance with Recommendation 36 (Criterion 36.1 (a) through (f)): search warrants; productions orders (typically used to compel production of evidence from disinterested third-parties such as banks, phone companies and other telecommunications service providers and to compel statements); any other warrant available under Canada's Criminal Code (such as a warrant for a number recorder on a telephone line); video or audio-link of a witness in Canada to proceedings in a foreign jurisdiction; an order for the lending of exhibits which have been tendered in Canadian court proceedings; an order for the examination of a place or site in Canada; the transfer of a sentenced prisoner (with his or her consent) to testify or assist in an investigation; service of documents; the enforcement of orders made by a court of criminal jurisdiction for the restraint, seizure or forfeiture of property situated in Canada; enforcement of foreign criminal fines; and enforcement of foreign criminal restraint and forfeiture orders.

1480. Canadian courts can also issue compulsory process for the evidence of witnesses and the production of documents in response to a request from a court in the foreign state via the letters rogatory process, but in such cases Canada cannot use the other compulsory means that are available to Treaty partners under the MLACMA.

1481. The tools most commonly used to obtain evidence on behalf of a requesting state are evidence gathering orders and search warrants. In order for a Canadian judge to issue a MLACMA search warrant or evidence gathering order, he or she must be satisfied that there are reasonable grounds to believe that "an offence under the foreign law has been committed" and that evidence of the commission of the offence will be found in Canada. The request for assistance must provide sufficient information to satisfy the judge on these two points. However, while treaty parties have access to the full slate of Canadian law enforcement tools to seek information and evidence, obtaining such orders appears, in practice, to be quite burdensome. To obtain simple production orders, in addition to the usual content required for executable MLA requests, the requesting state must provide Canada both a detailed explanation as to why it believes any evidence is located in Canada, and how such evidence will be relevant to proving elements of the foreign criminal case.

1482. Canada has a centrally-coordinated MLA regime involving: the Department of Justice which acts as a gatekeeper; Crown prosecutors who present the requests to Canadian Courts for execution; the Judiciary, and, on occasion, law enforcement agents who execute the Canadian court's compulsory orders. The MLACMA includes extensive judicial oversight of the process of collecting evidence for foreign governments. For example, no evidence that was obtained through compulsory orders obtained under MLACMA may be sent to a requesting state without judicial authorisation. The Department of Justice, while charged with guiding MLA requests through the MLA process, has very little control over the speed with which the MLA process is completed and has to rely upon the diligence of prosecutors, and the expectation that judges appreciate that timely responses to MLA requests are central to international criminal assistance. Undue delays in responding to MLA requests can hinder the ability of the requesting authorities to bring an accused to trial, given the short legal deadlines that often exist. This, in part, may explain the high number of abandoned requests in Canada's MLA regime.

1483. Canada can respond to a letters rogatory request from a foreign court addressed to a court in Canada. Assuming the letter rogatory contains sufficient information, counsel with the Department of Justice will bring an application before a Superior Court in Canada under the Canada Evidence Act for an order compelling the testimony of a witness or for the production of documents.

1484. Canada will also provide what assistance it can in response to a non-treaty letter of request. However, the scope of such assistance is limited to what can be provided without a court order since the evidence gathering powers in the MLACMA are available only to treaty partners and designated entities.

Conditions for refusal

1485. Where assistance is provided pursuant to a Treaty, the treaty itself restricts the use that can be made of the evidence concerning the matters set out in the letter of request. Where evidence has been gathered in Canada on behalf of a requesting state under the MLACMA, before the evidence can be sent to the requesting state, a judge must, by order, authorise the transmittal of the evidence. Affected parties may ask the judge to impose conditions on the sending of the evidence to the requesting state. In the majority of cases, sending orders are unconditional. In the few instances where a judge does impose conditions on the sending of the evidence, they are usually restricted to protecting the interests of those from whom evidence has been obtained. In this regard, a typical condition would be that the evidence be returned at the conclusion of all proceedings in the requesting state.

1486. Canada does not require that there be judicial proceedings underway in order to provide legal assistance. The exception is in cases where assistance is provided pursuant to a letters rogatory request and where a treaty request is made for the enforcement of foreign orders for restraint, seizure and forfeiture. In order for a letters rogatory request to be executed, there must be a matter pending before the court in the foreign jurisdiction, and therefore pre-trial investigatory assistance would not be available in the absence of a treaty. In the case of requests for the enforcement of foreign orders of restraint or seizure, the person must be charged with an offence which is also an indictable offence in Canada. In the case of requests for enforcement of a forfeiture order, the person must have been convicted of an offence which would be an indictable offence in Canada, if it had occurred in Canada. This latter situation is the only instance where Canada requires evidence of a conviction in order to provide assistance.

1487. Except in the case of requests for the enforcement of foreign orders of restraint, seizure and forfeiture, Canada does not require dual criminality in order to provide assistance and does not seek to include dual criminality as a requirement in the mutual legal assistance treaties that it negotiates. The analysis of whether dual criminality is established is conduct-based. That is, if the conduct is criminalized in both countries, it will be concluded that this criterion is satisfied, whether or not the denomination or the precise constituent elements of the respective offences are identical.

1488. Canada's MLATs typically contain a provision allowing for the refusal of a request for mutual assistance on the basis that it would be contrary to Canada's public interest to execute the request. Canada may use this provision to delay the execution of a request if execution would compromise a Canadian investigation.

1489. *Fiscal matters.* Canada does not impose a restriction on mutual legal assistance in criminal matters requests in Canada on the sole ground that the offence is also considered to involve fiscal matters. The MLACMA does not contain any reference to such limitations and it is not contained in Canada's bi-lateral treaties.

1490. *Secrecy.* According to the IAG, requests to Canada for mutual legal assistance will not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions or DNFBP. Records of financial institutions are obtainable in Canada under the MLACMA and the PCMLTF does not contain any restrictions in that regard either.

1491. Where legal professional privilege, known in Canada as solicitor-client privilege, affects evidence sought in Canada and it is not waived, the evidence will not be ordered, produced or sent. The search of law offices in Canada is subject to many restrictions and close judicial oversight (see Lavallee, Rackel and Heintz v. Canada (Attorney General); White, Ottenheimer and Baker v. Canada (Attorney General; R. v. Fink [2002] S.C.C. 61).

Process for executing requests

1492. The Department of Justice is responsible for the implementation of mutual legal assistance agreements and the administration of the MLACMA. The IAG carries out the functions assigned to the Minister of Justice under the MLACMA and provides advice to the Minister regarding his or her responsibilities under the statute. The IAG is designated as Canada's Central Authority in mutual assistance agreements. It is located at the headquarters of the Department of Justice in Ottawa. The MLA process is thus a centrally coordinated process.

1493. The MLACMA establishes a two-phase process for the gathering of evidence, which is briefly summarized as follows. The first phase is performed by counsel at the IAG. As the Minister's delegates, counsel at the IAG receive, review, approve and arrange for the execution by competent Canadian authorities of mutual legal assistance requests made to Canada by treaty partners or designated entities in criminal matters. The IAG ensures that all mutual legal assistance requests comply with treaty provisions and any other international or domestic standards that may be applicable. Canada did not provide any statistics on how long this stage generally lasts.

1494. Once a request has been approved, the second or judicial phase is triggered. It is at this stage that an application must be made to court for an order compelling the production of evidence or authorizing its seizure. Canada is a federal state with prosecutorial authorities at both the federal and provincial level. An approved request from a foreign state will be sent to either the regional office of the federal Department of Justice or to the office of the relevant provincial Attorney General depending upon the nature of the offence under investigation or prosecution in the requesting state. If the offence relates to drug trafficking, immigration, tax evasion, or another matter that is prosecuted by federal officials in Canada, the request will be sent to a regional office of the Department of Justice. If the offence is one that would be prohibited by Canada's Criminal Code, the request will be sent to the office of the provincial Attorney General in the province where the evidence is believed to be located. After the evidence has been gathered or seized pursuant to orders obtained under MLACMA, a second application must be made to a superior court judge for an order authorizing the transmittal to the requesting state of the gathered evidence.

1495. The MLA work of the IAG is handled by six of the 16 IAG lawyers, with the other ten lawyers focusing on extradition. The 6 paralegals and support staff are divided into extradition and mutual legal assistance teams. The IAG works in close cooperation with federal and provincial investigative and prosecutorial officials in executing incoming requests and in the process of making requests to other countries. In the major urban centres of Vancouver, Toronto and Montreal, the regional offices of the federal Justice Department also maintain teams of lawyers dedicated to handling both extradition and mutual assistance requests. The British Columbia Regional Office of the Department of Justice in Vancouver executes all incoming requests for assistance which are to be executed in that province. In Ontario and Quebec, the provincial Attorneys General similarly maintain teams dedicated to the execution of incoming requests.

1496. Canada has posted two experienced Canadian criminal counsel abroad. Two liaison positions have been established in Europe: one in Brussels for the European Union, and the other in Paris dealing primarily with extradition and mutual assistance requests to and from France.

1497. Canada did not provide information (as requested) about the actual or average length of time it takes to respond to money laundering assistance requests. In the absence of such data, the effectiveness of the system cannot be assessed.

1498. Statistics provided reveal that in the last five years Canada received 167 MLA requests (143 requests for evidence in money laundering cases). 46 of the total MLA requests were withdrawn by the requesting state (41 of these were ML MLA requests), which is about 25% of the total. Information on the reasons for these withdrawals is unknown to the team and Canada. Canada executed and complied 90 of the remaining 121 total MLA requests, currently leaving 31 outstanding requests which are presumed to be more recent requests.

Application of Recommendation 28 to request for mutual legal assistance

1499. The powers of competent Canadian authorities required under Recommendation 28 are available for use in response to requests for mutual legal assistance. Canada's mutual legal assistance measures apply equally to money laundering, terrorism and financing of terrorism offences. Where the request is made pursuant to a treaty, the offence must be one covered by the treaty. If there is no treaty, and the request is one by letter rogatory, then there are serious limitations. Under the MLACMA, there is the power to compel a witness to provide a statement other than at trial, which is not provided to Canadian police in domestic investigations, except for the investigation into a terrorism offence (see section 83.28 of the Criminal Code).

Mechanisms for determining the best venue for prosecution

1500. While there is no statute that applies to the determination of which country is best equipped to prosecute a matter, there is case law that sets forth the criteria that govern the exercise of discretion by Canadian prosecutorial authorities. The Supreme Court of Canada decision in *U.S.A. v. Cotroni* sets forth the test for when Canadian citizens should be prosecuted in Canada or abroad for their alleged criminal conduct. The determination of where a person may be prosecuted depends to a large extent on where the person is arrested. In cases where there has been a joint investigation involving Canadian police and their foreign counterparts, Canadian police do take part in consultations with their counterparts about the ultimate point of arrest. In cases where a person is arrested in Canada, who might simultaneously face the possibility of a Canadian and foreign prosecution based on the same conduct, there may be a request made to Canada for extradition[178]. There may be consultation between Canadian and foreign prosecution authorities on the appropriate territorial jurisdiction for the prosecution. Many of Canada's extradition treaties specifically provide for such consultation. Ultimately, the Courts in Canada leave the decision to prosecute or extradite in the hands of the Prosecution Service and the Department of Justice.

Additional elements

1501. As noted above, the powers to compel the production of evidence or authorise its seizure at the request of foreign authorities under the MLACMA are available only when the request is made pursuant to treaty or by a designated entity. Such requests must be made to Canada's central authority by the central authority of the requesting state or designated entity and if made directly police-to-police an MLACMA request is subsequently required to actually process the court order. Not all of the criminal investigatory tools are available for a judge who is considering a letter rogatory request, which limits the methods for obtaining evidence to the more limited production orders. Subsection 3(2) of the MLACMA specifically recognizes and maintains normal police to police contacts and arrangements. Where a foreign police agency provides evidence to its Canadian counterpart of the commission of an offence under Canadian law, Canadian police may choose to obtain an order under the Criminal Code or other domestic legislation to obtain the evidence for the Canadian investigation and may then be able to share that evidence with foreign authorities.

[178] Article 6 of the Canadian Charter of Rights and Freedoms protects the "right to remain in Canada for Canadian citizens", in cases where a Canadian citizen might either be prosecuted in Canada or extradited in relation to the same alleged conduct, the appropriate Attorney General within Canada (either federal or provincial) will perform an assessment based on factors identified under Canadian case law in order to determine whether prosecution in Canada is a "realistic" option in all of the circumstances.

1502. The discussions regarding Recommendation 36 (Criteria 36.1 – 36.6) also apply to mutual legal assistance requests related to terrorist acts and the financing of terrorism as they are offences in Canada.

Recommendation 37 & Special Recommendation V

1503. Except where direct enforcement of foreign orders for restraint or forfeiture of assets is requested, Canada does not require dual criminality for execution pursuant to the MLACMA.

1504. Canada does require dual criminality for extradition. However, because Canada uses a conduct oriented test, Canada will extradite where the conduct in issue would be a serious offence if it had been committed in Canada regardless of the fact that all of the elements of the foreign offence are non-congruent with all the elements of an offence in Canada (see section 3(2) of the Extradition Act).

1505. The discussions regarding Recommendation 37 (Criteria 37.1 – 37.2) also apply to mutual legal assistance requests related to terrorist acts and the financing of terrorism as they are offences in Canada.

Recommendation 38 & Special Recommendation V

1506. Under the MLACMA, Canada can directly enforce foreign orders for the restraint, seizure and forfeiture of assets on receipt of a request from a treaty partner or designated entity (see MLACMA sections 9.3 and 9.4). An order made by a court of criminal jurisdiction can be filed with the court in Canada and enforced as though it were an order of a Canadian court where the person has been charged in the requesting state or by the designated entity with an offence that would be an indictable offence were it to have been committed in Canada. This means, for example, that the owner or person in possession may challenge the order or apply to the Canadian court for the payment of legal, living and business expenses from the seized or restrained property. The property remains under the Canadian court's control while the foreign proceedings continue.

1507. With respect to foreign forfeiture orders, they may be filed and enforced as though they had been issued in Canada where the order has been issued by a court of criminal jurisdiction and the person has been convicted in the requesting state of an offence that would be an indictable offence were it to have been committed in Canada. The Minister of Justice must refuse a request for the enforcement of a foreign forfeiture order where the Minister has reasonable grounds to believe the request has been made for the purpose of punishing a person by reason of their race, sex, religion or other prohibited grounds. The Minister must also refuse where, in his or her opinion, giving effect to the order would prejudice an ongoing investigation, would impose an excessive burden on Canadian government resources, might prejudice Canada's security or where refusal of the request is in the public interest. Enforcing foreign restraint orders and forfeiture judgments can be cumbersome since the enforcement of such orders depends more upon the sufficiency of the foreign requests than would be the case in requests for legal assistance seeking evidence. The requesting state has to provide very detailed information regarding the grounds for the restraint, almost to a level of detail ordinarily reserved for obtaining domestic restraint in the first instance, even though under MLACMA the Canadian courts are not supposed to look behind the foreign order, but simply enforce same as if it were an order issued by a Canadian court. See MLACMA Section 9.3(4). Enforcing forfeiture orders has been done successfully, but it seems that the number of successful requests is not numerous: only four times in five years. Canada was unable to demonstrate to the assessors the effectiveness of the assistance it provides to foreign governments in confiscation matters.

1508. Although Canada initially provided statistics on the number of MLA requests it handled in a 5-year period, and then later provided some information on the success rate of those requests, it did not provide information about the average time in which MLA requests were executed in general or with regards to the relatively few forfeiture matters it handled nor explained any of the results Only 40% of forfeiture requests over the last five years were executed. In the absence of more compelling

MLA and extradition statistical data, the assessment of the MLA system's effectiveness is based on other information that was made available to the assessors. Canada on average has shared a little under CAD 100 000 in forfeited funds a year with its foreign partners. Considering that Canada forfeits about CAD 33 million in assets per annum, this international sharing figure seems low.

1509. Canada's MLA provisions for confiscation seem to encourage duplicative and potentially conflicting litigation in Canada. Presumably, Canada would not enforce forfeiture orders from foreign states that did not permit affected innocent owners the opportunity to challenge a confiscation order in the requesting state as the MLACMA gives the Minister relatively broad discretion to refuse to execute MLA requests if they are not in the interest of Justice. Nonetheless, Canada's MLA provisions, via MLACMA Section 9.4(9), incorporates Sections 462.41(3) and 462.42 of the Criminal Code, which permit any person, other than the accused, who is affected by a foreign restraint, seizure or forfeiture order to fully challenge the validity of the same in Canada and raise the "innocent owner" defence in Canada. There is no presumption of validity of the foreign order under Canadian law nor does MLACMA recognize that third-party property rights may have already been adequately protected by similar procedures in the foreign jurisdiction. This lack of comity results in the potential duplication of legal decisions made abroad, superimposes Canada's version of forfeiture onto foreign forfeiture regimes and proceedings, and creates the possibility of conflicts with the laws of requesting state and previous legal decisions made in the requesting state. A foreign judge handling a foreign forfeiture case would always be in better position to determine who is or is not an innocent owner, but Canada reserves the right to possibly hear or rehear that issue in Canada. Similarly, a Canadian judge can reduce a foreign forfeiture order of offence related property based upon "the proportionality" of the forfeiture to the offence giving rise to forfeiture and that claim can be brought by the accused. See MLACMA Section 9.4(9) incorporating Section 490.41(3) of the Criminal Code. This issue would normally be litigated in the requesting state.

1510. This duplication of the opportunity to make challenges in international confiscation matters increases the chances that defendants can bring lengthy legal battles in Canada. Proceeds of crime restrained for foreign governments may be released by a Canadian court to pay for legal fees and living expenses of the foreign criminal defendant under Canadian law prior to property being forfeited under the foreign law even if that would not be permitted under the applicable foreign law. This has the potential of undermining the criminal or forfeiture processes taking place abroad. The statement that the Section 462.34 financial hardship provisions apply to foreign forfeitures is odd given the fact that the innocent owner and proportionality provisions of the Criminal Code are expressly incorporated into the MLACMA, but the Criminal Code provisions that permit the release of frozen proceeds to pay for attorney fees or business and living expenses provisions are not as there is no specific reference to Section 462.34 of the Criminal Code in the MLACMA. Compare Section 9.3(4) with Section 9.4 (6) and (9).

1511. Canada can enforce foreign criminal orders for restraint, seizure or forfeiture, as described above, as long as they relate to the proceeds of crime or offence-related property. MLACMA does not provide for the enforcement of orders against property that is the equivalent value of forfeitable property, but has the power to enforce an order for "the payment of a fine" imposed in respect of an offence by a "court of criminal jurisdiction". Canada treats value based forfeiture judgements as fines. This means generally that Canada cannot enforce preliminary orders from legal systems that allow Courts to issue restraining orders in anticipation of an equivalent value forfeiture judgment until after the requesting state has actually obtained a final forfeiture judgement. The problem with this approach is that some jurisdictions, including Canada, do not have restraint mechanisms that can be used to place pre-judgement holds on non-tainted assets in anticipation of obtaining a fine or a value-based forfeiture judgement. Moreover, while the MLACMA has provisions that authorize Canadian courts to enforce foreign pre-judgment orders that seize or restrain proceeds or offence related property in anticipation of a forfeiture judgement against such identified proceeds or offence related property, the MLACMA does not provide similar authority for the enforcement of pre-judgment restraint or seizure orders obtained for anticipated fines or value-based forfeiture judgments.

1512. The IAG as Canada's central authority works closely with other central authorities and with investigative agencies. The timing of the execution of searches and seizures may be coordinated if Canada is provided with sufficient notice of the impending action in the requesting state. In situations where Canadian police are in a position to apply for orders under the Criminal Code for seizure, they may coordinate their actions with foreign counterparts. However, Canada has no formal arrangements or mechanisms were the confiscation experts in one country regularly meet with their Canadian counter parts. Confiscation coordination is ad hoc at best, and has been problematic with at least one major treaty partner. Canada does not seem to involve specialized confiscation points of contact, but, instead, seems to rely upon a central authority competence in confiscation law that rarely is present in most central authorities throughout the world.

1513. At the Federal level, Canada has not established an asset forfeiture fund that allows dedicated use of forfeited assets in a systematic way. Canada advised the assessment team that it had considered an asset forfeiture fund at a federal level to promote law enforcement, health education or other appropriate purposes, and decided against it, although Canada did not detail the process of their consideration. Forfeited funds can be shared with domestic and foreign law enforcement partners and the recipients themselves determine how those funds may be used or spent. There are riders on forfeited funds that the Federal government shares with the provinces requiring that the shared funds be used law enforcement, criminal justice and drug education purposes. Forfeited funds that are not shared eventually go into the general treasury and are spent by the Canadian Parliament as it sees fit.

1514. The Seized Property Management Act, which outlines Canada's proceeds of crime and offence related property asset management regime, includes authority to share anything forfeited to Canada in section 9(d) of that Act. Essentially, this provision allows Canada to share the "proceeds of disposition" (*i.e.* the money realised from the sale of forfeited assets). The Seized Property Management Act also specifically recognizes international sharing in section 11of the Act. Sharing must occur in accordance with the Act and the applicable Regulations.

1515. The Canadian Sharing Regulations allow Canada to share with a foreign government that participated in an investigation or prosecution that resulted in the forfeiture or provided information relevant thereto. There also must be a reciprocal forfeiture agreement with Canada for such sharing to be authorised. Canada has entered into many asset sharing arrangements with foreign states and is negotiating a number of additional agreements. Canada shares net proceeds after the forfeited items are liquidated, and cannot share an item in specie, that is, give the item to the other government to place into official use.

Additional elements

1516. As mentioned above, foreign orders for forfeiture must have been made by a "court of criminal jurisdiction" in order to be eligible to be enforced under the MLACMA. As most non-conviction based confiscation systems are "civil" in nature Canada cannot enforce such orders, even though many foreign Courts issuing such judgment are enforcing criminal laws and may in fact be acting under their criminal jurisdiction. This inability to enforce foreign *in rem* judgments does not apply in several Canadian provinces which have enacted comprehensive civil forfeiture legislative regimes. Canada indicated that constitutional issues eliminated this as a federal option, as only provinces have the competence to run civil court systems.

1517. The discussions regarding Recommendation 38 (Criteria 38.1 – 38.3) also apply to mutual legal assistance requests related to terrorist acts and the financing of terrorism as they are offences in Canada.

Statistics

1518. Inadequate statistics are maintained by the Department of Justice on some matters relevant to the effectiveness and efficiency of Canada's extradition and mutual legal assistance activities in

combating money laundering and terrorist financing. The IAG electronically records the receipt of a request, the requesting country, the nature of the request and when the file is closed. Special note is made of mutual assistance requests related to terrorism, money laundering and proceeds of crime.

1519. Canada responds to requesting countries immediately to confirm receipt of requests. The IAG is in regular contact with its counterparts to provide timely information regarding the execution of requests for assistance. Information was sought on the average time within which a request for assistance is executed but the data was not provided.

1520. The following table indicates the mutual legal assistance requests received and made by Canada for all offences from 2001-2006:

	Requests incoming	**Requests outgoing**	**Total**
2001-2002	387	140	**527**
2002-2003	406	104	**510**
2003-2004	311	84	**395**
2004-2005	318	77	**395**
2005-2006	350	84	**434**

1521. The following table indicates the mutual legal assistance requests received and made by Canada relating to money laundering, terrorism and financing of terrorism from 2001-2006:

	Requests involving money laundering – incoming	**Requests involving money laundering – outgoing**	**Requests involving terrorism – incoming**	**Requests involving terrorism – outgoing**	**Requests involving financing of terrorism – incoming**	**Requests involving financing of terrorism – outgoing**
2001-2002	22	38	5	5	2	0
2002-2003	32	15	8	2	3	0
2003-2004	28	14	6	4	1	0
2004-2005	23	32	4	1	2	0
2005-2006	38	14	4	4	1	0

1522. Canada indicated that the total number of mutual legal assistance requests received in all categories for the period between 2001 and 2006 is 167 and as follows:

MONEY LAUNDERING

Requests receive	143
Requests executed	78
Requests withdrawn/abandoned	41
Requests still active	24

RESTRAINT/FORFEITURE

Requests received	10
Requests executed	4
Requests withdrawn/abandoned	3
Requests refused	1
Requests still active	2

TERRORIST FINANCING

Requests receive	14
Requests execute	8
Requests withdrawn	2
Requests still active	4

1523. The following table indicates the value of the forfeited goods shared with other states:

Year	Value of forfeited goods
2002	CAD 153 000 (shared with Foreign States)
2003	CAD 18 500 (shared with Foreign States)
2004	CAD 270 000 (shared with Foreign States)
2005	CAD 54 000 (shared with Foreign States)
2006	N/A

6.3.2 Comments and Recommendations

1524. Canada has some problems with providing efficient MLA assistance. Canada should keep better MLA statistics than were provided to the assessors. Canada should consider options for streamlining judicial assistance such as streamlining processes to get financial and business records for foreign criminal investigations and consider devising a system that requires less judicial oversight of such matters. Not all involuntary production of business records or testimony should require judicial inquiries or oversight. For example, only if a party raises a valid legal objection to a production order should there be a need for judicial intervention.

1525. Canada should consider ways to give foreign confiscation requests more weight and become less subject to Court interference with the foreign criminal process. For example, Canada could make forfeiture assistance contingent upon the requesting state having a process that permits affected third-parties to challenge the forfeiture and that the proceedings in the foreign state otherwise comport with the Canadian concepts of due process, and then let the AG make that initial determination and place the burden upon the party challenging the foreign request to show that the requesting state's process for challenging a forfeiture falls below Canadian Constitutional standards. Canada should consider devising a way of executing foreign value based forfeiture judgments and related freeze, seizure or restraint orders to the same extent it can encumber proceeds and offence related assets before a foreign forfeiture judgment is obtained. Or, in the alternative, within the parameters of Canada's Constitutional framework, provide for pre-conviction restraint of an accused's assets for the payment of any potential fine, thereby protecting those assets from dissipation before the foreign court issues the fine, or value based forfeiture judgment.. Canada should create an informal process for the coordination of international confiscation cases jointly with the RCMP, the IAG and the prosecution service entities that execute MLA requests and their counter-parts in foreign governments so that these case can be handled more expeditiously and by persons who are experts in forfeiture law.

1526. Canada should allocate more resources to the authorities in charge of processing MLA requests.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

Rec.	Rating	Summary of factors underlying ratings
Rec.36	LC	• There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data.
Rec.37	C	• The Recommendation is fully met.
Rec.38	LC	• There are doubts about the effectiveness of the measures in place under Recommendation 38: there is limited evidence of effective confiscation assistance as only four cases have been successful in last 5 years and international sharing statistics indicate that while asset sharing with foreign states is possible, it rarely occurs. Canada executes requests to enforce corresponding value judgments as fines, which has limitations and cannot be enforced against property held by third parties.
SR.V	LC	**Regarding compliance with Recommendation 38** • All elements missing in R. 38 are missing for SR.V; • There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data.

6.4 Extradition (R.39, 37 & SR.V)

6.4.1 Description and Analysis

Recommendation 39 & Special Recommendation V

1527. *ML as an extraditable offence*. The money laundering offence is an extraditable offence under Canada's Extradition Act. Money laundering is a criminal offence under the Criminal Code and thus the dual criminality aspect of extradition can usually be met.

1528. The Minister of Justice is responsible for the implementation of extradition agreements, the administration of the 1999 Extradition Act ("Act"), including the processing of requests for extradition or provisional arrest under the Act or an applicable agreement. The Act provides that if certain preconditions are met a person may be extradited: 1) for the purpose of prosecution, 2) for the purpose of imposing a sentence on the person, or 3) for the purpose of enforcing a sentence already imposed on the person. Canada is party to 50 bilateral extradition treaties and has designated a number of countries as extradition partners.

1529. Canada's assistance under the Act may be engaged on the basis of 1) an extradition treaty between Canada and the state or entity making the request, 2) a multilateral agreement to which both Canada and the requesting party are signatories and which contains a provision on extradition, 3) a specific agreement entered into between Canada and the requesting state or entity with respect to a person or persons in a particular case, and 4) a general designation of the requesting state or entity as an "extradition partner" under the Act thereby allowing the extradition partner full coverage under the provisions of the Act notwithstanding the absence of an extradition treaty. In addition to a number of members of the Commonwealth, Canada has designated as extradition partners, two non-commonwealth countries, Costa Rica and Japan, as well as the International Criminal Court, and International Criminal Tribunals concerned with the prosecution of persons responsible for violations of international law in Rwanda and in the Former Yugoslavia.

1530. A request for provisional arrest may precede a formal request for extradition. Provisional arrest refers to a request for the apprehension of an individual, generally in circumstances of urgency or a similar ground of public interest, prior to the preparation of the documentary material upon which the formal extradition will be requested. A provisional arrest request may be made through Interpol.

1531. The Minister of Justice has the discretion to approve an application for a provisional arrest warrant if satisfied that a) the offence in question is subject to certain minimum penalty requirements set out in the Act, and 2) the extradition partner will make a formal request for the extradition of the person within a given time-period (specified by the treaty, other agreement or the Act) subsequent to the person's provisional arrest. Once a formal extradition request is received, the Minister of Justice may issue an authority to proceed. An authority to proceed authorises an extradition hearing to be held in order to consider whether the person should be committed for extradition.

1532. Once approved, the IAG forwards the request and all supporting material to the regional office of the Department of Justice in the jurisdiction where the person sought is believed to be located. That regional office will assign legal counsel to initiate and assume conduct proceedings before a judge to seek an order for the committal for extradition of the person. Regional counsel will also represent the extradition partner and the Minister of Justice throughout any appeal or judicial review proceedings.

1533. The person whose extradition is sought appears at the extradition hearing and participates through his legal counsel or directly. The Canadian offence that corresponds to the conduct supported by the foreign request will be identified by IAG counsel and named in a document called an Authority to Proceed ("ATP"), which is filed with the Canadian court before judicial proceedings begin. In the case of a person sought for the purpose of prosecution, the judge will determine if the evidence provided by the extradition partner is such that the person would be committed for trial in Canada if

the conduct had occurred in Canada and the corresponding offence had been charged in Canada. In the case of a person sought for the imposition or enforcement of a sentence the judge will determine if the person has been convicted with respect to conduct that corresponds to the Canadian offence listed in the ATP. Where the person sought for extradition has been convicted in the foreign State in absentia, the matter will be treated in Canada has though it were a request for prosecution rather than imposition or enforcement of a sentence.

1534. The Extradition Act allows evidence to be presented at the extradition hearing in a variety of ways: 1) in the usual manner applicable to Canadian domestic proceedings such as through the testimony of witnesses, or 2) in reliance on the provisions for the introduction of evidence set out in an applicable extradition arrangement, or 3) by means of a "record of the case". Evidence gathered in Canada must satisfy the rules of evidence under Canadian law in order to be admitted.

1535. The Extradition Act renders admissible at the extradition hearing a document called the Record of the Case, which summarizes the evidence available to the extradition partner for use in the prosecution, notwithstanding the fact that this document contains evidence otherwise inadmissible in Canadian domestic proceedings, as long as certain safeguards are respected. This includes having a judicial or prosecuting authority of the extradition partner certify that the evidence summarized is available for trial and is either sufficient to justify prosecution or gathered in accordance with their law. If the presiding judge is satisfied with the evidence, he or she will order the person detained pending the Minister of Justice's decision whether to surrender the person. Otherwise, the person will be discharged and released.

1536. The judicial phase of the extradition process is a determination only that the evidence is sufficient to warrant that the person be extradited. The ultimate decision with respect to whether the person will in fact be surrendered to the extradition partner is that of the Minister of Justice. At this phase of the process the Minister of Justice will consider any representations from the person or the person's counsel with respect to why the person should not be extradited or concerning any conditions to which the surrender order should be subject. In reaching a decision on surrender the Minister of Justice will be obliged to weigh the submissions of the person against Canada's international obligations with respect to extradition. The Minister of Justice in reaching his or her decision must respect the rights of the person sought as guaranteed by the Canadian Charter of Rights and Freedoms.

1537. If the person sought for extradition is serving a sentence in Canada, the Minister of Justice may order temporary surrender so that the person can face prosecution or appeal proceedings in the courts of the extradition partner and then be returned to Canada to serve the remainder of his or her outstanding sentence here. While the Minister of Justice relies upon advice from the IAG, he or she decides personally in each case. When the Minister of Justice agrees to surrender the person, the IAG helps coordinate arrangements for the actual transfer of the person to authorised agents of the requesting state or entity.

1538. *Extradition of nationals*. Canada can extradite its own nationals subject to the discretionary ground of refusal set out in section 47 of the Extradition Act or the relevant extradition agreement. Any actions taken by Canadian authorities in relation to a foreign request for extradition will be governed by the Canadian Charter of Rights and Freedoms. The Charter is a part of Canada's Constitution, which is the supreme law of Canada. The Charter guarantees certain rights and freedoms. For example, Section 6 of the Charter gives Canadian citizens "the right to remain in Canada." This means that where the person sought for extradition is a Canadian citizen and the offence for which extradition is requested is one that is capable of being prosecuted in Canada, the relevant Canadian Attorney General (either federal or provincial) must perform an assessment of whether prosecution in Canada is a "realistic" option. The assessment, known as a "Cotroni assessment", is based on factors that were enumerated in a decision from the Supreme Court of Canada called U.S.A. v. Cotroni [1989] 1 S.C.R. 1469. Historically, the result of most of these assessments has been to favour extradition.

1539. *Delays to process extradition requests*. The Extradition Act sets out time lines for specific steps to ensure minimal delays. For example, it is expected that extradition cases are to take priority at courts. The Extradition Act contains provisions calling for early dates to be set in extradition matters. The Department of Justice Canada has also created specialized teams throughout the country to help deal more swiftly and efficiently with requests for extradition and mutual legal assistance.

1540. The Extradition Act sets out time lines for specific steps in the extradition process to ensure minimal delay. Extradition cases are to take priority in accordance with section 21(3) of the Extradition Act: "The judge shall set an early date for the extradition hearing, whether that date is in or out of the prescribed sessions of the court." Extradition appeal cases are to take priority in accordance with section 51 of the Extradition Act: "An appeal under this Act shall be scheduled for hearing by the court of appeal at an early date whether that date is in or out of the prescribed sessions of that court."

1541. The use of the diplomatic channel is not mandatory in Canada as the Department of Justice is designated by Statute as the Central Authority for the implementation of extradition agreements, the administration of the Extradition Act and requests for extradition made under them. A few of Canada's more recent extradition treaties reflect this by providing for direct transmission of extradition requests between Canada's Department of Justice and Canada's treaty partner's appropriate authority. However, per international convention and the great majority of Canada's extradition agreements, extradition requests generally continue to be conveyed through diplomatic channels.

1542. *Statistics*. Canada provided the number of formal extradition requests it has received in a five year period from 2001 to 2006 and data showing the number of completed and abandoned incoming MLA requests, but did not provide any data on how long those requests were pending, or explain why requests were abandoned or denied. Only 24 of 106 persons requested for extradition over the last five years (less than 25%) have been returned to the requesting state.

1543. The following table indicates the number of extradition requests received and made by Canada for all offences from 2001-2005:

	Incoming requests	Outgoing requests	Total
2001	148	52	**200**
2002	187	37	**224**
2003	200	41	**241**
2004	178	36	**214**
2005	183	31	**214**

1544. The following table indicates the number of extradition requests received and made by Canada relating to money laundering, terrorism and financing of terrorism from 2001-2005:

	Requests involving money laundering – incoming	Requests involving money laundering – outgoing	Requests involving terrorism – incoming	Requests involving terrorism – outgoing	Requests involving financing of terrorism – incoming	Requests involving financing of terrorism – outgoing
2001	9	4	4	0	2	0
2002	5	2	3	0	0	0
2003	9	1	1	0	2	0
2004	17	2	1	0	0	0
2005	14	1	3	0	0	0

1545. There were 58 incoming requests relating to money-laundering and TF, but there were 106 persons sought for extradition as follows:

Money Laundering: Total of 103 persons sought for extradition[179]

- 23 individuals were returned to the Requesting State.
- The requests for 28 individuals were abandoned or withdrawn.
- For 52 individuals, the cases are still pending (that is, either the person has still not been located or the case is still at some stage of the extradition process, including the judicial, ministerial and appellate stages).

Terrorist Financing: Total of 3 persons sought for extradition

- 1 returned.
- 1 request withdrawn.
- 1 still ongoing.

1546. Recommendation 39 (Criteria 39.1 – 39.4) also applies to extradition proceedings related to terrorist acts and the financing of terrorism as they are offences in Canada.

Additional elements

1547. Persons cannot be extradited based only on warrants of arrests or judgements. There must be an assessment of the evidence, which takes place in the course of the judicial phase, which is followed by the Ministerial phase of the extradition proceedings.

1548. The simplified procedure of extradition of consenting persons who waive formal extradition proceedings will speed up the process and is set out in sections 70 -71 (consent) and section72 (waiver of extradition) of the Extradition Act For purposes of waiver, a description of the evidence (record of the case) is sufficient and certain ministerial acts are waived. Some of the cumbersome Ministerial approvals are dispensed with as well.

Recommendation 37 (dual criminality relating to extradition) and Special Recommendation IV

1549. With respect to extradition, dual criminality is required. Dual criminality requires that the conduct constitute an offence in both countries and that it be punishable by a prescribed period of incarceration. By default, as provided in the Extradition Act, in most cases, for the offence to be extraditable, it must carry a maximum penalty of at least two years of imprisonment. However, particular treaties may fix a lower sentence as a minimum, as does the Canada-U.S. treaty, for example. Canada uses a conduct test and will only extradite where the conduct in issue constitutes an offence that carries the relevant sentence minimum. However, it is not necessary that the offence under Canadian law have the same name or precise constituent elements as the foreign offence.

6.4.2 Recommendations and Comments

1550. Canada should maintain better extradition request data and should consider doing a critical evaluation of the extradition process.

[179] Of the 52 matters on 24 May 2007, there were only 32 requests still pending.

6.4.3 Compliance with Recommendations 37 & 39 and Special Recommendation V

Rec.	Rating	Summary of factors underlying ratings
Rec.37	C	• The Recommendation is fully met.
Rec.39	LC	• Insufficient statistical data was provided to make a thorough assessment, particularly the assessment of the delay element, but even the limited data provided indicates that obtaining extradition from Canada quickly may be difficult.
SR.V	LC	**Regarding compliance with Recommendation 39** • No meaningful statistical data provided to assess delay element (effectiveness issue).

6.5 Other Forms of International Co-operation (R.40, SR.V & R.32)

6.5.1 Description and Analysis

Obligation to provide the widest range of international co-operation

Law enforcement authorities

1551. Law enforcement authorities in Canada regularly provide informal assistance to police forces from other countries, in accordance with the laws of Canada. Generally, Canadian police are able to provide information or documentation that is publicly available or those that can be obtained on a voluntary basis. This usually involves direct communication between the police forces and may include transmission of information through Interpol.

1552. The RCMP is able to provide international cooperation to their foreign counterparts under Interpol, the international Liaison Officer (LO) program, MLAT and Extradition requests. The RCMP has formal arrangements that it can enter into with foreign counterparts for exchange of information, such as, Memoranda of Understanding (MOU) or Letters of Agreement (LOA). When sensitive information in the national interest is shared with or released to other governments, departments or organizations not covered by the Security Policy and Standards of the Government of Canada, the RCMP must ensure, through written agreements, *e.g.* MOU, that appropriate safeguards are established for the safekeeping of the information.

1553. The RCMP, in accordance with the Privacy Act, will share information related to domestic national security information with appropriate international agencies depending on that agency's "need and right to know" and in considering how such information would help further a criminal investigation. The RCMP includes with all outgoing written correspondence, messages and documents shared with other foreign agencies the required caveats that concern the ownership and the classification of the shared information. The RCMP may, with the Minister of PSEPC's prior approval, enter into a written or oral arrangement, or otherwise cooperate, with foreign security and intelligence organizations. This does not apply to foreign law enforcement agencies or organizations. National Security Investigations Section (NSIS) of the RCMP will be the point of contact for all foreign intelligence agencies in matters of national security.

1554. The RCMP Liaison Officer program was established to train and deploy highly skilled and multi-lingual regular members to strategic locations throughout the world. Partnering with international law enforcement agencies, foreign governments and Canadian embassies, the role of a LO is to maintain a link between Canadian law enforcement and the law enforcement agency of a host country to prevent and detect criminal offences against Canadian federal laws. Currently there are 35 RCMP liaison officers in 25 different locations in three geographic regions: Asia-Pacific/South Africa; Europe-Middle East-Africa; and Western Hemisphere.

1555. Mutual Legal Assistance Treaty (MLAT) requests and Extradition requests from participating countries are other mechanisms in which information is exchanged between international law enforcement agencies. A review of the money laundering investigational files indicate that through the

use of MLATs, Canada Law Enforcement provided the evidence/support for the restraint and eventual forfeiture of assets in the United States, Cuba, Antigua, the Cayman Islands, Switzerland and Luxembourg.

1556. The RCMP receives numerous requests to provide additional training internationally. Training has been provided to representatives from many countries including Columbia, Dominican Republic, Jamaica, Cuba, Austria, Czech Republic, Russian Federation, Peru, Venezuela, Hong Kong, Kenya, Panama, Bogotá, Pakistan, Bahrain, and Guatemala.

FINTRAC as an FIU

1557. FINTRAC is authorised to share information about suspected money laundering or terrorist financing with a foreign financial intelligence unit or similar foreign entity if a Memorandum of Understanding is signed between the two organisations. FINTRAC is authorised to receive information from these similar foreign entities when no MOU is signed between the two organizations. According to the PCMLTFA, the Minister of Finance or FINTRAC, with approval of the Minister may enter into a written agreement with a similar foreign entity for the exchange of information that there are reasonable grounds to suspect would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence.

1558. When deciding to pursue an MOU with a similar foreign entity (hereafter FIU), FINTRAC considers a number of factors, including the following: Canadian foreign policy; FINTRAC's operational priorities; the FIU's enabling legislation; other jurisdictional legislation relating to curbing money laundering or terrorist financing; the privacy/access laws that exist in the jurisdiction (physical, IT and others); the jurisdictions participation in the FATF or FATF Regional-Style Bodies; the FIUs standing in the Egmont Group and adherence to the Egmont Principles of Information Exchange; and the measures that the FIU has in place to protect information. FINTRAC's signed MOUs are consistent with the Egmont Group Model MOU Template.

1559. Requests for information from MOU partners are normally received through the Egmont Secure Website (ESW) a secure communication channel used by most Egmont-member FIUs. Once an FIU query (FIUQ) is received FINTRAC sends an acknowledgment of receipt email via ESW. A copy of the FIUQ is made and immediately assigned to an analyst in order to determine if FINTRAC has transaction information related to the FIUQ. If so, analysts use all information available to them to build a case in response to the query. If FINTRAC does not have financial transaction information relating to the query received, a negative response is provided to the querying FIU. As a matter of practice, the assessment team was told that all queries are dealt with at least on a preliminary basis within 30 days or sooner for an urgent request. Negative responses are generally provided within five days of receipt of the query.

1560. The threshold for disclosing to foreign counterparts is the same as for domestic police forces, and once the analysts are of the view that the threshold has been met, the disclosure is worked through the same approval process described earlier with respect to domestic disclosures. Similarly, in its disclosures to foreign FIUs, FINTRAC provides the same designated information as it does domestically (see Section 2.5).

1561. If FINTRAC is in a position to disclose designated information in response to a FIUQ it is sent via ESW (provided the FIU has a current security certificate, to ensure the information that is being sent is encrypted). One of the stipulations of the MOU between FINTRAC and its foreign counterparts is that any information provided to the foreign agency may only be used for its intended purpose (investigation or prosecution of a money laundering or terrorist financing offence), and the information may not be further disseminated to any third party without the explicit prior consent of FINTRAC. FINTRAC also adheres to these stipulations regarding the information received from foreign FIUs.

1562. FINTRAC currently has 44 MOUs in place and continues to actively negotiate additional MOUs.

International Fora

1563. Canada has responded to the challenges of international cooperation by posting experienced Canadian criminal counsel abroad. Two liaison positions have been established in Europe: one in Brussels for the European Union, and the other in Paris, to coordinate Federal Prosecution Service (FPS)[180] (see Section 6.3 of the report).

Supervisors co-operation

1564. *FINTRAC.* Until the new provisions were enacted in December 2006, the PCMLTFA did not allow FINTRAC to exchange compliance-related information with its foreign counterparts. PCMLTFA now allows FINTRAC to enter into information sharing arrangements or agreements under new section 65(2) with any agency in a foreign state that has responsibility for verifying AML/CFT or with an overseas organization with respect to compliance information relating to any reporting entity under the Act as well as the assessment of risk relating to the institution's level of compliance.

1565. FINTRAC advised the examiners that at this time the organisation had not entered into any arrangements or agreements of this nature. In addition, FINTRAC has MOUs with most of the Canadian financial sector supervisors both at a federal and provincial level to receive compliance information from these agencies. Given the fact that FINTRAC is the supervisory agency as regards AML/CFT compliance issues and the wide range of institutions under AML/CFT obligations in Canada, to a large extent, FINTRAC would rely on the information received from federal and provincial regulatory agencies to meet requests for information from supervisory counterparts. However, the actual mechanisms for sharing are still in discussion.

1566. *OSFI*. Under the OSFI and Bank Act, the Superintendent of Financial Institutions is empowered to share information relating to banks with other agencies that are involved in the regulation of financial institutions provided that the Superintendent is satisfied that the information will be held by those agencies on a confidential basis.

1567. Although not required by law, OSFI generally shares information with overseas regulators via MOU. OSFI MOUs refer specifically to sharing information relating to terrorism and financial crimes. Financial crimes are specifically defined as money laundering, unauthorised banking, investment or insurance business and all other violations of law on financial markets. The crime of financing terrorism would not seem to be included as "…violations of law on financial markets".

1568. OSFI demonstrates effectiveness based on its co-operation in conducting cross border examinations in a number of countries in which its licensees have subsidiaries. Assistance has been rendered to OSFI in the absence of formal MOUs. However cross border examinations of institutions in Canada would be subject to a formal MOU requirement.

1569. *Provincial regulators*. Four provincial Securities Regulators (Ontario, Quebec, Alberta and British Columbia) are signatories under IOSCO's Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information. However, the MOU examined did not refer to the exchange of information relating to AML/CFT. The definition of "laws

[180] The Federal Prosecution Service, through the National Security Group, is responsible for developing operational policy related to the prosecution of terrorism offences, providing legal advice to investigative bodies (*e.g.* Royal Canadian Mounted Police, Canada Border Services Agency (CBSA), etc.) in relation to the investigation of terrorism offences, and conducting prosecutions of terrorism offences involving the national interest and supporting prosecutions conducted by the provincial Attorneys General.

and regulations" under the MOU is expressly limited to issues relating to securities. However, this does not preclude securities regulators to exchange AML/CFT compliance information should their securities legislation permit it.

1570. The Ontario Securities Commission has its Office of Domestic and International Affairs that deals with overseas governments and regulators. Its governing statute at section 153 does also specifically refer to wide powers of the Commission to share information internationally with foreign regulators, stock exchanges, SRO and law enforcement authorities. This may permit the OSC to share information even in the absence of a MOU. The IDA has broad powers to share information with other regulatory and police agencies whether or not a formal information sharing agreement is in place. In Québec, section 297 and following of the *Securities Act* refer to broad powers of the *Autorité des marchés financiers* for sharing information with foreign and national authorities, including securities regulators, police forces, the Minister of Revenue or any other department, body or organization with whom the *Autorité des marchés financiers* may enter into an agreement to facilitate the administration or enforcement of securities and fiscal legislation as well as penal or criminal legislation.

1571. In the case of Credit Unions, there are several supervisors. In the case of the Deposit Insurance Corporation of Ontario, the Credit Union and *Caisses Populaires* Act does not provide DICO with the express power to share information (whether AML/CFT related or otherwise) cross border. In the case of the Financial Services Commission of Ontario the governing statute also seems to have this shortfall (there is no statutory authority for the Superintendent to share information under his general powers and duties in Section 5 of the Financial Services Commission of Ontario Act, 1997). Desjardins Group also plays a supervisory role in the case of its group of credit unions. Whilst Desjardins has demonstrated outreach to other jurisdictions to assist in development of Co-operative movement, the assessors did not see any basis for or evidence of the sharing of information with other supervisory counterparts on a cross border basis. Canada indicated that all credit union supervisors can exchange compliance information with international counterparts although there is no legal framework that explicitly authorises the exchange of such data.

1572. The assessors take the view that the main avenue for the cross-border sharing of supervisory information relating to AML/CFT compliance issues would be through FINTRAC, the main AML/CFT supervisory authority although there is no barriers to OSFI, the OSC, the IDA or the AMF sharing AML/CFT supervisory information with foreign counterparts. This mechanism of directing AML/CFT information through FINTRAC appears necessary given in particular the absence of legal framework for certain provincial regulators that explicitly authorises them to exchange AML/CFT compliance information with foreign counterparts.

Gateways and channels for prompt and constructive exchanges of information

Law enforcement authorities

1573. Canada became a member of International Criminal Police Organization in 1949, and the RCMP was delegated the responsibility for administering and operating the National Central Bureau (Interpol Ottawa). Interpol Ottawa is located at RCMP National Headquarters and forms part of the International Liaison Program. Interpol Ottawa works closely with the Canadian Central Authority and serves as the link between official Canadian and international law enforcement agencies. Interpol Ottawa is the central coordination point for the Canadian law enforcement community in pursuing criminal investigations abroad, establishing rapid contact with foreign police agencies and liaison officers, transmitting requests for information required in investigations to NCBs in other countries and assisting on judicial proceedings. Interpol Ottawa provides information on various organized crime groups and their activities, criminal activity with international ramifications, and provides money laundering information for use in countering international money laundering.

FINTRAC as an FIU

1574. FINTRAC has developed and implemented a process to obtain feedback from its partner FIUs about the query process and disclosures. The assessment team was told that FINTRAC has generally received positive feedback and is currently considering how best to respond to comments and to further strengthen these relationships.

Supervisors co-operation

1575. While FINTRAC as AML/CFT compliance supervisor now has legislative authority to share supervisory information, it must do so via agreement or arrangements with its international supervisory counterparts. FINTRAC has not entered yet into arrangements or agreements of this nature (although Canada indicated that FINTRAC is currently negotiating with several counterparts abroad) and therefore a serious issue arises as to the effectiveness of the system and the perceived inability at this point for an international supervisory counterpart to receive supervisory information relating to AML/CFT in sectors outside of those supervised by OSFI, IDA, the OSC and the AMF.

1576. Whilst OSFI is able to share AML/CFT compliance information on its FRFIs under the MOU that it executes with supervisory counterparts (and even possibly in the absence of such a MOU under the OSFI Law), the IOSCO MOU is restricted in terms of the information that can be shared and in several cases (not including the Ontario Securities Commission and the AMF in Québec the regulators themselves do not appear to have an inherent jurisdiction to share information on a cross border basis. The same situation appears to exist in the case of other provincial regulators.

Spontaneous exchanges of information or upon request

Law Enforcement authorities

1577. As described earlier in this Section, the RCMP is able to assist foreign counterparts with both spontaneous and more formally administered requests for information. These exchanges are subject to the RCMP information sharing protocols (see comments latter in this Section on controls and safeguards).

FINTRAC as an FIU

1578. As stipulated in the PCMLTFA, FINTRAC is authorised to exchange information, either spontaneously or upon request, in relation to money laundering offences, terrorist activity financing offences and offences that are substantially similar. Although FINTRAC can receive information about money laundering and the underlying predicate offence, FINTRAC can only provide information relevant to the money laundering offence (not about the underlying predicate offence). Since June, 30 2007, FINTRAC is able to share a larger amount of designated information, including "*the grounds on which a person or entity made a report under section 7* (i.e. *a suspicious transaction report) about the transaction or attempted transaction and that the Centre considers relevant in the circumstances*". An MOU between FINTRAC and the foreign agency must be in place to govern this exchange.

Supervisors co-operation

1579. FINTRAC's powers to share supervisory information will be dependent on the terms of the agreements or arrangements that would be established between FINTRAC and its supervisory counterpart. As these have not yet been established it is not clear whether information will be provided on a spontaneous basis as well as upon request.

1580. Information exchange will occur with OSFI in practice within the context of an MOU. However provided that the requirements of the Bank and OSFI laws are met, there would be no bar to

spontaneous information exchange. The MOU provides that for the most part, information requests must be made in writing but that in cases where expedition is required, then the request should be followed up in writing. The assessors also consider that the OSFI laws are framed widely enough for OSFI to share information even in the absence of a MOU.

1581. Similarly under the Securities Act of Ontario, the OSC can receive and provide information broadly with regulators and law enforcement. There is no legal limitation as to whether the information must be the subject to a request or whether it may be shared on a spontaneous basis. Canada indicated that the same holds true for the Autorité des marches financiers in Québec.

1582. The IDA has broad powers to share information with other regulatory and police agencies whether or not a formal information sharing agreement is in place.

1583. The assessors noted limitations as regards other provincial securities regulators whose information sharing is based on the IOSCO MOU. In addition there was no express power of provincial credit union supervisors to share AML/CFT information internationally.

Authorisation to conduct inquiries on behalf of foreign counterparts

Law Enforcement authorities

1584. The RCMP can use a number of criminal intelligence and police databases to conduct inquiries on behalf of foreign counterparts. The information contained in those systems is governed by different sharing protocols that aim at protecting the right to privacy of the individuals mentioned in the different databases.

FINTRAC

1585. FINTRAC is able to conduct inquiries on behalf of foreign counterparts in relation to with which it has an MOU. In such cases, FINTRAC is able to access its databases of all report types. FINTRAC is also able to access federal and provincial databases maintained for purposes related to law enforcement information or national security, and in respect of which there is an existing agreements, and to publicly available information, including commercially available databases, in developing the case. The threshold and limitations on designated information for disclosing the results of inquiries conducted on behalf of foreign counterparts is the same as previously discussed for domestic disclosures.

Supervisors co-operation

1586. Provided that there is an agreement or arrangement in place, FINTRAC may make queries relating to AML/CFT supervisory information on behalf of international counterparts and relate their findings to the requesting authority. FINTRAC has overarching powers to carry out inspections and otherwise obtain information from of financial institutions that are covered by the PCMLTFA. Additionally, it may rely on information received from domestic supervisors to respond to queries from these overseas counterparts.

1587. Both OSFI and the Ontario Securities Commission can make enquiries on behalf of international partners as regards AML/CFT issues and communicate these findings to the counterpart supervisor. In the case of other securities regulators, such exchanges may not be possible in the absence of express power to share AML/CFT information internationally.

1588. OSFI is not an investigatory body per se, and would be limited by its governing law to conducting investigations which relate to obligations under their own governing statutes.

Exchanges of information without disproportionate or unduly restrictive conditions

Law Enforcement authorities

1589. The RCMP is committed to exchanging information with foreign counterparts in circumstances that help to effectively combat money laundering and terrorist financing. The RCMP handles requests in accordance with all Canadian laws and its own internal procedures and protocols for information sharing. These procedures and protocols provide clear guidelines for proportionate classification of material along with the necessary conditions that must be enforced on protected, classified material.

1590. The RCMP also uses Interpol and the RCMP International Liaison Officer Program to help facilitate the flow of information between international policing agencies.

FINTRAC as an FIU

1591. FINTRAC's legislation requires that an MOU be signed and that a legal threshold be met to exchange information related to suspected money laundering and terrorist financing with an MOU partner. It is important to note that disclosures to MOU partners are similar to disclosures to domestic law enforcement and national security agencies.

Supervisors co-operation

1592. The exchange of supervisory information is not made subject to disproportionate or unduly restrictive conditions. FINTRAC's main criteria with regards to supervisory information is that there is an appropriate agreement or arrangement in place and that the compliance information will be kept confidential and used only for the purposes of ensuring compliance and measuring risks. In OSFI's case, the criteria are that the recipient agency is a supervisory agency and that the agency will keep the information confidential. In the case of the OSC the powers are broader. Other provincial regulators would have to rely on FINTRAC acting as a conduit for the exchange of information internationally.

Cases involving fiscal matters

1593. Under the PCMLTFA, FINTRAC may disclose designated information to an MOU partner when it has reasonable grounds to suspect that this information would be relevant to investigating or prosecuting a money laundering or a terrorist activity financing offence, or that is substantially similar to either offence. Whether or not the query involves fiscal matters, FINTRAC will consider disclosing information as long as the query also involves money laundering and/or terrorist financing activity matters.

1594. For OSFI, once an MOU is in place with another regulator, information is shared as permitted under the MOU subject to the conditions contained therein.

Existence of secrecy or confidentiality requirements

Supervisors co-operation

1595. The supervisory authorities in Canada including FINTRAC, OSFI, the provincial supervisors and SROs all have very clear and broad power to access information from their supervised entities, which may then be passed on to overseas counterparts through the appropriate channels provided that the statutory or administrative preconditions are met (*e.g.* the execution of an information sharing agreement or arrangement). In the case of supervisory authorities that do not have the appropriate power to share directly, such information exchange would be likely to occur through FINTRAC. The assessors did not consider that secrecy or confidentiality laws would have affected the ability of the relevant supervisors to co-operate with their counterparts, through the abovementioned avenues.

Controls and safeguards

Law Enforcement authorities

1596. The RCMP supports the concept of integrated policing through the exchange of criminal intelligence and information with external partners. The RCMP also recognizes this exchange and sharing process is governed by federal legislation, Ministerial Treasury Board Directives, Ministerial directives, and RCMP policies, and various specific caveats and conditions. There are fundamental protocols and Best Practices the RCMP uses to ensure that criminal intelligence and information that is shared with foreign partners and agencies is used only in an authorised manner. The RCMP have policies that help guide it to appropriate decisions for handling requests and sharing or exchanging criminal intelligence and information with foreign partners and agencies. The large majority of RCMP information is subject to security classification. The security level of the information in question will govern many aspects of information sharing or exchange process with external partners.

1597. RCMP documents containing police information or criminal intelligence also include standard caveats that provide further direction on how, and with whom, the document can be shared. These caveats generally outline conditions that are binding on the recipient, regarding the use and disclosure of the information contained in the document.

FINTRAC as an FIU

1598. Consistent with Canada's privacy legislation, FINTRAC undertakes strict safeguards to protect the confidentiality of the information collected through the PCMLTFA. This principle of protecting information is also applied to information received from other competent authorities. A confidentiality clause in FINTRAC's MOU template stipulates that all information exchanged will be subject to strict controls and safeguards to ensure that the information is used only in an authorised manner and treated in a confidential manner and will be protected by FINTRAC and the foreign authority by the same confidentiality as provided by the legislation of the country of the receiving Authority for similar information received from domestic sources.

Supervisory authorities

1599. FINTRAC as AML/CFT supervisor is subject to the safeguards indicated above. In OSFI's case, the criterion is that the recipient agency is a supervisory agency and that the agency will keep the information confidential. In the case of the OSC the powers appear to be broader.

Additional elements

1600. The RCMP may, with the Minister of PSEPC's prior approval, enter into a written or oral arrangement, or otherwise cooperate, with foreign security and intelligence organizations. As such, there are working arrangements and understandings between the RCMP and those intelligence agencies in respect to the sharing of information. Information received from any of these agencies will be treated to the standard care maintained by the agency which generated the document and any other conditions they wish to impose.

1601. Other arrangements with foreign agencies are established and maintained as long as they remain compatible with Canada's foreign policy towards the country or international organization in question.

1602. OSFI does not have authority to deal with non-counterparts in respect of confidential information on supervised financial institutions. However, OSFI can and does assist both domestic and foreign regulators where non-confidential information is involved. For examples, OSFI has an active program of tracking alleged unauthorised banking and insurance activity in Canada and elsewhere. Information received as part of this activity is freely and regularly exchanged with law enforcement,

other regulators, prosecutors (domestic and foreign), supervised financial institutions, and others. Where appropriate OSFI also posts this information to its web site.

Statistics

1603. *FIU*. FINTRAC keeps adequate statistics concerning the number of formal request for assistance made to or received by the FIU from foreign counterparts, including the number of spontaneous referrals. No statistics are kept on the number of requests granted or refused and the time requested to respond.

1604. *Supervisory authorities*. OSFI keeps statistics on the number of formal requests for assistance made or received.

Data on other forms of international co-operation

1605. The following tables provide summary information about FINTRAC exchange of information with foreign FIUs (up to date as of October 17, 2006). The number of disclosures made by FINTRAC to foreign FIUs continues to increase.

	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007[1]	**Totals**
Spontaneous Disclosures	2	3	0	4	9	**18**
Disclosures in response to a Query	8	19	22	27	13	**89**

[1] Fiscal year 06-07 statistics include data up to October 17, 2006.

1606. At the time of the on-site visit, FINTRAC had received 264 requests from foreign FIUs and sent 46 requests to its counterparts (in Australia, Barbados, Bahamas, Belgium, Denmark, Japan, UK and USA).

1607. The number of queries from FINTRAC (46 since 2000-2001) to foreign FIUs is relatively low, taking into account that the majority of these queries were sent to one neighbouring country. FINTRAC has signed up to now 44 MOUs with foreign FIUs. Nevertheless, a wide range of these MOUs has been signed in 2005 (9) and 2006 (16). This could partly explain the low number of requests until now.

1608. The following tables provide an overview of requests received and made by OSFI to foreign counterparts.

Regulator's Country receiving request	**Reason**
Jamaica	Review of Canadian bank's subsidiary operations conducted by OSFI
Mexico	Review of Canadian bank's subsidiary operations conducted by OSFI
Cayman Islands	Review of Canadian banks' subsidiary operations conducted by OSFI
Jersey	Review of Canadian bank's subsidiary operations conducted by OSFI
Guernsey	Review of Canadian bank's subsidiary operations conducted by OSFI
Regulator's Country making request	
UK	Status of Canadian Banks' AML/CFT programs
Germany	Provide Results of OSFI's AML Review of German Bank's Canadian operations
USA	Provide Results of OSFI's AML Review of US Bank's Canadian operations

1609. No information exchanges (in either direction) have been refused. No statistics are kept by OSFI on the time requested to respond to a request initiated by its counterparts.

6.5.2 Recommendations and Comments

1610. *FINTRAC as a supervisory authority*. FINTRAC, if it is to act as a conduit for overseas supervisors to obtain information relating to AML/CFT compliance within the Canadian system, should rapidly enter into agreements with key supervisory counterparts in order to allow proper information sharing. This is necessary in order for FINTRAC to be in a position to render assistance to supervisory counterparts. This requirement is even more critical as a number of Canadian regulatory bodies (not including OSFI, the OSC, the IDA and the AMF) have not been given the explicit power to share AML/CFT information with overseas regulatory counterparts.

1611. Canadian Authorities may wish to consider removing the requirement in the PCMLTFA for formal arrangements or agreements between FINTRAC and foreign supervisory counterparts in order to provide international assistance on a more prompt and effective basis.

1612. Canadian Authorities should ensure that the MOUs established between FINTRAC and Canadian regulatory authorities make appropriate reference to the use of the information received in international requests. If there are requirements for the governing laws of the regulators to be changed to allow for international exchange of information, then this should be implemented.

6.5.3 Compliance with Recommendation 40 and Special Recommendation V

Rec.	Rating	Summary of factors underlying ratings
Rec.40	LC	*FINTRAC as a supervisory authority* • FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.
SR.V	LC	**Regarding compliance with Recommendation 40** *FINTRAC as a supervisory authority* • FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.

7. RESOURCES AND STATISTICS

7.1 Resources and Statistics (R. 30 & 32)

1613. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report *i.e.* all of Section 2, parts of sections 3 and 4, and in section 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report contains only the box showing the rating and the factors underlying the rating.

Rec.	Rating	Summary of factors underlying ratings
Rec.30	PC	*In relation to the FIU*: • The number of staff dedicated to the analysis of ML/TF cases is too low, especially considering the amount of reports coming in. *In relation to law enforcement agencies:* • The RCMP lacks resources to properly undertake ML/TF investigations. *In relation to the Department of Justice* • There seems to be very little if any coordinated or sophisticated training efforts in the forfeiture area. • The authorities in charge of processing MLA requests lack resources. *In relation to prosecution agencies:* • Insufficient training is provided for combating ML and TF. *In relation to supervisors:* • FINTRAC current internal organisation and resources dedicated to supervision are insufficient to allow it to perform its compliance function effectively.
Rec.32	LC	• Incomplete statistics are kept in relation to ML investigations. • Incomplete statistics are kept in relation to ML sentencing. • Statistics on confiscation are incomplete. • There is no data available on the time requested to respond to extradition and MLA requests. • No statistics are kept by OSFI on the time to respond to a request initiated by its counterparts.

7.2 Other relevant AML/CFT measures or issues

N/A

7.3 General framework for AML/CFT system

N/A

TABLES

Table 1. Ratings of Compliance with FATF Recommendations

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC), or could, in exceptional cases, be marked as not applicable (NA).

Forty Recommendations	Rating	Summary of factors underlying rating
Legal systems		
1. ML offence	LC	▪ The ML offence does not cover all designated categories of predicate offences (copyright related offences). ▪ Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions or R.1. ▪ The number of convictions for Section 462.31 ML is very low, as is the percentage of convictions in comparison to charges laid.
2. ML offence – mental element and corporate liability	LC	▪ The number of convictions for Section 462.31 ML is very low. ▪ Due to the lack of data on ML sentencing, is not possible to assess whether natural and legal persons are subject to effective, proportionate and dissuasive sanctions for ML.
3. Confiscation and provisional measures	LC	▪ The fine in lieu forfeiture provision does not fully and effectively meets the requirement for equivalent value provisions and does not apply to property held by third parties. ▪ Based on the limited quantitative and qualitative information available, it does not seem that the confiscation and seizure regime is fully effective, particularly with respect to value based confiscation.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	C	▪ The Recommendation is fully met.
5. Customer due diligence	NC	*Scope issue* ▪ the requirement to conduct CDD does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). *Numbered accounts* ▪ Although numbered accounts are permissible and used, there is no direct requirement to maintain them in such a way that full compliance can be achieved with the FATF Recommendations. *When CDD is required* ▪ There is no requirement to carry out CDD measures when there is a suspicion of ML or TF and when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data. ▪ Customer identification for occasional transactions that are cross-border wire transfers takes place for transactions above CAD 3 000. This threshold is currently too high and no equivalent requirement is in place for domestic wire transfers. *Required CDD measures* ▪ The current customer identification measures for natural persons are insufficient, especially in relation to non face-

Forty Recommendations	Rating	Summary of factors underlying rating
		to-face business relationships. *Identification of persons acting on behalf of the customer* ▪ The requirement to identify up to three persons who are allowed to give instructions in respect of an account is too limitative. *Third party determination and identification of beneficial owners* ▪ Except for IDA supervised entities, financial institutions are neither required to understand the ownership and control structure of the customer nor obliged to determine who are the natural persons that ultimately own or control the customer. *Purpose & intended nature of the business relationship* ▪ There are currently no requirements (except for securities dealers) to obtain information on the purpose and intended nature of the business relationship. *Ongoing Due Diligence* ▪ Except for securities dealers, there are currently no requirements to conduct ongoing due diligence on the business relationship although the need to identify customers for large cash transactions and electronic fund transfers provide certain automatic trigger points. ▪ Except for securities dealers financial institutions are not required to ensure that documents, data and information collected under the CDD process is kept up-to-date and relevant. *ML/FT risks – enhanced due diligence* ▪ There is no requirement to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction. *ML/FT risks – reduced or simplified due diligence* ▪ The current exemptions mean that, rather than reduced or simplified CDD measures, no CDD apply, which is not in line with the FATF standards. ▪ Exemptions from CDD and third party determination bring in very far reaching exceptions that introduce potential gaps in the customer identification process (especially the exemptions apply to financial entities that operate in FATF countries based on presumption of conformity only). ▪ There is no explicit provisions that set out that CDD or third party determination exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. ▪ Financial institutions, in certain circumstances, are given the permission to exempt from CDD requirements or third party determination obligations certain customers resident in another country. However, Canada has not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations. *Timing of verification* ▪ PCMLTF Regulations sets out unreasonable verification timelines to be carried out by certain financial sectors and/or in relation to certain customers. *Failure to satisfactorily complete CDD* ▪ Financial institutions (except securities dealers in some circumstances) are not prevented from opening an account or commencing business relationship or

Forty Recommendations	Rating	Summary of factors underlying rating
		performing a transaction and they are not required to make a suspicious transaction report. ▪ In situations where the financial institution has already commenced a business relationship but is unable to perform adequate CDD and establish beneficial ownership, there is no requirement to terminate the business relationship and to consider making a suspicious transaction report.
6. Politically exposed persons	NC	▪ There were no mandatory legislative or other enforceable requirements in relation to PEPs at the time of the on-site visit.
7. Correspondent banking	PC	▪ Financial entities are not required to assess the respondent institution's AML/CFT controls and to ascertain that these controls are adequate and effective. ▪ Financial institutions are not required to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of AML/CFT requirements) and the quality of supervision of that entity. ▪ In the context of payable through accounts, the respondent entity is not required to perform all the normal CDD obligations set out in Recommendation 5 on its customers that have direct access to the accounts of the correspondent institution in line with the FATF standards. ▪ The effectiveness of the measures in place cannot yet be assessed.
8. New technologies & non face-to-face business	NC	▪ There are no specific legislative or other enforceable obligations addressing the risks posed by the application of new technological developments. ▪ Financial institutions are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. ▪ No effective CDD procedures for non face-to-face customers are in place.
9. Third parties and introducers	NC	▪ In the only two scenarios where reliance on a third party or introduced business is legally allowed without an agreement or arrangement, the measures in place are insufficient to meet the FATF requirements. ▪ In addition to the two reliance on third parties/introduced business scenarios contemplated by the Regulations, the financial sector uses introduced business mechanisms as a business practice. However, no specific requirements as set out in Recommendation 9 apply to these scenarios.
10. Record keeping	LC	*Scope issue* ▪ The record keeping requirement does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). ▪ Financial institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which does not meet the requirement to make CDD records available on a *timely* basis to competent authorities, especially in normal business circumstances.
11. Unusual transactions	PC	▪ There is no explicit nor enforceable requirement for financial institutions to examine all complex, unusual large transactions under the current legislation (except for IDA members). Except for IDA members, the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ There is no explicit requirement to examine the background and purpose of these unusual transactions (except for IDA members). ▪ There is no requirement to keep record of financial institutions' findings in relation to complex, unusual large or unusual patterns of transactions.
12. DNFBP – R.5, 6, 8-11	NC	*Scope issue* ▪ Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the requirements under Recommendations 5, 6 and 8-11. *Application of Recommendation 5 to casinos* ▪ The requirements applicable to casinos are insufficient in relation to: (1) when CDD is required; (2) required CDD measures; (3) identification of persons acting on behalf of the customer; (4) third party determination and identification of beneficial owners ; (5) purpose & intended nature of the business relationship ; (6) ongoing Due Diligence; (7) ML/FT risks and (8) failure to satisfactorily complete CDD. *Application of Recommendation 5 to real estate brokers and sales representatives and accountants* ▪ The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification are too limitative. ▪ The CDD requirements that real estate agents and sales representatives and accountants are subject to are substantially very basic and extremely limited. *Application of Recommendation 6 to casinos, real estate brokers and sales representatives and accountants* ▪ Canada has not implemented any specific AML/CFT measures concerning PEPs that are applicable to DNFBPs. *Application of Recommendation 8 to casinos, real estate brokers and sales representatives, accountants* ▪ There are no specific legislative or other enforceable obligations for DNFBPs to take measures to prevent the misuse of technological developments in ML/TF schemes. ▪ The DNFBPs are not required to have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions. *Application of Recommendation 9 to casinos, real estate brokers and sales representatives and accountants* ▪ There are currently no provisions for DNFBPs that address the issue of relying on intermediaries or third parties to perform elements of the CDD process outside the outsourcing type of scenario. *Application of Recommendation 10 to casinos, real estate brokers and sales representatives and accountants* ▪ The circumstances in which real estate agents and sales representatives and accountants have to keep records are too limitative. ▪ Real estate agents and sales representatives, casinos and accountants institutions must ensure that all records required to be kept under the PCMLTFA can be provided within 30 days which is not in line with the FATF requirement to make CDD records available on a timely basis to competent authorities.

Forty Recommendations	Rating	Summary of factors underlying rating
		Application of Recommendation 11 to casinos, real estate brokers and sales representatives and accountants ▪ There is currently no explicit provision requiring that DNFBPs pay special attention to all complex, unusual large transactions that have no apparent or visible economic or lawful purpose (the monitoring obligation is implied and indirect (it flows from reporting suspicious transactions, large international electronic funds transfer and large cash transactions) and it does not cover the full range of monitoring situations as stipulated in Recommendation 11). The other requirements under Recommendation 11 are not met either.
13. Suspicious transaction reporting	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report. ▪ There is no requirement to report attempted transactions. ▪ The low numbers of STRs sent by certain financial sectors raise concerns in relation to the effectiveness of the reporting system.
14. Protection & no tipping-off	C	▪ The Recommendation is fully met.
15. Internal controls, compliance & audit	LC	▪ The requirement for internal controls does not extend to all financial institutions as defined by the FATF (notably financial leasing, factoring and finance companies). ▪ There is no mandatory explicit requirement to maintain up to date internal procedures, policies and controls and such policies do not include the detection of unusual and suspicious transactions. ▪ There is no explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information. ▪ There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance for small financial institutions (including some MSBs) for which a simple self-assessment is admitted. ▪ There is no general requirement concerning screening procedures when hiring employees.
16. DNFBP – R.13-15 & 21	NC	*Scope issue* ▪ Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and therefore are not subject to the suspicious transactions reporting requirements. *Application of Recommendation 13 to casinos, real estate brokers and sales representatives and accountants/accountant firms* ▪ The circumstances in which real estate agents and sales representatives and accountants have to report suspicious transactions under the PCMLTFA are too limited. ▪ Attempted transactions are not yet covered by the Suspicious Transaction Reporting requirement. ▪ The relatively low numbers of STRs sent by real estate agents/sales representatives and accountants raise significant concerns in relation to the effectiveness of the reporting system in these sectors. *Application of Recommendation 15 to casinos, real estate brokers and sales representatives and accountants/accountant firms* ▪ There is no explicit requirement to: (1) keep up to date internal procedures, (2) have policies to monitor for and detect unusual and suspicious transactions and (3) ensure that the AML/CFT compliance officer has timely access to

Forty Recommendations	Rating	Summary of factors underlying rating
		customer identification data and other CDD information, transactions records and other relevant information. ▪ There is no mandatory requirement for an independent audit function to test AML/CFT regime compliance. ▪ Except for casinos, there are no requirements concerning screening procedures when hiring employees. *Application of Recommendation 21 to casinos, real estate brokers and sales representatives and accountants/accountant firms* ▪ There is no general enforceable requirement for DNFBPs to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations but only through general guidance or advisories sent on a case by case basis. ▪ There are no effective measures in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. ▪ There is no requirement to examine the background and purpose of these transactions and to document the related findings.
17. Sanctions	PC	▪ With the exceptions of OSFI and IDA regulated institutions, only criminal sanctions are available to FINTRAC under the PCMLTFA for all other types of financial institutions and these are only applicable for the most serious failures, and need to be proved to the criminal standard. ▪ OSFI only uses a limited range of actions/sanctions in the AML/CFT context (namely supervisory letters and in a limited number of cases, staging). ▪ The lack of effective sanctions applied in cases of major deficiencies raises real concern in terms of effectiveness of the sanction regime, particularly taking into account that only one criminal sanction and a very limited number of administrative sanctions have been applied.
18. Shell banks	LC	▪ Financial entities are not required to terminate business relationships with shell banks, nor with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. ▪ The effectiveness of the measures in place cannot yet be assessed.
19. Other forms of reporting	C	▪ The Recommendation is fully met.
20. Other NFBP & secure transaction techniques	C	▪ The Recommendation is fully met.
21. Special attention for higher risk countries	PC	▪ There is no general enforceable requirement for financial institutions to give special attention to transactions or business relationships connected with persons from or in countries which do not or insufficiently apply the FATF Recommendations. ▪ There are no effective measures in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems. ▪ There is no requirement to examine the background and purpose of these transactions and to document the related findings.
22. Foreign branches & subsidiaries	NC	▪ Currently, the PCMLTFA and PCMLTF Regulations contain no explicit enforceable provision requiring financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements although foreign branches of Canadian financial institutions are Canadian entities under the Bank Act and the Insurance Companies Act that are subject to Canadian laws.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ There is no requirement that particular attention be paid to branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendations. ▪ There is no legal obligation in the PCMLTFA and PCMLTF Regulations that, where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (*i.e.* host country) laws and regulations permit. ▪ There is no requirement that financial institutions be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (*i.e.* host country) laws, regulations or other measures.
23. Regulation, supervision and monitoring	PC	▪ Exclusion from the AML/CFT regime of certain financial sectors (such as financial leasing, factoring, finance companies, etc.) without proper risk assessments. ▪ For the financial institutions subject to the PCMLTFA, there is a very unequal level of supervision of AML/CFT compliance, with certain categories of financial institution appearing to be insufficiently controlled (MSBs, certain credit unions/*caisses populaires*, life insurance intermediaries…). This is due to the limited staff resources of FINTRAC dedicated to on-site assessments compared to the high number of reporting entities, which has not always been compensated by the involvement of the primary prudential regulators in AML/CFT issues. ▪ "Fit and proper" requirements are not comprehensive. ▪ At the time of the on-site visit, there was no specific obligation for FRFIs to implement screening procedures for persons who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. ▪ There is currently no registration regime for MSBs.
24. DNFBP - regulation, supervision and monitoring	NC	*Scope issue* ▪ Lawyers, Quebec Notaries, BC Notaries, dealers in precious metals and stones, Internet casinos, ship based casinos and TCSPs are not captured by the PCMLTFA and not subject to FINTRAC supervision. *Supervision of casinos* ▪ The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the grounds of AML/CFT non-compliance issues have been made available to the assessment team. *Supervision of other DNFBPs* ▪ Limited staff resources deprives FINTRAC from closely and efficiently monitoring DNFBPs' compliance with the PCMLTFA requirements especially in sectors/provinces where the primary regulators or SROs are not or insufficiently involved in AML/CFT compliance supervision. ▪ The sanction regime available to FINTRAC is currently inadequate (see conclusions in relation to Rec. 17). Provincial regulators may have administrative sanctions at their disposal but there is no evidence that these are dissuasive, effective and proportionate, since no data or statistics regarding sanctions taken by these regulators on the ground of AML/CFT non-compliance issues have been

Forty Recommendations	Rating	Summary of factors underlying rating
		made available to the assessment team.
25. Guidelines & Feedback	LC	▪ There is a lack of specific guidelines intended for sectors such as life insurance companies and intermediaries. ▪ There is not enough general feedback given outside the large financial institutions sector.
Institutional and other measures		
26. The FIU	PC	▪ FINTRAC has insufficient access to intelligence information from administrative and other authorities (especially from CRA , CSIS and Customs). ▪ FINTRAC is not allowed by the PCMLTFA to gather additional financial information from reporting entities. ▪ Effectiveness: (1) the number of staff dedicated to the analysis of potential ML/FT cases is low especially in comparison with the amount of reports coming in, which may have an impact on the number of cases that FINTRAC generate; (2) feedback from law enforcement authorities outlines the relatively limited added value of FINTRAC disclosures in law enforcement investigations; (3) the timeliness of FINTRAC disclosures to law enforcement authorities was raised as an issue at the time of the on-site visit; (4) 80% of the disclosures made by FINTRAC result from voluntary information from law enforcement; only 20% result from STRs which raises serious concerns with respect to the capability of FINTRAC to generate ML/TF cases on the basis of STRs or other reports it receives from the private sector; (5) so far, very few if any convictions for ML or TF have resulted from a FINTRAC disclosure which is an additional factor to consider when looking at FINTRAC's ability to produce intelligence to be used in criminal investigations and prosecutions.
27. Law enforcement authorities	LC	▪ The RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations.
28. Powers of competent authorities	C	▪ The Recommendation is fully met.
29. Supervisors	LC	▪ FINTRAC has no power to impose administrative sanctions.
30. Resources, integrity and training	PC	*In relation to the FIU*: ▪ The number of staff dedicated to the analysis of ML/TF cases is too low, especially considering the amount of reports coming in. *In relation to law enforcement agencies:* ▪ The RCMP lacks resources to properly undertake ML/TF investigations. *In relation to the Department of Justice* ▪ There seems to be very little if any coordinated or sophisticated training efforts in the forfeiture area. ▪ The authorities in charge of processing MLA requests lack resources. *In relation to prosecution agencies:* ▪ Insufficient training is provided for combating ML and TF. *In relation to supervisors:3* ▪ FINTRAC current internal organisation and resources dedicated to supervision are insufficient to allow it to perform its compliance function effectively.
31. National co-operation	LC	▪ Interagency cooperation between the FIU and law enforcement authorities is not fully effective and needs to be enhanced.
32. Statistics	LC	▪ Incomplete statistics are kept in relation to ML investigations. ▪ Incomplete statistics are kept in relation to ML sentencing.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ Statistics on confiscation are incomplete. ▪ There is no data available on the time requested to respond to extradition and MLA requests. ▪ No statistics are kept by OSFI on the time to respond to a request initiated by its counterparts.
33. Legal persons – beneficial owners	NC	▪ There is no requirement to ensure adequate transparency, for instance there is no obligation that information on the beneficial ownership of shares in legal persons is required to be collected by either the corporate registry, within corporate records held by legal persons or by lawyers, accountants or TCSPs. ▪ While law enforcement and other authorities have sufficient powers, those powers are not adequate to ensure the existence of adequate, accurate and timely information on the beneficial ownership of legal persons, which can be accessed or obtained in a timely fashion by competent authorities. ▪ There are no measures to ensure that bearer shares are not misused for ML, particularly for private corporations.
34. Legal arrangements – beneficial owners	PC	▪ There are limited and indirect legal requirements to obtain, verify, or retain information on the beneficial ownership and control of trusts and fiducie in Québec. ▪ While the investigative powers are generally sound and widely used, there is minimal information that is adequate, accurate and timely concerning the beneficial owners of trusts and fiducie in Québec that can be obtained or accessed by the competent authorities in a timely fashion. Where some information is held, such as by CRA, there are limits on the circumstances in which information on trusts can be shared.
International Co-operation		
35. Conventions	LC	*Implementation of the Palermo and Vienna Conventions:* ▪ Canada has ratified the Palermo and Vienna Conventions and implemented them with some omissions however (the ML offence does not cover all required categories of predicate offences and Section 462.31 ML offence contains a purposive element that is not broad enough to meet the requirements of the Conventions). *Implementation of the CFT Convention:* ▪ Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.
36. Mutual legal assistance (MLA)	LC	▪ There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data.
37. Dual criminality	C	▪ The Recommendation is fully met.
38. MLA on confiscation and freezing	LC	▪ There are doubts about the effectiveness of the measures in place under Recommendation 38: there is limited evidence of effective confiscation assistance as only four cases have been successful in last 5 years and international sharing statistics indicate that while asset sharing with foreign states is possible, it rarely occurs. Canada executes requests to enforce corresponding value judgments as fines, which has limitations and cannot be enforced against property held by third parties.
39. Extradition	LC	▪ Insufficient statistical data was provided to make a thorough assessment, particularly the assessment of the delay element, but even the limited data provided indicates that obtaining extradition from Canada quickly may be

Forty Recommendations	Rating	Summary of factors underlying rating
		difficult.
40. Other forms of co-operation	LC	*FINTRAC as a supervisory authority* ▪ FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.
Nine Special Recommendations	**Rating**	**Summary of factors underlying rating**
SR.I Implement UN instruments	LC	*Implementation of the CFT Convention:* ▪ Article 18(1)(b) of the Convention, which requires countries to implement efficient measures to identify customers in whose interest accounts are opened is insufficiently implemented. Canada's implementation of Recommendation 5 does not include adequate measures to ascertain the identity of beneficial owners.
SR.II Criminalise terrorist financing	LC	▪ The lack of any TF convictions and the very limited number of prosecutions shows that the offence has not yet been fully and effectively used.
SR.III Freeze and confiscate terrorist assets	LC	▪ The actions taken to communicate the names of listed persons or entities do not cover all types of financial institutions and the lists are not effectively communicated to other types of asset holders. ▪ With the exception of guidance given to federally regulated financial institutions (and copied to provincial regulators/SROs), Canada has issued insufficient guidance to other financial institutions and DNFBPs that may be holding funds of other assets concerning their obligations in taking action under freezing mechanisms. This may have an impact on Canada's ability to freeze terrorist funds or other assets for such entities without delay. ▪ The existing measures to effectively monitor the compliance with the legislation governing the obligations under SRIII are insufficient (except for federally regulated financial institutions supervised by OSFI).
SR.IV Suspicious transaction reporting	LC	▪ Some financial institutions as defined by the FATF (especially financial leasing, finance companies, providers of e-money) are not covered by the obligation to report. ▪ There is no requirement to report attempted transactions.
SR.V International co-operation	LC	**Regarding compliance with Recommendation 38** ▪ All elements missing in R. 38 are missing for SR.V. ▪ There are concerns about the ability of Canada to handle MLA requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data. **Regarding compliance with Recommendation 39** ▪ No meaningful statistical data provided to assess delay element (effectiveness issue). **Regarding compliance with Recommendation 40** *FINTRAC as a supervisory authority* ▪ FINTRAC has the legal capacity to exchange information with foreign counterparts but has not yet put the arrangements and agreements in place.
SR VI AML requirements for money/value transfer services	NC	▪ There is no registration regime for MSBs as contemplated by SR VI. ▪ Overall, requirements and implementation of Recommendations 4-11, 21-23 and SR. VII is inadequate which has a significant negative impact on the effectiveness of AML/CFT measures for money transmission services. ▪ MSBs are not required to maintain a list of their agents.

Forty Recommendations	Rating	Summary of factors underlying rating
		▪ The sanction regime available to FINTRAC and applicable to MSBs is not effective, proportionate and dissuasive.
SR VII Wire transfer rules	NC	▪ Canada has not implemented SRVII.
SR.VIII Non-profit organisations	LC	▪ The existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications is insufficient to fully address the risk in some segments of the NPO sector.
SR.IX Cross Border Declaration & Disclosure	C	▪ The Recommendation is fully met.

Table 2: Recommended Action Plan to Improve the AML/CFT System

AML/CFT System	Recommended Action (listed in order of priority)
1. General	
2. Legal System and Related Institutional Measures	
Criminalisation of Money Laundering (R.1 &, 2)	▪ Canada should cover all designated categories of predicate offences. ▪ Canada should amend Section 462.31 ML offence (in relation to the intent mental element) in order to fully met the requirements of the Conventions or Recommendation 1. ▪ Canada should ensure that the statutes available for countering ML are effectively used. ▪ Canada should develop a more proactive approach to prosecuting the specific money laundering charge under s.462.31.
Criminalisation of Terrorist Financing (SR.II)	▪ Canada should pay attention to the overall effectiveness of the TF offence and regime and ensure that the TF offence is effectively used.
Confiscation, freezing and seizing of proceeds of crime (R.3)	▪ Canada should review the fine in lieu forfeiture provision to be in line with the FATF requirements. ▪ Canada should ensure that the confiscation and seizure regime is fully effective, particularly with respect to value based confiscation.
Freezing of funds used for terrorist financing (SR.III)	▪ There needs to be more communication on listed persons provided to certain categories of financial institutions and other potential asset holders as well more clear and practical guidance to reporting entities (including DNFBPs and MSBs) that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms. ▪ Canada should enhance the existing measures to monitor the compliance with the legislation governing the obligations under SRIII (except for federally regulated financial institutions supervised by OSFI).
The Financial Intelligence Unit and its functions (R.26 & 30)	▪ FINTRAC should be able to obtain additional financial information from the reporting entities, especially during the analytical process. ▪ FINTRAC should be authorised to have access to more intelligence data from CSIS, CRA and the Canadian Customs Agency to reinforce its analytical work. ▪ Canada should examine FINTRAC effectiveness in disclosing ML/TF cases to law enforcement authorities. ▪ Canada should ensure that FINTRAC has sufficient analysts that are in charge of developing ML/TF cases and processing disclosures to law enforcement authorities for further investigations.
Law enforcement, prosecution and other competent authorities (R.27 & 28)	▪ Canada should ensure that the RCMP gets sufficient resources that would allow it to focus on a larger spectrum of ML/TF investigations.
Cross Border declaration or disclosure (SR.IX)	▪ There are no recommendations for this section.
3. Preventive Measures – Financial Institutions	
Risk of money laundering or terrorist financing	▪ Canada should rely on a more comprehensive, thorough and formal risk assessment process. The underlying principle should be that the financial activities referred to in the FATF standards should be covered unless there is a proven low risk of ML/TF.
Customer due diligence, including enhanced or reduced measures (R.5 to 8)	*In relation to Recommendation 5:* ▪ With regard to numbered or confidential accounts, Canada should consider adopting detailed rules or guidance on the use of such accounts by financial institutions. Such rules should clearly set out the obligation for compliance officers to have access to CDD information.

AML/CFT System	Recommended Action (listed in order of priority)
	▪ New provisions will come into force in 2008 with regard to the circumstances where financial institutions have to perform customer identification. Canada should ensure that the new provisions are fully in line with the FATF requirements. ▪ With regard to the identification measures for natural persons, Canada should ensure that only reliable CDD documentation is acceptable, especially in non face-to-face situations. Canada should consider introducing additional requirements for identifying foreign customers. ▪ New provisions will come into force in June 2008 with regard to identification of beneficial owners. Canada should ensure that the new provisions are fully in line with the FATF requirements and are properly implemented by all financial institutions. ▪ The requirement to identify up to three persons who are authorised to give instructions in respect of an account should be extended to any person purporting to act on behalf of the customer. ▪ The PCMLTF Regulations, enacted in June 2007 and coming into force in June 2008 require financial entities to keep a record of the intended use of the account. Canada should ensure that such requirement is implemented by all financial institutions in line with the FATF standards. ▪ Based on the provisions adopted in June 2007 and coming into force in 2008, Canada should ensure that financial institutions fully implement the obligation to conduct ongoing due diligence on the business relationship and ensure all documents, data and information collected under the CDD process in line with the FATF standards (as it is already the case for securities dealers) are kept up-to-date and relevant. ▪ In relation to ML/FT risks, Canada should ensure that financial institutions perform enhanced due diligence for higher risk categories of customer, business relationship or transaction once the new regulations enter into force in June 2008. This should be done in line with the FATF standards. Current scenarios of full exemptions from CDD and third party determination should be subject to simplified or reduced CDD. Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that Canada is satisfied are in compliance with and have effectively implemented the FATF recommendations (*i.e.* Canada should not rely on presumption of conformity of FATF countries for instance). Canada should adopt explicit provisions that set out that such exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply. Canada should consider developing guidelines for financial institutions that are permitted to determine the extent of the CDD measures on a risk sensitive basis. ▪ With regard to the timing of customer's identity verification, new regulations that will enter into force in June 2008 should be implemented in line with the FATF standards and Canada should consider adopting shorten timelines in the insurance, foreign exchange, MSBs and securities sectors for corporations' or entities' identification, especially in normal business circumstances. *In relation to Recommendation 6*: ▪ Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. *In relation to Recommendation 7:* ▪ Canada should require financial entities to assess the respondent institution's AML/CFT controls and to ascertain

AML/CFT System	Recommended Action (listed in order of priority)
	that these controls are adequate and effective. ▪ Institutions should also be required to determine the reputation of the foreign financial entity (other than take reasonable measures to ascertain whether there are any civil or criminal penalties that have been imposed on the foreign financial institution in respect of AML/CFT requirements) and the quality of supervision of that entity. ▪ In the context of payable through accounts, the respondent entity should be required to perform all customer identification in line with the FATF standards. ▪ Canada should ensure that reporting entities implement measures that meet the FATF standards. *In relation to Recommendation 8:* ▪ Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards.
Third parties and introduced business (R.9)	▪ Since introduced business arrangements exist in Canada in other circumstances than those captured by Sections 56(2) and 57(5) of the PCMLTF Regulations, Canada should adopt provisions that address all aspects of Recommendation 9 and ensure that financial institutions implement them.
Financial institution secrecy or confidentiality (R.4)	▪ There are no recommendations for this section.
Record keeping and wire transfer rules (R.10 & SR.VII)	*In relation with Recommendation 10:* ▪ Canada should ensure that all types of transactions (including business correspondence) carried out by financial institutions (except for IDA members) are subject to proper record keeping requirements that permit their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. ▪ Canada should ensure that all customer and transactions records and information are available on a timely basis to domestic competent authorities. *In relation with SRVII:* ▪ Canada should ensure that the new provisions enacted in December 2006 and coming into force in June 2008 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. ▪ Canada should ensure that the wire transfers operated by casinos outside the banking network are subject to equivalent requirements.
Monitoring of transactions and relationships (R.11 & 21)	*In relation with Recommendation 11:* ▪ Canada should ensure that the new provisions enacted in June 2007 are fully in line with the FATF requirements and ensure that reporting entities implement measures that meet the FATF standards. *In relation with Recommendation 21:* ▪ The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to all financial institutions. ▪ Effective measures should be put in place whereby financial institutions are advised of other countries that have specific weaknesses in their AML/CFT systems. This should be completed by a provision requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

AML/CFT System	Recommended Action (listed in order of priority)
Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	*In relation with Recommendation 13 & SRIV* ▪ All financial institutions covered by the definition of the FATF should be subject to the suspicious transactions reporting requirement unless a proven low risk of ML and FT is established in the sectors that are currently exempted. ▪ Canada should ensure that the different categories of financial institutions contribute more equally to the total number of STRs received by FINTRAC. *In relation with Recommendation 14* ▪ There are no recommendations for this section. *In relation with Recommendation 19* ▪ There are no recommendations for this section. *In relation with Recommendation 25* ▪ FINTRAC should develop more general feedback for smaller reporting entities.
Internal controls, compliance, audit and foreign branches (R.15 & 22)	*In relation to Recommendation 15* ▪ The current requirements should be expanded, made more explicit and enforceable, in particular (1) written policies and procedures should be explicitly required, and should be kept up to date, and their minimum mandatory content should include the detection of unusual and suspicious transactions; (2) there should be an explicit requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information; (3) the requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened for MSBs and small financial institutions, and made more explicit generally; (4) Canada should impose screening procedures when hiring employees for financial institutions. *In relation to Recommendation 22* ▪ Canada should ensure that the provisions in relation to Recommendation 22 that will enter into force in June 2008 are in line with the FATF requirements and are properly implemented by all financial institutions.
Shell banks (R.18)	▪ Canada should adopt a requirement for financial entities to terminate business relationships with shell banks as well as with any foreign financial institution that has, directly or indirectly, correspondent banking relationships with shell banks. ▪ Canada should ensure that the measures adopted in relation to shell banks are fully implemented by financial institutions.
The supervisory and oversight system - competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 30, 29, 17 & 25)	*In relation to Recommendation 17, 23 & 29* ▪ Canada should ensure a proper and effective implementation of the regime of administrative and monetary penalties and ensure that competent authorities put in place effective, proportionate and dissuasive sanctions. ▪ Canada should implement a more equal level of supervision of AML/CFT compliance vis-à-vis certain categories of financial institution (MSBs, certain credit unions/*caisses populaires*, life insurance intermediaries…). ▪ Canada should ensure that "fit and proper" requirements are in place. ▪ Canada should adopt screening procedures for persons who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded. ▪ Canada should implement the registration regime for MSBs. *In relation to Recommendation 25* ▪ Canada should provide more specific guidelines for sectors such as life insurance companies and intermediaries.

AML/CFT System	Recommended Action (listed in order of priority)
Money value transfer services (SR.VI)	▪ Canada should ensure effective implementation of the registration system for MSBs in force in June 2008 and ensure that the requirements applicable to MSBs fully meet the FATF requirements.
4. Preventive Measures –Non-Financial Businesses and Professions	
Customer due diligence and record-keeping (R.12)	▪ All DNFBPs as defined by the FATF should be subject to the AML/CFT regime. ▪ The circumstances in which real estate agents and sales representatives and accountants have to carry out customer identification and keep records should be extended to be in line with the types of activities targeted under Recommendation 12. *In relation to Recommendation 5:* ▪ Canada should ensure that the entire set of requirements under Recommendation 5 apply to all non-financial professions. *In relation to Recommendations 6, 8, 9 and 11:* ▪ Canada should require the non-financial professions to implement requirements in relation to Recommendations 6, 8, 9 and 11. *In relation to Recommendation 10:* ▪ Canada should ensure that all types of transactions carried out by the non-financial professions are subject to proper record keeping requirement that permits their reconstruction so as to provide, if necessary, evidence for prosecution of criminal activity. ▪ Canada should ensure that all customer and transactions records and information collected by the non-financial professions are available on a timely basis to domestic competent authorities.
Suspicious transaction reporting (R.16)	*In relation to Recommendation 13:* ▪ All DNFBPs as defined by the FATF should be subject in Canada to the suspicious transactions reporting requirement in all circumstances defined in Recommendation 16. *In relation to Recommendation 15:* ▪ The current requirements should be expanded, specified and enforced, especially: (1) the policies and procedures should be required to be written and their minimum mandatory content should include the detection of unusual and suspicious transactions for all DNFBPs; (2) there should be a requirement to ensure that the AML/CFT compliance officer has a timely access to customer identification data and other CDD information, transactions records and other relevant information; (3) the requirement for an independent audit function (internal or external) to test on a regular basis the compliance of the AML regime should be strengthened; (4) Canada should impose screening procedures when hiring employees to DNFBPs. *In relation to Recommendation 21*: ▪ The requirement to give special attention to business relationships or transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be included in an enforceable legal instrument applicable to DNFBPs. ▪ Effective measures should be put in place whereby DNFBPs are advised of other countries that have specific weaknesses in their AML/CFT systems. ▪ Finally a provision should be introduced requiring that the background and purpose of such transactions having no apparent economic or visible lawful purpose be examined and the findings documented.

AML/CFT System	Recommended Action (listed in order of priority)
Regulation, supervision and monitoring (R.24-25)	▪ All DNFBPs as defined by the FATF should be subject to the AML/CFT regime. ▪ Canada should ensure that supervisory action (especially on-site examinations) vis-à-vis casinos, but more importantly with respect to all other DNFBPs is strongly reinforced. ▪ The role, functions and monitoring powers of other regulators and SROs in ensuring compliance of DNFBPs with the AML/CFT requirements should be clarified. ▪ Canada should consider revisiting the supervision issue as a whole and give further consideration on whether FINTRAC should be the only authority in charge of ensuring compliance with the AML/CFT requirements. ▪ The sanction regimes applicable to DNFBPs, including casinos, should be reinforced and Canada should ensure that the sanctions available for failures to apply AML/CFT requirements are effective, proportionate and dissuasive.
Other designated non-financial businesses and professions (R.20)	▪ There are no recommendations for this section.
5. Legal Persons and Arrangements & Non-Profit Organisations	
Legal Persons – Access to beneficial ownership and control information (R.33)	▪ Canada should adopt further requirements to prevent the unlawful use of legal persons in relation to ML and TF. ▪ Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal persons on a timely basis. ▪ Canada should adopt measures to ensure that bearer shares are not misused for ML, particularly for private corporations.
Legal Arrangements – Access to beneficial ownership and control information (R.34)	▪ Canada should ensure that competent authorities have access to accurate and current information on the ultimate beneficial owners and controllers of all legal arrangements on a timely basis. ▪ Canada should implement measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts and fiducie in Québec.
Non-profit organisations (SR.VIII)	▪ Canada should improve the existing co-ordination mechanisms between competent authorities, especially between the CRA and the parties responsible for listing and freezing applications.
6. National and International Co-operation	
National co-operation and coordination (R.31)	▪ Canada should enhance interagency cooperation between the FIU and law enforcement authorities.
The Conventions and UN Special Resolutions (R.35 & SR.I)	▪ Canada should ensure that the ML offence does cover all designated categories of predicate offences and Canada should consider removing the purpose element from Section 462.31 of the CC to be in line with the UN Conventions. ▪ Canada should enact stronger measures to customer identification so as to be more compliant with Article 18(1)(b) of the CFT Convention.
Mutual Legal Assistance (R.36-38, SR.V)	▪ Canada should ensure that MLA requests are handled in a timely and effective manner. ▪ Canada should consider ways to improve the mechanisms to respond to foreign confiscation requests.
Extradition (R.39, 37, SR.V)	▪ Canada should ensure that extradition requests are handled in a timely and effective manner.
Other Forms of Co-operation (R.40, SR.V)	▪ FINTRAC should rapidly enter into agreements with key supervisory counterparts in order to allow proper information sharing.
7. Resources and Statistics	
Resources of Competent Authorities (R.30)	*In relation to the FIU*: ▪ FINTRAC should increase the number of staff dedicated to the

AML/CFT System	Recommended Action (listed in order of priority)
	analysis of ML/TF cases. *In relation to law enforcement agencies:* ▪ Canada should increase the resources of the RCMP in relation to ML/TF investigations. *In relation to the Department of Justice* ▪ Canada should put in place more sophisticated training efforts in the forfeiture area. ▪ The authorities in charge of processing MLA requests should be given more resources. *In relation to prosecution agencies:* ▪ More training should be provided for combating ML and TF. *In relation to supervisors:* ▪ Resources of FINTRAC to carry out its supervision duties should increase.
Statistics (R.32)	▪ Canada should collect more statistics in relation to ML investigations. ▪ Canada should collect more statistics in relation to ML sentencing. ▪ Canada should collect more statistics on confiscation. ▪ Canada should collect more data on the time requested to respond to extradition and MLA requests. ▪ OSFI should collect more statistics on the time to respond to a request initiated by its counterparts.

Table 3: Authorities' Response to the Evaluation

Relevant sections and paragraphs	Country Comments
General	Legislative amendments to the PCMLTFA passed in December 2006 and associated regulations enacted in June 2007 and December 2007 will address a substantial number of deficiencies identified in this report. Please see Annex 1 for a detailed list of legislative and regulatory amendments to Canada's AML/CFT regime that came into force after June 2007 and have not been considered in this evaluation. Canada's regulations allow a period of time between enactment and coming into force to provide an opportunity for businesses and sectors to modify systems.
Section 2.5	Recommendation 26 Canada believes that a partially compliant rating does not adequately reflect Canada's legal reality and FINTRAC's sophisticated organisation. First, it should be noted that, in order to safeguard Canadians' rights under the *Canadian Charter of Rights and Freedoms,* FINTRAC has no investigative powers. FINTRAC is not able to request further information directly from reporting entities for analysis purposes as this activity corresponds to investigative powers. There is therefore a clear constitutional impediment to requesting additional information and this should have been properly reflected in the analysis. Second, FINTRAC is effective in receiving, analysing and disclosing information to competent authorities: • FINTRAC has one of the most sophisticated FIU information technology systems in the world. Its unique technology-driven approach to analysis permits effective analysis of large volumes of transactions by its 36 tactical financial analysts. As the report notes in para 371, total staff at FINTRAC is "more than adequate". • The report notes in para 388 that FINTRAC disclosures provide added value to recipients in terms of identifying new leads and contributing to investigations. • The timeliness of disclosures is an issue that has been addressed by FINTRAC, as indicated in feedback received since 2006 and has also been improving, as noted in para 391. • Disclosures related to voluntary information (VIRs) demonstrate FINTRAC's responsiveness to the investigative priorities identified by law enforcement. • Like many FIUs, FINTRAC is not responsible for investigation or prosecution of cases. As such, it is not appropriate that its effectiveness be measured on the basis of convictions for ML/TF.
Section 2.5	Recommendation 30 Canada believes that a partially compliant rating does not adequately reflect the situation of resources in Canadian authorities, in particular those of FINTRAC. FINTRAC has one of the world's most sophisticated FIU IT systems, which supports the analysis of STRs and other transactions. 35 analysts conduct the analysis of financial transactions to develop FINTRAC disclosures. The work of these analysts is supported by FINTRAC's 80 information technology staff through, for example, the electronic filing of all report data, matching software that links incoming reports to current/former cases and other reports in the system based on a variety of data elements (*e.g.* name, account number, address, etc.), and tools that permit efficient database searches and case compilation. FINTRAC designed its compliance program based on a sophisticated risk-based model and has staffed the appropriate number of compliance officers to carry out the supervisory activities required to discharge its mandate of ensuring compliance with the PCMLTFA. As the report notes in para 371, total staff at FINTRAC is "more than adequate".
Sections 3.1-3.2	Recommendation 5 Canada believes that a non compliant rating clearly fails to recognize the broad-based record-keeping and client identification measures that have been in place in Canada since 2002. In addition, OSFI, the IDA and FINTRAC have issued and enforced guidance on implementation. Regulatory amendments enacted in June 2007 introduce enhanced customer due diligence provisions that come fully into force in June 2008. These provisions will further reinforce compliance with this recommendation and address most deficiencies identified.

Relevant sections and paragraphs	Country Comments
Section 3.2	Recommendation 6 Regulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.2	Recommendation 8 Rregulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.3	Recommendation 9 Canada believes that the report fails to recognize that there are only two specific situations where no written agreements are necessary for Canadian financial institutions to rely on another entity to identify their customers. When reliance is done through written agreements, Canada believes that these relationships fall outside the scope of Recommendation 9. In addition, a clarifying provision in the regulations enacted in June 2007 which come into force in June 2008 will address deficiencies identified.
Section 3.5	Special Recommendation VII Legislative and regulatory provisions enacted in June 2007 which come into force in June 2008 address deficiencies identified.
Section 3.6	Recommendation 11 Regulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.6	Recommendation 21 Regulatory provisions enacted in June 2007 which come into force in June 2008 address the deficiencies identified.
Section 3.8	Recommendation 22 Canada believes that the report fails to recognize that the Bank Act currently applies to bank branches outside Canada. As the PCMLTFA applies to banks, it also *de facto* applies to foreign bank branches. Legislative amendments enacted in December 2006 and coming into force in June 2008 will make it explicit that the PCMLTFA applies to foreign branches and subsidiaries.
Section 3.10	Recommendation 23 Canada believes that a partially compliant rating does not adequately reflect the supervisory situation in Canada. OSFI and FINTRAC have been effectively enforcing AML/CFT requirements for years. FINTRAC designed its compliance program based on a sophisticated risk-based model and has staffed the appropriate number of compliance officers to carry out the supervisory activities required to discharge its mandate of ensuring compliance with the PCMLTFA.
Section 3.10	Recommendation 17 Legislative amendments enacted in December 2006 and regulatory provisions implementing an administrative monetary penalty regime enacted in December 2007 which come into force in December 2008 address the gaps in compliance with this recommendation.
Section 3.11	Special Recommendation VI MSBs have been subject to broad-based reporting, CDD, and record keeping requirements since 2001. These obligations are being further expanded in regulations enacted in June 2007 which come into force in June 2008. There has been effective compliance monitoring of the sector by FINTRAC. Legislative amendments enacted in December 2006 and regulatory provisions enacted in June 2007 will establish an MSB registration regime as of June 2008.
Section 4.1	Recommendation 12 Casinos, accountants and real estate agents have been subject to some CDD and record-keeping requirements since 2001. Regulations enacted in June 2007 which come into force in June 2008 will expand requirements for these sectors. New regulations enacted in December 2007 and coming into force in December 2008 cover additional DNFBP sectors, thereby further addressing deficiencies identified. Regarding Internet and cruise ship casinos, it should be noted that Internet casinos

Relevant sections and paragraphs	Country Comments
	are illegal under the Criminal Code and enforcement action has been taken. There are no Canadian flagged ships operating casinos and shipboard casinos are subject to restrictions to limit access and abuse.
Section 4.2	Recommendation 16 Casinos, accountants and real estate agents have been subject to suspicious transaction reporting requirements since 2001. Regulations enacted in December 2007 which come into force in December 2008 will expand these requirements to cover additional DNFBP sectors, thereby further addressing deficiencies identified.
Section 4.3	Recommendation 24 Supervision mechanisms have been in place since 2001 for the casino, real estate and accounting sectors. Legislative amendments enacted in December 2006 and regulatory provisions enacted in December 2007 which come into force in December 2008 will further address deficiencies.

ANNEX 1

Legislative and regulatory Changes to the Canadian AML/CFT regime

Amendment	Legislation Enacted	Regulations Enacted	Measure Fully In Force
Extending record retention time period for FINTRAC	Dec 14, 2006	n/a	Feb 10, 2007
Enhanced information sharing on non-profit organisations	Dec 14, 2006	n/a	June 30, 2007
Enhanced FINTRAC disclosure information	Dec 14, 2006	June 27, 2007	June 30, 2007
Prohibition against correspondent relationships with shell banks	Dec 14, 2006	June 27, 2007	June 30, 2007
Correspondent banking due diligence requirements	Dec 14, 2006	June 27, 2007	June 30, 2007
Explicit prohibition on opening accounts for unidentified customers	Dec 14, 2006	n/a	June 23, 2008
Application to foreign branches or subsidiaries	Dec 14, 2006	n/a	June 23, 2008
Non-face-to-face CDD measures	n/a	June 27, 2007	June 23, 2008
Use of an agent or mandatary for customer identification (clarifying provision)	n/a	June 27, 2007	June 23, 2008
Beneficial owner requirements	n/a	June 27, 2007	June 23, 2008
Enhancing CDD and Record Keeping	Dec 14, 2006	June 27, 2007	June 23, 2008
PEPs requirement for financial institutions	Dec 14, 2006	June 27, 2007	June 23, 2008
Special attention to complex and unusual transactions (*i.e.* risk assessment)	Dec 14, 2006	June 27, 2007	June 23, 2008
Reporting suspicious attempted transactions	Dec 14, 2006	June 27, 2007	June 23, 2008
Special attention to business from countries of risk (*i.e.* risk assessment)	Dec 14, 2006	June 27, 2007	June 23, 2008
MSB registration	Dec 14, 2006	June 27, 2007	June 23, 2008
Wire transfers travel rule	Dec 14, 2006	June 27, 2007	June 23, 2008
Enhancing measures for casinos, accountants and real estate, including: • Enhanced CDD and record-keeping. • Non face to face measures. • Use of agent and mandatary. • Special attention to transactions.	Dec 14, 2006	June 27, 2007	June 23, 2008
Inclusion of Lawyers, BC Notaries and Jewellers, including measures on: • CDD and record-keeping. • Non face to face measures. • Use of agent and mandatary. • Special attention to transactions. • Triggers for STR reporting (except lawyers). • Coverage by FINTRAC to ensure compliance.	Dec 14, 2006	Dec 2007	Dec 2008
Administrative Monetary Penalties provisions	Dec 14, 2006	Dec 2007	Dec 2008
Application to businesses and professions at risk (real estate developers)	n/a	Feb 2008	Feb 2009

Appendix M:

FATF, *6th Follow-Up Report: Mutual Evaluation of Canada* (Paris: FATF, 2014)

FATF

6TH FOLLOW-UP REPORT

Mutual Evaluation of Canada

February 2014

Appendix M

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

CONTENTS

ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
AMP	Administrative Monetary Penalties
CAR	Compliance Assessment Report
CBSA	Canada Border Services Agency
CDD	Customer Due Diligence
CRA	Canada Revenue Agency
CSIS	Canadian Security Intelligence Service
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial Intelligence Unit
FRFIs	Federally Regulated F*inancial Institutions*
FUR	Follow-up Report
LC	Largely compliant
MER	Mutual Evaluation Report
MSBs	Money Service Businesses
NC	Non-compliant
OSFI	Office of the Superintendent of Financial Institutions
PC	Partially compliant
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
PCMLTFR	Proceeds of Crimes (Money Laundering) and Terrorist Financing Regulations
RCMP	Royal Canadian Mounted Police
STR	Suspicious Transaction Report

MUTUAL EVALUATION OF CANADA: 6TH FOLLOW-UP REPORT

Note by the Secretariat

I. INTRODUCTION

1. The third mutual evaluation report (MER) of Canada was adopted in February 2008[1].

2. Canada was placed in the regular follow-up process, and reported back to the FATF in February 2009, February 2011, October 2011, October 2012 and February 2013. [2]

3. Canada first applied for removal from the follow-up process in February 2009. The follow-up report then noted that Canada had made real progress in several areas to improve its compliance with the FATF Standards and had in particular reached an adequate level of compliance with Recommendations 23 and 26. However, the Plenary deemed the progress reported in relation to Recommendation 5 to be insufficient. As pointed out in the report, a number of deficiencies remained in relation to this Recommendation, including in key areas such as beneficial ownership, ongoing due diligence and actions to be taken with respect to higher and lower risk scenarios. The Plenary thus determined that all the criteria for the removal from the follow-up process were not met (See first follow-up report in Annex 1).

4. In June 2012, Canada committed to apply again for removal in February 2013, considering that a number of amendments to the Proceeds of Crimes (Money Laundering) and Terrorist Financing Regulations (PCMLTFR) then in preparation would address most remaining issues in relation to Recommendation 5 by that date.

5. The amendments to the PCMLTF Regulations were approved on 31 January 2013 by the federal Cabinet and became public on that date. They were formally published in the *Canada Gazette* on 13 February 2013[3] and came into force on 1 February 2014. Canada decided on this one-year transition period to allow the reporting entities reasonable time to adjust their systems, policies and practices to the new CDD measures.

6. The FATF *Process and Procedures* provides that a jurisdiction should have *"an effective AML/CFT system in force"* to exit follow-up. Because the 2013 amendments aimed at addressing the remaining Recommendation 5 deficiencies only came into force on 1 February 2014, the February 2013 5th follow-up report by Canada was an interim report. It contained an analysis of the amendments to the PCMLTF Regulations that were published on 31 January 2013, and their impact on Canada's compliance with Recommendation 5 once they are in force. Canada indicated that it would apply to move from regular follow-up to biennial updates in February 2014.

---

1 www.fatf-gafi.org/countries/a-c/canada/documents/mutualevaluationofcanada.html.

2 First follow-up available in Annex I, other reports have not been published.

3 www.gazette.gc.ca/rp-pr/p2/2013/2013-02-13/pdf/g2-14704.pdf. A consolidated version of the amended PCMLTFR is available: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/.

7. This report is drafted in accordance with the procedure for removal from the regular follow-up, as agreed by the FATF Plenary in October 2008 and subsequently amended[4]. It contains a detailed description and analysis of the actions taken by Canada in respect of the core and key Recommendations rated partially compliant (PC) or non-compliant (NC) in the mutual evaluation. The procedure requires that a country "*has taken sufficient action to be considered for removal from the process – To have taken sufficient action in the opinion of the Plenary, it is necessary that the country has an effective AML/CFT system in force, under which the country has implemented the core[5] and key[6] Recommendations at a level essentially equivalent to a Compliant (C) or Largely Compliant (LC), taking into consideration that there would be no re-rating*"[7]. Canada was rated PC or NC on the following Recommendations:

Core Recommendations – NC or PC ratings
R.5 (NC)
Key Recommendations – NC or PC ratings
R.23 (PC), R.26 (PC)
Other Recommendations – PC ratings
R.7, R.11, R.17, R.21, R.30, R.34
Other Recommendations – PC ratings
R.6, R.8, R.9, R.12, R.16, R.22, R.24, R.33, SRVI, SRVII

8. As prescribed by the Mutual Evaluation procedures, Canada provided the Secretariat with a full report on its progress. The Secretariat has drafted a detailed analysis of the progress made for Recommendations 5, 23 and 26, and has prepared a summary of actions taken on other recommendations (see section VI), but has not done a detailed analysis of them[8]. A draft report was provided to Canada for its review, and comments received. Comments from Canada have been taken into account in the final draft. During the process, Canada has provided the Secretariat with all information requested.

9. As a general note on all applications for removal from regular follow-up: the procedure is described as a *paper based desk review*, and by its nature is less detailed and thorough than a mutual evaluation report. The analysis focuses on the Recommendations that were rated PC/NC, which means that only a part of the AML/CFT system is reviewed. Such analysis essentially consists of looking into the main laws, regulations and other material to verify the technical compliance of domestic legislation with the FATF standards. In assessing whether sufficient progress had been made, effectiveness is taken into account to the extent possible in a paper based desk review and

4 Third Round of AML/CFT Evaluations Processes and Procedures, par. 41 www.fatf-gafi.org/media/fatf/documents/process%20and%20procedures.pdf.

5 The core Recommendations as defined in the FATF procedures are R.1, SR.II, R.5, R.10, R.13 and SR.IV.

6 The key Recommendations are R.3, R.4, R.26, R.23, R.35, R.36, R.40, SR.I, SR.III, and SR.V.

7 FATF Processes and Procedures par. 39 (c).

8 See Annex 2 for the presentation by Canada of measures taken to address deficiencies on non-core and non-key.

primarily through a consideration of data provided by the country. It is also important to note that these conclusions do not prejudge the results of future assessments, as they are based on information which was not verified through an on-site process and is not, in every case, as comprehensive as would exist during a mutual evaluation.

II. MAIN CONCLUSIONS AND RECOMMENDATIONS TO THE PLENARY

10. As highlighted by the 5th follow-up report, the amendments to the PCMLTF Regulations that came into force on 1 February 2014 constitute a significant improvement of Canada's level of compliance with Recommendation 5, in particular in most of the key areas that had been identified in the first follow-up report: the deficiencies identified in relation to beneficial ownership and ongoing due diligence have been substantially addressed, and substantial progress has been made in relation to enhanced measures. A number of minor or very minor issues (in relation to scope, numbered accounts, circumstances in which CDD is required, identification of the persons purporting to act on behalf of the customers, beneficial ownership and enhanced measures), and two issues of more significance (in relation to exemptions and failure to complete CDD) remain to be addressed. It was therefore concluded that, overall, the Canadian AML/CFT regime has reached a level of compliance essentially equivalent to an LC with Recommendation 5.

11. On Recommendations 23 and 26, the 2009 1st follow-up report concluded that Canada had made real progress, and taken positive action to remedy the most significant deficiencies, including on effectiveness. It was therefore considered that there had been sufficient progress to conclude that Canada had implemented Recommendations 23 and 26 at an adequate level of compliance. The 5th follow-up report concluded that Canada had made continuous progress and significant improvement could be noted with regard to the effectiveness of the adopted measures.

12. It is recommended to remove Canada from the regular follow-up process.

III. OVERVIEW OF CANADA'S PROGRESS

A. OVERVIEW OF THE MAIN CHANGES SINCE THE ADOPTION OF THE MER

13. In 2011, a 10-year evaluation of Canada's AML/CFT regime (the Regime) was released[9]. The evaluation covered the period 2000-2010, and made recommendations regarding the further improvement of the Regime including:

- the continuation of the Regime with at least the same level of resourcing
- the conduct of a public opinion survey to determine the level of public awareness of the ML/TF threat and the actions of the Regime
- the creation of an Interdepartmental Working Group to identify future steps for continuing to improve the Regime's compliance with international commitments, information sharing, concerns of reporting entities, data and statistics, and the Regime's management framework.

9 www.fin.gc.ca/treas/evaluations/amlatfr-rclcrpcfat-eng.asp.

14. These recommendations served as a basis for a five-year Parliamentary review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), which was published in 2013[10].

15. Regarding the adaptation of the legal framework, Canada took key measures in the fields of Customer Due Diligence (CDD), and freezing of assets of corrupt officials. More details are available in the next section.

16. Canada also took a series of measures in order to strengthen its Financial Intelligence Unit (FIU), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Priority was given to reinforce the compliance program of FINTRAC, with the provision of additional resources, and its private sector outreach program. A new range of administrative sanctions is now at FINTRAC's disposal. FINTRAC's ability to share financial intelligence with law enforcement authorities has also been expanded. Closer coordination has also been developed in relation to the supervisory activities of the Office of the Superintendent of Financial Institutions (OSFI), the prudential regulator of federal financial institutions.

17. Regarding Designated Non-Financial Businesses and Professions (DNFBPs), the application of the AML/CFT regime was expanded to additional businesses and professions, notably British Columbia Notaries and dealers in precious metals and stones. With respect to legal counsel and legal firms, client identification due diligence and record-keeping obligations were introduced in 2008. However, these provisions are currently inoperative as a result of a court ruling and related injunctions. The Supreme Court of Canada recently granted leave to the Government of Canada to appeal the ruling.

B. THE LEGAL AND REGULATORY FRAMEWORK

18. Since the adoption of the MER in 2008, Canada has completed key AML/CFT legislative steps:

- Amendments were made to the PCMLTFA and to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* (PCMLTFR) in 2008 shortly after Canada's MER. These amendments included measures in relation to the circumstances in which CDD has to take place[11].
- Further amendments to the PCMLTFR were made in 2013, aimed at addressing the remaining deficiencies in relation to Recommendation 5, on beneficial ownership, on the purpose and nature of the business relationship, on enhanced due diligence and ongoing due diligence, and on exemptions. Those amendments came into force on 1 February 2014, and are detailed in the next section.

19. The PCMLTF Administrative Monetary Penalties (AMP) Regulations[12] came into force in December 2008. The Regulations provide FINTRAC with the power to apply monetary penalties (civil penalties) to any financial institution and DNFBPs subject to the AML/CFT regime, for non-

10 www.parl.gc.ca/Content/SEN/Committee/411/banc/rep/rep10mar13-e.pdf.

11 See Annex 1, First follow-up report.

12 http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/index.html.

compliance with the PCMLTFA. 19. With regard to financial countermeasures, amendments creating Part 1.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* were introduced through Budget 2010 to provide the Minister of Finance with the power to take targeted legally enforceable, graduated and proportionate financial countermeasures with respect to jurisdictions or foreign entities that lack sufficient or effective AML/CFT controls. These measures can be taken either on the basis of a call by an international organization, such as the FATF, or a unilateral decision based on domestic considerations. These measures could range from requiring reporting entities to enhance current customer identification and due diligence requirements under the PCMLTFA to restricting or prohibiting transactions with identified foreign jurisdictions or entities. The necessary legislative changes have received Royal Assent in 2010, and will be brought into force when accompanying regulations are completed.

20. Canada implemented a federal registration regime for money service businesses (MSBs) which has been in force since June 2008. Money services businesses have to register with FINTRAC.

21. The 2010 federal Budget[13] announced that tax crimes would be made a predicate offence for money laundering. The Criminal Code regulations were amended to reflect this change and have been in force since July 2010.

22. The Freezing Assets of Corrupt Foreign Officials Act (FACFOA)[14] was created and adopted in law on March 23, 2011 to allow the Canadian government to rapidly freeze the assets of politically exposed foreign persons (PEFPs) at the written request of a foreign state, where that state is experiencing political turmoil and freezing such assets is in the interest of international relations. Since its introduction, this legislation has been used to freeze the assets of, for example, certain Tunisian and Egyptian officials.

IV. DETAILED ANALYSIS OF PROGRESS MADE IN RELATION TO CORE RECOMMENDATION 5 *(RATED NC)*

23. The basis for the AML/CFT preventive legislation in relation to financial institutions and DNFBPs in Canada is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), which was amended in December 2006[15]. The Regulations that implement part of the Act and that are relevant to Recommendation 5 are the PCMLTF Regulations (PCMLTFR)[16].

24. Canada was found Non-Compliant in relation to Recommendation 5 in its MER, which also noted that a number of amendments to the PCMLTFA and the PCMLTFR were being prepared.

25. These amendments were analysed in Canada's first follow-up report, which concluded that they strengthened Canada's customer due diligence framework, notably by introducing measures in relation to the circumstances in which CDD has to take place (including in non face-to-face scenarios), beneficial ownership, customer identification for occasional transactions that are cross-border wire transfers, collecting information on the purpose and intended nature of the business

13 See Annex 5 in www.budget.gc.ca/2010/pdf/budget-planbudgetaire-eng.pdf.

14 http://laws-lois.justice.gc.ca/eng/regulations/SOR-2011-78/index.html.

15 http://laws-lois.justice.gc.ca/eng/acts/P-24.501/index.html.

16 http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/index.html.

relationship and measures to be taken in case of failure to complete CDD. Although Canada had strengthened its AML/CFT regime with the new regulatory requirements that entered into force in June 2008, the new provisions did not fully address the MER concerns, and some important deficiencies remained. This may be in part due to the fact that the regulations were passed very early in the mutual evaluation process, at which time the set of Recommendation 5 deficiencies in the MER were not known to Canada. There remained a significant set of deficiencies, including in several key areas: beneficial ownership; higher risk/enhanced CDD and ongoing due diligence.

26. On January 31, 2013, further amendments to the PCMLTFR, which were mainly aimed at addressing the remaining deficiencies in relation to Recommendation 5 (but also apply to DNFBPs), entered into Canadian law. These amendments came in force on 1 February 2014 and bring progress in relation to a number of deficiencies, including in the key areas identified in the first FUR:

- The circumstances in which CDD is required (cases where financial institutions have a suspicion of ML or TF);
- Beneficial ownership identification;
- Collecting information on the purpose and intended nature of the business relationship;
- Ongoing due diligence;
- Enhanced measures in higher risk scenarios;
- Exemptions (not allowed any more in cases of a suspicion of ML or TF)

27. The detailed analysis below assesses the impact this series of amendments have on Canada's level of compliance with Recommendation 5.

a) Scope - The requirement to conduct CDD does not extend to all financial institutions (notably financial leasing, factoring and finance companies)

28. In Canada's MER[17], the assessors noted that *"certain financial institutions that undertake financial activities, as defined by the FATF Recommendations are not currently covered by the AML/CFT regime. These sectors or activities[18] are as follows (excluding entities that are caught because they also engage in financial activities under the regime): financial leasing; factoring; finance companies (i.e. entities specialized in consumer lending, credit cards, equipment financing and small business loans that are not loan companies); providers of e-money; Internet payment providers[19]; and cheque cashiers[20] when only cashing cheques issued to denominated persons[21]."* The assessors

17 Mutual evaluation report of Canada, 2008, paragraph 631.

18 *"That came to the knowledge of the assessors."*

19 *"Internet payment and e-money providers are only subject to the Act if they also offer funds remittance or transmission services and, as such, would be considered money services businesses."*

20 *"Cheque cashing businesses that also offer money remittance services are included in the definition of MSBs under the PCMLTFA and are therefore subject to the requirements of the PCMLTFA."*

21 *"Credit card issuers are covered by the AML/CFT regime. The assessment team was advised that VISA, Mastercard and American Express are the only general purpose credit cards available in Canada. As a result of VISA and Mastercard internal rules, credit cards are only issued by regulated and supervised financial*

considered that the approach taken by Canada to create these exemptions was not in line with the FATF Methodology: only those activities for which there is a proven ML/TF risk are covered by the PCMLTFA, whereas under the FATF Methodology a list of financial activities and operations must be covered by the AML/CFT regime unless there is a proven low risk of ML of TF.

29. Some progress was noted in Canada's first follow-up report, notably the development of an AML/CFT risk assessment methodology and the application of this methodology to two sectors (factoring and leasing companies), which concluded that these sectors are low risk. The basis for excluding leasing companies raised a number of issues; however, given the lack of FATF guidance in this area and the uncertainties as to precisely what are the criteria or elements that justify an exclusion, it was considered very difficult in the framework of the follow-up process to come to a definitive conclusion as to whether the conclusions meet the "proven low risk" threshold set out in the standard. Canada's first follow-up report noted that a relatively minor set of other sectors (e.g. finance companies), remain outside the scope of the AML/CFT regime although they have not yet been subject to a proper risk assessment. The MER also noted that some segments of these sectors are included in the scope of the PCMLTFA since such financial services may be also carried out by entities already covered by the AML/CFT regime. Canada indicated that risk assessments of the other sectors that remained outside of the scope of the AML/CFT regime were planned.

30. Canada has informed that it is currently working on a broader risk assessment of these and other sectors. Specifically, on June 18, 2013, Canada published its Action Plan on Transparency of Corporations and Trusts in support of the G-8 countries' commitment to demonstrate leadership in improving their respective regimes to prevent the illegal use of corporations and trusts. Canada's G-8 Action Plan commits to developing a new money laundering and terrorist financing risk assessment framework and conducting a formal assessment of these risks domestically to better inform the development and implementation of effective policies and operational approaches to mitigate risks.

31. Canada has already begun working towards the commitments set out in the Action Plan. An interdepartmental Risk Assessment Working Group led by the Department of Finance has been established and the Terms of Reference were approved in spring 2013. In addition, the Department of Finance has initiated the development of an ML/TF threat assessment as an initial step towards a complete risk assessment.

32. **Conclusion**: some progress has been made since the adoption of the MER in relation to deficiency a) although, as noted above, a final conclusion could not be reached as to whether the conclusions regarding leasing companies meet the "proven low risk" threshold set out in the standard. As stressed in Canada's first FUR, the set of sectors that remain outside the scope of the AML/CFT regime and that have not yet been the subject of a proper risk assessment is not a major deficiency in the context of Canada.

---

institutions, both for PCMLTFA and prudential purposes. Finance companies that are not caught under the PCMLTFA can also issue general purpose credit cards (in addition to stored value cards) but do so through subsidiaries that are regulated for AML/CFT and prudential purposes."

b) Although numbered accounts are permissible and used, there is no direct requirement to maintain them in such a way that full compliance can be achieved with the FATF Recommendations

33. In its MER[22], Canada explained that although there was no explicit prohibition on opening anonymous accounts, basic CDD requirements on all new accounts holders since 1993 had in practice prevented the existence of anonymous accounts. However, in relation to numbered accounts, which are permissible in Canada, the assessors noted that *"there are no detailed rules or guidance on how [numbered] accounts should be managed by the financial institutions. The obligation for compliance officers to have access to CDD information is not clearly stated either."* It was thus recommended[23] that Canada should *"consider adopting detailed rules or guidance on the use of [numbered] accounts by financial institutions. Such rules should clearly set out the obligation for compliance officers to have access to CDD information"* so as to ensure compliance with the FATF Standards.

34. The first FUR concluded that this deficiency had been partially addressed through the following measures. First, a new section 9.2 of the PCMLTFA, which came into force in June 2008, clearly provides that no account can be opened if the financial institution cannot establish the identity of the client. Second, the OSFI B-8 Guidelines were revised in 2008[24], and the following provision was included: "*if FRFIs [*Federally Regulated F*inancial Institutions] provide services, such as account numbering or coding services, which effectively shield the identity of a client for business reasons (e.g., a corporate acquisition where the premature circulation of information could jeopardize the transaction), or where client identity is withheld for proprietary reasons, FRFIs must ensure that the client has been appropriately identified and the information is accessible by the Chief Anti-Money Laundering Officer."* The language of the OSFI Guidelines was strengthened in 2008, and its content is in line with what was recommended in Canada's MER. However these guidelines cannot be considered to be enforceable means, and it was noted in the first FUR that the deficiency concerning the access of compliance officers to CDD information was not addressed.

35. In preparing this follow-up report, Canada has not reported further progress with respect to deficiency b).

36. **Conclusion**: deficiency b) has been partially addressed. However, as noted in Canada's first FUR the remaining issue is *"relatively minor"*. Canada notes that this issue (no requirement in law or other enforceable means for financial institutions to ensure the access of the AML/CFT compliance officer to the CDD information collected in relation to numbered accounts) is in relation to an example from the 2004 Methodology, which is no longer explicitly part of the 2012 Standards.

22 Mutual evaluation report of Canada, 2008, paragraph 649.

23 Mutual evaluation report of Canada, 2008, paragraph 738.

24 www.osfi-bsif.gc.ca/Eng/Docs/b8.pdf

c) When CDD is required - there is no requirement to carry out CDD measures when there is a suspicion of ML or TF and when financial institutions have doubts about the veracity or adequacy of previously obtained CDD data

i. When there is a suspicion of ML or TF

37. As noted in Canada's first FUR, section 53.1 of the PCMLTFR, which came into force in June 2008, requires financial institutions to take reasonable measures to ascertain the identity of every client who conducts a transaction that is required to be reported to FINTRAC, i.e. when there is a suspicion of ML or TF, except in the following circumstances: (1) if the financial institution has already identified the individual as required; (2) if the financial institution believes that doing so would inform the individual that it is submitting a STR; or (3) the transaction being reported is an attempted transaction.

38. Section 53.1 constituted an improvement but did not fully address the deficiency: Canada requires financial institutions to take *reasonable measures* to conduct CDD in case of a suspicion of ML or TF, whereas under the FATF Standards taking reasonable measures is only applicable with respect to the obligation to verify the identity of the beneficial owners. However, it was noted in the first FUR that the language of FINTRAC Guideline 6[25], although not binding, clearly provides that financial institutions have to identify every client who conducts a suspicious transaction. Canada was thus invited to adopt similar direct language in the PCMLTFR. Canada has not reported any action in that regard but advises that the provision was drafted so as to not conflict with the restriction against tipping-off which is codified in the FATF Standards *("if the institution believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process.").*

39. Regarding the lack of requirement to conduct CDD in relation to suspicious *attempted* transaction, an amendment to section 53.1 of the PCMLTFR, which came into force on 1 February 2014, requires financial institutions to take reasonable measures to ascertain the identity of every natural person or entity who conducts *or attempts to conduct* a transaction that should be reported to FINTRAC. This amendment addresses the issue relating to attempted transactions.

ii. When financial institutions have doubts about the veracity or adequacy of previously obtained CDD data

40. As noted in Canada's first FUR, subsection 63(1.1) of the PCMLTFR, which came into force in June 2008, requires financial institutions to reconfirm the client's identity in situations where it has ascertained the client's identity but it has doubts about the information collected. This measure only applies to customers that are natural persons (and not to legal persons or arrangements). Despite this remaining issue, Canada's first FUR concluded that this element of deficiency c) had been substantially addressed.

41. **Conclusion**: significant progress has been achieved but deficiency c) has not been fully addressed. The amendments to Section 53.1 of the PCMLTFR have remedied one of the remaining issues that related to the obligation for financial institutions to conduct CDD when they have a

25 www.fintrac-canafe.gc.ca/publications/guide/guide6/6-eng.asp.

suspicion of ML or TF. The only remaining deficiency will be the requirement to take *reasonable measures* to conduct CDD in case of a suspicion of ML or TF, which is relatively minor.

d) When CDD is required - Customer identification for occasional transactions that are cross-border wire transfers takes place for transactions above CAD 3 000. This threshold is currently too high and no equivalent requirement is in place for domestic wire transfers.

42. Satisfactory progress was reported in Canada's first FUR in relation to this deficiency. The new paragraphs 59(1)(b) - for MSBs - and 54(1)(b) - for financial entities - of the PCMLTFR, which came into force in June 2008, reduced the threshold from CAD 3 000 to CAD 1 000 for the identification of the clients who conduct wire transfers. The record-keeping and client identification regulatory provisions apply to MSBs when they remit or transmit funds of CAD 1 000 or more, domestically or internationally. For financial entities, the provision applies to electronic funds transfers.

43. **Conclusion**: as noted in Canada's first FUR, deficiency d) has been addressed.

e) Required CDD measures - The current customer identification measures for natural persons are insufficient, especially in relation to non face to-face business relationships.

44. In Canada's MER[26], the main weakness noted in relation to customer identification measures was that, in the case of individuals not physically present, financial institutions, except MSBs, had to ascertain the identity of the individual by confirming that a cheque drawn by that individual on an account at a financial entity had been cleared, i.e. a cheque that was written by the individual, cashed by the payee and cleared through the individual's account. The assessors indicated that they were *"uncomfortable with the third party cleared cheque confirmation process as it was seen as a potential loophole for illegal use. As a sole means to confirm identity in non face-to-face situations, it is unreliable"*.

45. A number of positive measures have been taken to address this issue through amendments to section 64 of the PCMLTFR that came into force in June 2008. The third party cleared cheque confirmation process can still be used but needs to be combined with at least one other identification method (for instance referring to an independent and reliable identification product that is based on personal information in respect of the person and a Canadian credit history of the person of at least six month's duration).

46. **Conclusion**: as noted in Canada's first FUR, deficiency e) has been addressed.

f) Identification of persons acting on behalf of the customers - The requirement to identify up to three persons who are allowed to give instructions in respect of an account is too limitative

47. The FATF Standards require that, when conducting CDD measures in relation to legal persons or arrangements, financial institutions should verify that *any* person purporting to act on behalf of

[26] Mutual evaluation report of Canada, 2008, paragraph 667.

the customer is so authorised, and take reasonable measures to verify the identity of that person. Two issues were identified in the context of the mutual evaluation. First, there is no explicit obligation for financial institutions to verify that the person purporting to act on behalf of the customer is so authorized. Second, in accordance with the PCMLTFR,

- in the case of business accounts in relation to which more than three persons are authorised to act, financial entities (and securities dealers until June 2008) only have to ascertain the identity of *at least three* of these persons.
- where an entity was authorized to act as a co-trustee of a trust, trust companies only had to ascertain the identity of *up to three* persons authorized to give instructions with respect to the entity's activities as co-trustee.

48. In June 2008, the repeal of subsection 57 (2) from the PCMLTFR removed the possibility for securities dealers to identify at least three of the persons authorized to act in relation to a business account.

49. In preparing this report, Canada reported that paragraph 54(1)(a) and subparagraph 55(d)(ii) need to be understood in the context of the risk-based approach. Financial institutions are expected to adjust the number of persons the identity of whom they need to ascertain according to the risk, with, in any case, a minimum of three persons for financial entities and a maximum of three for trust companies. It is not certain whether the FATF Standards strictly require that financial institutions should identify and verify the identity of *every* person purporting to act on behalf of the customer and therefore whether the Canadian approach in relation to financial entities is acceptable. The fact that, in higher risk scenarios, trust companies would not be required to ascertain the identity of all the persons authorized to give instructions with respect to the entity's activities as co-trustee is clearly a deficiency, although it is minor.

50. Canada has not reported further progress with respect to deficiency f).

51. **Conclusion**: deficiency f) has been partially addressed. The remaining issue is minor.

g) Third party determination and identification of beneficial owners - except for IDA [Investment Dealers Association] supervised entities, financial institutions are neither required to understand the ownership and control structure of the customer nor obliged to determine who are the natural persons that ultimately own or control the customer

52. Some progress was noted in Canada's first FUR. In accordance with section 11.1 of the PCMLTFR, which came into force in June 2008, financial entities, securities dealers, life insurance brokers and companies and MSBs have to take *reasonable measures*, when confirming the existence of an entity, to obtain and, if obtained, to keep a record of:

- *for corporations*: the name and occupation of all directors of the corporation and the name, address and occupation of all persons who own or control, directly or indirectly, 25% or more of the shares of the company;

- *for entities other than corporations* ("entity" as defined under the PCMLTFA means a body corporate, a trust, a partnership, a fund or an unincorporated association or organisation): name, address and occupation of all persons who own or control, directly or indirectly, 25% or more of the entity.
- *for trusts*: section 55 of the PCMLTFR requires trust companies to identify and verify the identity of the settlers and co-trustees of trusts. Section 11 requires trust companies to identify the beneficiaries that are known at the time the trust company becomes a trustee for the trust. Trust companies are the only category of financial institutions allowed to act as trustees for a trust. As regards other financial institutions that provide accounts or business relationships to a customer who is a trustee of a trust, Canada relies on the general section 11.1 obligation (see second bullet point).

53. These measures were considered insufficient in the first FUR, which noted that the following important issues remained:

- The requirement to "take reasonable measures to obtain information on beneficial owners when confirming the existence of the entity" is weaker than the FATF Standards which require that financial institutions should "identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner". The lack of a requirement to verify the information collected, combined with the need to only take reasonable measures to identify, was considered to be a *"particularly important"* issue.
- In relation to customers that are trusts, although clear identification obligations apply to trust companies, other financial institutions were subject to the generic requirement under which a trust is defined to be a "entity". These financial institutions were then obliged to identify persons that own or control 25% or more of the entity, which could cover trustees (as the persons in control), but whether settlors were covered was not clear. Furthermore, a beneficiary does not "control" the trust, and it is not clear whether a beneficiary would "own" the trust. It was thus not certain that the new provisions fully covered the deficiency.
- No specific measures had been taken to address the fact that corporations can issue bearer shares.

54. The amendments to Section 11.1 of the PCMLTFR, which came into law on 31 January 2013 and into force on 1 February 2014, addressed a number of those issues.

55. Subsections 11.1 (1) and (2) provide that financial entities, securities dealers, life insurance companies and life insurance brokers or agents are required to *"obtain the following information:*

> *(1) (a) in the case of a corporation, the names of all directors of the corporation and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation;*

(b) in the case of a trust, the names and addresses of all trustees and all known beneficiaries and settlors of the trust;

(c) in the case of an entity other than a corporation or trust, the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the entity; and

(d) in all cases, information establishing the ownership, control and structure of the entity.

(2) Every person or entity that is subject to subsection (1) shall take reasonable measures to confirm the accuracy of the information obtained under that subsection."

56. First, these subsections create an obligation to identify the beneficial owner as well as to collect information establishing the ownership, control and structure of the entity, and to take reasonable measures to verify this information. Second, all financial institutions subject to this section will have to identify all trustees and known beneficiaries and settlors of the trust, and to take reasonable measures to verify this information.

57. Subsection 11.1(4) further provides that if financial institutions are *"not able"* to obtain the abovementioned information or confirm its accuracy, they have to *"take reasonable measures to ascertain the identity of the most senior managing officer of the entity"* and treat the entity as high risk and apply enhanced CDD measures. Subsection 11.1(4) is not in line with the 2003 Standards, in particular the requirements dealing with cases of failure to complete a part of the CDD measures. Consistent with the 2003 Standards, where financial institutions are unable to identify the beneficial owners or confirm their identity, they *"should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report"*. However, in such situations, subsection 11.1(4) does not require financial institutions to take any of these measures. Despite this, the issues relating to failure to complete CDD are dealt with below – see deficiencies q) and r) – and subsection 11.1(4) is not considered to be an issue under deficiency g) for the purpose of this report.

58. It should be noted that Canada explains that subsection 11.1(4) is aimed at reflecting the multiple-step approach to the identification of the beneficial ownership of legal entities that was introduced in the 2012 Standards (paragraph 5(b)(i) of the Interpretive Note to Recommendation 10)[27]. This report does not assess the measures with respect to the 2012 Standards. However, a preliminary analysis, which does not prejudge the results of Canada's Fourth Round mutual evaluation, raises a number of doubts about whether the subsection would be in line with paragraph 5(b)(i) of the Interpretive Note to Recommendation 10:

[27] See paragraph 5(b)(i) of the Interpretive Note to Recommendation 10, *The FATF Recommendations*, 2012. Financial institutions should first identify the natural persons who ultimately have a controlling ownership interest in a legal person; second, to the extent that there is doubt as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, they should identify the natural persons (if any) exercising control of the legal person or arrangement through other means; third, where no natural person has been identified, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

- it is not certain that the two-step Canadian approach followed in the amended section 11.1 covers all the elements of the three-step 2012 FATF Standards approach (in particular, that "other means" beneficial owners are captured by section 11.1);
- it is not clear whether the obligation to *take reasonable measures to ascertain the identity* of the most senior managing officer is in line with step 3 of the 2012 FATF Standards approach to establishing the beneficial ownership of legal persons.
- it is unclear how subsection 11.1(4) would apply to trusts.

59. Canada has not reported progress in relation to the third remaining issue identified in the first FUR, i.e. the fact that corporations can issue bearer shares, thus making it difficult to determine the beneficial owner. However, as noted in Canada's MER, "*it is likely that these shares have limited use in practice*."[28]

60. **Conclusion**: the amendments to section 11.1 of the PCMLTFR brought Canada into substantial compliance with the 2003 FATF standard on the identification of beneficial ownership.

h) Purpose & intended nature of the business relationship - there are currently no requirements (except for securities dealers) to obtain information on the purpose and intended nature of the business relationship.

61. Some progress was reported in the first FUR: paragraphs 14(c.1) and 23(a.1) of the PCMLTFR, which came into force in June 2008, require financial entities and securities dealers to keep records that set out the intended use of new accounts. However, the insurance and MSBs sectors were out of the scope of the requirement. Furthermore, this obligation was potentially more limited than what the FATF Standards require (information should be obtained on the purpose and intended nature of the *business relationship*, which is a broader notion than an account).

62. As part of the 2013 amendments to the PCMLTFR, a new section 52.1 requires that "Every person or entity that enters into a business relationship under these Regulations shall keep a record that sets out the purpose and intended nature of the business relationship". The amendments also introduce a definition of "Business relationship" in section 1 which covers any relationship of a financial institution with a client to "conduct financial transactions or provide services related to those transactions and, as the case may be, (a) if the client holds one or more accounts with that person or entity, all transactions and activities relating to those accounts; or (b) if the client does not hold an account, only those transactions and activities in respect of which any [financial institution] is required to ascertain the identity of a person or confirm the existence of an entity under these Regulations." These new provisions therefore address the two remaining issues as noted in Canada's first FUR in relation to deficiency h).

63. **Conclusion**: the amendments that create section 52.1 of the PCMLTFR and introduce a definition of business relationships in section 1 of the PCMLTFR, address deficiency h).

[28] Mutual evaluation report of Canada, 2008, paragraph 1396.

i) Ongoing Due Diligence - except for securities dealers, there are currently no requirements to conduct ongoing due diligence on the business relationship although the need to identify customers for large cash transactions and electronic fund transfers provide certain automatic trigger points.

j) Ongoing Due Diligence - except for securities dealers financial institutions are not required to ensure that documents, data and information collected under the CDD process is kept up-to-date and relevant.

64. As noted in the first FUR, Section 9.6 of the PCMLTFA, which came into force in June 2008, requires all businesses covered by the Act to (1) adopt a compliance program; (2) develop policies and procedures for assessing ML/TF risks; and (3) if some higher risks are identified following this risk assessment, take enhanced measures for (i) identifying clients, (ii) keeping records and (iii) monitoring financial transactions. Section 71.1 of the PCMLTFR, which also came into force in June 2008, specifies the nature of these enhanced measures ("prescribed special measures"), which include taking reasonable measures to keep client and beneficial ownership identification information up-to-date and taking reasonable measures to conduct ongoing monitoring for the purpose of detecting suspicious transactions. The first FUR concluded that these requirements were not in line with the FATF standard, which requires that ongoing due diligence should be conducted on all business relationships (not only in higher risk scenarios).

65. The amendments to the PCMLTFR that came into force on 1 February 2014 introduced sections 54.3 (financial entities), 56.3 (life insurance sector), 57.2 (securities dealers), 59.01 (MSBs) and 61.1 (departments or agents of Her Majesty in Right of Canada or of a Province that sell or redeem money orders), which require these financial institutions to *"(a) conduct ongoing monitoring of its business relationship with that person or entity; and (b) keep a record of the measures taken and the information obtained under paragraph (a)."* The amendments also define "business relationships" (see definition above) and "ongoing monitoring" (*"monitoring on a periodic basis based on the risk assessment undertaken in accordance with subsection 9.6(2) of the Act and subsection 71(1) of these Regulations, by a person or entity to which section 5 of the Act applies of their business relationship with a client for the purpose of (a) detecting any transactions that are required to be reported in accordance with section 7 of the Act; (b) keeping client identification information and the information referred to in section 11.1 and 52.1 up to date; (c) reassessing the level of risk associated with the client's transactions and activities; and (d) determining whether transactions or activities are consistent with the information obtained about their client, including the risk assessment of the client"*).

66. Sections 54.3, 56.3, 57.2, 59.01 and 61.1 thus require all financial institutions covered by the Canadian AML/CFT framework to conduct ongoing monitoring on their business relationships. Consistent with the definition of "ongoing monitoring", this obligation includes both conducting ongoing due diligence and keeping CDD information up-to-date.

67. **Conclusion**: deficiencies i) and j) were addressed by the amendments to the PCMLTFR.

k) ML/FT risks - enhanced due diligence - there is no requirement to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction.

68. As was noted in the first FUR, subsection 9.6(2) of the PCMLTFA, which came into force in June 2008, now requires financial institutions to develop and apply policies and procedures to assess the risk of a ML or TF activity financing offence, and subsection 9.6(3) requires them to take *"prescribed special measures for identifying clients, keeping records and monitoring financial transactions in respect of the activities that pose the high risk"*. Section 71.1 of the PCMLTFR, which also came into force in June 2008, specifies that the prescribed special measures are the development and application of written policies and procedures for (a) taking reasonable measures to keep client identification information and beneficial ownership information up to date; (b) taking reasonable measures to conduct ongoing monitoring for the purpose of detecting suspicious transactions; and (c) mitigating the risks identified. The first FUR thus concluded that measures (a) and (b) *"are not enhanced due diligence measures as foreseen in the FATF Recommendations but are, on the contrary, CDD measures that should be mandatory for all customers or transactions"*.

69. The amendments to the PCMLTFR that came into force on 1 February 2014 modify section 71.1 and the notion of "prescribed special measures". These measures are:

(a) *"taking enhanced measures based on the risk assessment undertaken in accordance with subsection 9.6(2) of the Act to ascertain the identity of any person or confirm the existence of any entity"*, in addition to the standard customer identification measures; and

(b) *"taking any other enhanced measure to mitigate the risks identified in accordance with subsection 9.6(3) of the Act, including, (i) keeping client identification information and the information referred to in section 11.1* [beneficial ownership information] *up to date, and (ii) in addition to the measures required in sections 54.3, 56.3, 57.2, 59.01, 59.11, 59.21, 59.31, 59.41, 59.51, 60.1 and 61.1* [ongoing monitoring requirements], *conducting ongoing monitoring of business relationships for the purpose of detecting transactions that are required to be reported to the Centre under section 7 of the Act* [suspicious transactions]*"*.

70. Under (a), prescribed special measures will have to include enhanced customer identification and verification measures.

71. However, the way (b) is worded is ambiguous, since the prescribed special measures should also cover *"any other enhanced measure to mitigate the risks"*, but these enhanced measures include in (i) and (ii) requirements that should apply to *any* business relationships (not only in high risk scenarios). Canada explains that *"it is a fundamental principle of legal interpretation that statutory provisions should not be interpreted in such a way that would lead to absurdity or internal inconsistency.* 'Absurdity' *includes situations where the wording in question contradicts the remainder of the provision"*. Canada adds that "*given that both the chapeau of s.71.1 and 71.1(b) specifically require reporting entities to implement enhanced measures, it would give an absurd result if "standard" measures were considered to be enhanced for the purposes of s.71.1"*. Therefore, for Canada, *"it would be clear to all regulators and courts in Canada, as well as stakeholders, that*

s.71.1(b)(i) and (ii) refer to enhanced measures, in accordance with the purpose of s.71.1." In order to remove any ambiguity in the nature of this part of the prescribed special measures, Canada is encouraged to clarify the meaning of (i) and (ii) e.g. through guidance.

72. **Conclusion**: the amendments to section 71.1 brought substantial progress in relation to deficiency k). Canada is encouraged to clarify the meaning of paragraph 71.1(b) of the Regulations, e.g. in guidance, so as to confirm that deficiency k) has been fully addressed.

l) ML/FT risks - reduced or simplified due diligence - the current exemptions mean that, rather than reduced or simplified CDD measures, no CDD apply, which is not in line with the FATF standards.

m) ML/FT risks - reduced or simplified due diligence - exemptions from CDD and third party determination bring in very far reaching exceptions that introduce potential gaps in the customer identification process (especially the exemptions apply to financial entities that operate in FATF countries based on presumption of conformity only).

73. The PCMLTFR provides for a number of exemptions from the client identification and record-keeping requirements in certain specific circumstances but does not establish a simplified or reduced CDD regime. These exemptions are mainly contained in sections 9 and 62 of the PCMLTFR. It should also be noted that sections 19 and 56 of the PCMLTFR create a form of exemption by requiring that life insurers only conduct CDD in relation to the purchase of an immediate or deferred annuity or a life insurance policy for which the client may pay CAD 10,000 or more over the duration of the annuity or policy.

74. The Glossary of the 2004 Methodology authorizes countries to exempt some financial institutions or activities from the application of some or all of the AML requirements in two situations:

- *"when a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring"; or*
- *"in strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above".*

75. In the context of its mutual evaluation, Canada explained that the exemptions relate to low risk transactions, products or customers and were developed following extensive discussions between the Department of Finance, FINTRAC, the Royal Canadian Mounted Police (RCMP) and the reporting entities. However, the assessors indicated that no more information had been provided at the time of the on-site visit, which means that a low risk of ML had not been *"proven"* as required by the Methodology. It was therefore recommended in the MER that the transactions, products and customers exempted from the application of CDD measures should be subject to a simplified or reduced CDD regime.

76. In the first FUR, Canada explained that sections 9.6 of the PCMLTFA and 71.1 of the PCMLTFR (which both came into force in June 2008) on risk assessment and risk mitigation "overrule" the exemptions contained in the PCMLTFR, which results in a requirement for financial institutions to

apply enhanced CDD measures in cases of a higher ML/TF risk even in the situations covered by the exemptions. However, the first FUR concluded that the exemptions remain per se applicable as long as the account is not identified as high risk, which is not in line with the FATF Standards or the recommendation set out in the MER. Furthermore, the list of exemptions contained in section 9, and more importantly section 62, had been expanded following the mutual evaluation.

77. In preparing this report, Canada has indicated that the exemptions under section 62(2) of the PCMLTFR apply predominantly to highly regulated and limited products which can only be used by individuals located within Canada, or to accounts opened on behalf of domestic entities that are regulated under the PCMLTFA or other federal/provincial law. Canada has also mentioned that most of the exemptions to CDD requirements deal with registered financial products, which have tax implications for Canadians and are highly regulated. Client information is collected by the Canada Revenue Agency for tax purposes, and this is why Canada considers unnecessary for financial institutions to collect it or to be required to collect it under the PCMLTFA. However, as noted above, the FATF standard clearly provides that exemptions from CDD requirements need to be based on a "proven low risk" of ML/TF, a term that intentionally sets a high standard for the justification of exemptions. Canada indicates that it is currently working on a broader risk assessment of these and other sectors, that could provide the justification for the exemption.

78. The amendments to the PCMLTFR that came into force on 1 February 2014 introduce subsection 62(5), which provides that the exemptions contained in subsections 62(1) to (3) do not apply when the financial institution is required to take reasonable measures to ascertain the identity of the natural persons who conduct or attempt to conduct suspicious transactions (i.e. no exemption in cases of suspicious transactions). Canada explains that subsection 62(5) creates a general monitoring obligation which also applies to exempted transactions, and as such submits these to a form of simplified CDD regime. It is however unclear what in practice an obligation to monitor exempted transactions for the purpose of detecting suspicions of ML or TF would consist of and whether it can amount to a simplified CDD regime, which, under the FATF Standards, should comprise, although in a simplified form, the four standard CDD requirements as described in Recommendation 5.

79. **Conclusion**: section 9.6 of the PCMLTFA introduced some CDD obligations in relation to the transactions, products and customers subject to CDD and third party determination exemptions. Subsection 62(5) introduced by the 2013 amendments to the PCMLTFR creates further CDD obligations. However, the nature of these requirements is not in line with the Standards, and it should also be noted that Canada has created new exemptions since the adoption of the MER. Therefore, the amendments that came into force on 1 February 2014 are not sufficient to address deficiencies l) and m).

n) ML/FT risks - reduced or simplified due diligence - there is no explicit provisions that set out that CDD or third party determination exemptions are not acceptable where there is a suspicion of ML or FT or specific higher risk scenarios apply.

80. Subsections 62(1) to (3) of the PCMLTFR contain lists of types of transactions, products and customers in relation to which the CDD (and third party determination) obligations do not apply. The amendments to the PCMLTFR that entered into law on 31 January 2013 and came into force on

1 February 2014 introduce subsection 62(5) which provides that these exemptions do not apply when the financial institution is required to take reasonable measures to ascertain the identity of the natural persons who conduct or attempt to conduct suspicious transactions.

81. In relation to the other part of deficiency n) (i.e. there are no explicit provisions that set out that CDD or third party determination exemptions are not acceptable where specific higher risk scenarios apply), Canada explains that *"most of the exemptions deal with registered financial products, which have tax implications for Canadians and are highly regulated, or domestic entities that are regulated under the PCMLTFA or other federal/provincial law"* and therefore "*specific high risk scenarios (such as PEPs) are not applicable in this case"*.

82. **Conclusion**: Subsection 62(5) of the PCMLTFR, which came into force on 1 February 2014 will address deficiency n).

o) ML/FT risks - reduced or simplified due diligence - financial institutions, in certain circumstances, are given the permission to exempt from CDD requirements or third party determination obligations certain customers resident in another country. However, Canada has not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations.

83. The FATF Standards (INR5, 2003 Recommendations) provide that where countries allow financial institutions to apply simplified CDD measures to customers from any other jurisdiction, they must be satisfied that the jurisdiction is in compliance with and has effectively implemented the FATF Recommendations. As noted in the MER and the first FUR, the exemptions listed in the PCMLTFR are not explicitly limited to situations where the customer resides in Canada, even though, as noted by Canada, a number of them would apply to *"highly regulated and limited products which can only be used by individuals located within Canada, or to accounts opened on behalf of domestic entities that are regulated under the PCMLTFA or other federal/provincial law"*.

84. Some exemptions explicitly apply to customers that operate in foreign countries:

- Paragraph 62(2)(m) provides that CDD requirements do not apply when *"there are reasonable grounds to believe that the account holder is a public body or a corporation that has minimum net assets of $75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange that is prescribed by section 3201 of the Income Tax Regulations and operates in a country that is a member of the Financial Action Task Force on Money Laundering.*
- Subsection 9(5) states that the obligation to identify the third party (and not to determine whether the customer is acting on behalf of a third party), does not apply to customers of securities dealers that are "*engaged in the business of dealing in securities only outside of Canada (...) and where (a) the account is in a country that is a member of the Financial Action Task Force; (b) the account is in a country that is not a member of the Task Force referred to in paragraph (a) but has implemented the recommendations of the Task*

> *Force relating to customer identification and, at the time that the account is opened, the securities dealer has obtained written assurance from the entity where the account is located that the country has implemented those recommendations; or (c) the account is in a country that is not a member of the Task Force referred to in paragraph (a) and has not implemented the recommendations of the Task Force relating to customer identification but, at the time that the account is opened, the securities dealer has ascertained the identity of all third parties relating to the account as described in paragraph 64(1)* [which includes identification requirements for customers in non face-to-face situations]".

85. Therefore, as noted in the MER, section 62(2)(m) (previously section 62(2)(b)) and section 9(5) rely on a presumption that countries in which customers that may be exempted from CDD measures operate have implemented the FATF Standards. However, Canada had not carried out a systematic country risk analysis to ensure that third countries in which customers of Canadian financial institutions are resident are in compliance with and have effectively implemented the FATF Recommendations.

86. No specific progress was reported in this area since the first FUR. However, as noted above, in view of the preparation of this follow-up report, Canada indicated that risk assessments are conducted through its Illicit Financing Advisory Committee which will inform Directive and Regulations issued under Part 1.1 of the PCMLTF Act. When in force, Part 1.1 will provide the Minister of Finance with the power to take targeted legally enforceable, graduated and proportionate financial countermeasures with respect to jurisdictions or foreign entities that lack sufficient or effective AML/CFT controls. These measures can be taken either on the basis of a call by an international organization, such as the FATF, or a unilateral decision based on domestic considerations, and could range from requiring reporting entities to enhance current CDD requirements under the PCMLTFA to restricting or prohibiting transactions with identified foreign jurisdictions or entities. In addition, guidance is provided through FINTRAC advisories and OSFI notices encouraging enhanced CDD with respect to clients and beneficiaries involved in transactions with high risk jurisdictions.

87. **Conclusion**: deficiency o) has been addressed, though the relevant legislation is not yet in force.

p) Timing of verification - the PCMLTF Regulations set out unreasonable verification timelines to be carried out by certain financial sectors and/or in relation to certain customers.

88. In Canada's MER[29], the assessors noted that the PCMLTFR established generally acceptable timelines for ascertaining customer identity, but that certain serious weaknesses remained in relation to the identity verification carried out by a number of financial sectors (in particular, securities and life insurance) and/or vis-à-vis certain types of customers (entities, including corporations).

[29] Mutual evaluation report of Canada, 2008, paragraph 708.

89. As noted in the first FUR, a number of amendments to sections 64, 65 and 66 of the PCMLTFR, which came into force in June 2008, reduced the timelines for verifying the identity of customers of life insurers (from 6 months to 30 days), customers of securities dealers (from 6 months to before any transaction other than an initial deposit is carried out on the account for natural persons and 30 days for entities); and customers of MSBs that are entities (from 6 months to 30 days). The conclusion was that the new timelines adequately address the deficiency identified in the MER.

90. **Conclusion**: deficiency p) has been adequately addressed.

q) Failure to satisfactorily complete CDD - financial institutions (except securities dealers in some circumstances) are not prevented from opening an account or commencing business relationship or performing a transaction and they are not required to make a suspicious transaction report.

91. Some progress in this area was reported in Canada's first FUR. A new section 9.2 of the PCMLTFA, which came into force in June 2008, prohibits reporting entities from opening an account for a client if it cannot ascertain the identity of the client in accordance with the prescribed measures. However, the first FUR concluded that this provision had only partially addressed deficiency q). In particular, it was noted that there is no obligation in law or regulation for financial institutions to consider making a suspicious transaction report in cases where the identity of the client cannot be established and properly verified. Canada explains that there is however such a requirement in FINTRAC guidance. Section 9.2 of the PCMLTFA only prohibits reporting entities from opening an account in such situations, which is more limited than the FATF requirement to also prohibit reporting entities from commencing a business relationship or performing a transaction.

92. Canada has not reported further progress. However, Canadian officials indicate that:

- It is not possible in Canada to include a legal obligation to *consider* doing something.
- *"The common law legal principle of a positive obligation applies. Specifically, this means that where law or regulation sets out a positive obligation on stakeholders to comply with a specific provision, failure to comply with this obligation means that stakeholders are in violation of the law. There is no need to specifically indicate in the law what happens if stakeholders cannot comply with the obligation, as it is well understood that it is not legal to go ahead with a transaction or account opening if the obligation in question is not fulfilled."*

93. However, other common law countries have introduced such obligations. Furthermore, section 9.2 of the PCMLTFR is an indication that Canada can introduce this type of requirement, although Canada notes that this is an exception which was aimed to address the FATF concerns.

94. **Conclusion**: deficiency q) has been partially addressed.

r) Failure to satisfactorily complete CDD - in situations where the financial institution has already commenced a business relationship but is unable to perform adequate CDD and establish beneficial ownership, there is no requirement to terminate the business relationship

95. Canada has not reported specific progress in this area. However, Canadian officials indicate that the two explanations given in relation to deficiency q) are also relevant with respect to deficiency r). The comments made above in relation to these explanations are reiterated.

96. **Conclusion**: deficiency r) has not been addressed.

RECOMMENDATION 5 – OVERALL CONCLUSION

97. In the year that followed the adoption of its MER, Canada took a number of positive steps to address some of the deficiencies identified in relation to Recommendation 5 through the adoption of new provisions both in the PCMLTFA and the PCMLTFR. However, as noted in the first FUR, a significant set of deficiencies had not been addressed. In particular, several remaining issues were noted in the following key areas: beneficial ownership (deficiency g); higher risk/enhanced CDD and lower risk/exemptions (deficiencies k to o); and ongoing due diligence (deficiencies i and j).

98. Since the first FUR, Canada has made a number of amendments to the PCMLTFR which aim at addressing most of the remaining issues that were noted in the first FUR. These amendments entered into law on 31 January 2013 and came into force on 1 February 2014. They significantly improve Canada's level of compliance with Recommendation 5. In particular, the remaining issues in relation to beneficial ownership and ongoing due diligence are addressed, the amendments also substantially remedy the weaknesses with respect to the enhanced CDD obligations and bring some progress in relation to the exemptions from the CDD obligations.

99. In total, the following issues remain to be addressed:

- six minor or very minor issues, in relation to deficiencies a (scope), b (numbered accounts), c (when CDD is required), f (identification of persons purporting to act on behalf of the customers), g (beneficial ownership) and h (enhanced measures);
- two issues of more significance, in relation to, respectively, deficiencies l, m and o (exemptions), and q and r (failure to complete CDD).

100. This means that Canada has reached a level of compliance essentially equivalent to an LC with Recommendation 5.

V. DETAILED ANALYSIS OF PROGRESS MADE IN RELATION TO KEY RECOMMENDATIONS 23 AND 26 (RATED PC)

101. Based on the first FUR, it was concluded that Canada had made real progress and had taken positive action to remedy the most significant deficiencies. It was thus considered that there had been sufficient progress to conclude that Canada had implemented Recommendations 23 and 26 at a level equivalent to a C or an LC. It was also recommended to continue monitoring progress, especially with regard to the effectiveness of the adopted measures.

Recommendation 23 – description and analysis

a) Exclusion from the AML/CFT regime of certain financial sectors (such as financial leasing, factoring, finance companies, etc.) without proper risk assessments.

102. See the analysis above in relation to Recommendation 5 a) (par. 25 and s.).

b) For the financial institutions subject to the PCMLTFA, there is a very unequal level of supervision of AML/CFT compliance, with certain categories of financial institution appearing to be insufficiently controlled (MSBs, certain credit unions/caisses populaires, life insurance intermediaries…). This is due to the limited staff resources of FINTRAC dedicated to on-site assessments compared to the high number of reporting entities, which has not always been compensated by the involvement of the primary prudential regulators in AML/CFT issues.

FINTRAC – AML/CFT supervisor for all reporting entities[30]:

103. Canada reports that the number of FINTRAC staff has increased in the compliance section from 49 to 87 staff (from the time of the on-site visit in 2007 to March 31, 2013). FINTRAC was re-structured in the fall of 2008 with employees from other sectors in FINTRAC moving to the compliance section.

Table 1. **Evolution of FINTRAC staff – Compliance and direct enforcement activities**

Fiscal Year (As of April 1st)	Full Time Equivalents in FINTRAC's Compliance Program	Full Time Equivalents in FINTRAC's Direct Enforcement Activities
2008-09	60	34
2009-10	56	34
2010-11	64	40
2011-12	79	52
2012-13	87	67

104. FINTRAC also received additional funding in 2010 (an additional CAD 8 million/USD 7.652 million in annual funding announced in Federal Budget 2010) and CAD 5 million (USD 4.782 million) of this on-going funding was specifically ear marked to enhance FINTRAC's compliance program.

105. *National Compliance Program[31]*. Canada indicates that its compliance program focus evolved from a guidance/outreach approach to a formal risk-based approach (RBA) Compliance

30 In order to assist it, FINTRAC has signed MOUs with certain regulators or supervisors to share information. In addition to this, some regulators have provisions under their own legislation or codes of conduct that impose similar requirements to, or which complement the key provisions in the PCMLTFA through separate enforcement powers (for example, OSFI and IDA) (Mutual evaluation report of Canada, 2008, paragraph 935).

31 Mutual evaluation report of Canada, 2008, paragraphs 1092 to 1106.

Enforcement Program. As the RBA has shifted towards greater enforcement, it has undergone an appreciable overhaul. This has resulted in a revamped risk based compliance program which began in 2010 and continues to be modernized. The analysis completed in determining sectors of high and low risk feed into determining the number of reporting entities in each sector that will have compliance examinations conducted by FINTRAC.

106. In terms of coverage, FINTRAC's financial conglomerates and large reporting entities strategies ensure that the key industry players with large market shares are examined regularly given the inherent risks that are associated with their size and respective business models, as well as the consequences of any potential non-compliance. A share of compliance enforcement activities is also directed at randomly selected reporting entities to maximize coverage, validate benchmarks, and promote compliance more generally.

107. A number of new tools are utilized by FINTRAC to determine sectors that pose a high risk of being abused for ML/TF, including Compliance Assessment Reports, desk reviews and IT tools:

108. *Use of Compliance Assessment Report*. Canada indicates that Compliance questionnaires have been replaced with a new enforcement tool, the Compliance Assessment Report (CAR). As part of their obligations to report on their compliance with the PCMLTFA, reporting entities must complete the CAR when requested to do so by FINTRAC.

109. Canada mentions that CARs allow FINTRAC not only to validate the existence of reporting entities but also to better profile reporting entities within a sector. Canada adds that CARs have helped expand the coverage, and more importantly, in a manner that is tailored and cost effective. Early results are showing that CARs help raise awareness and deter non-compliant behaviour. CAR results have also been leveraged to initiate desk and on-site exams.

110. Canada reports that in 2012-2013, 4, 008 CARs were issued across several sectors in order to help assess compliance regime obligations. These sectors were selected on the basis of risk considerations.

Table 2. **Compliance Assessment Reports Sent by FINTRAC – Break Down By Sector**

Sector	Activity Sector	2010/11	2011/12	2012/13	Total
Accountants	Accountants	n/a	1 480	n/a	**1 480**
Dealers in Precious Metals and Stones	Dealers in Precious Metals and Stones	n/a	1 500	2 000	**3 500**
Financial Entities	Banks	18	n/a	n/a	**18**
	Credit Unions / Caisses Populaires	n/a	n/a	302	**302**
	Trust & Loan Companies	11	8	48	**67**
Life Insurance	Life Insurance (including agents and brokers)	33	1 559	829	**2 421**
Real Estate	Real Estate	n/a	1 479	n/a	**1 479**
Money Service	Money Service Businesses	n/a	n/a	50	**50**
Securities	Securities Dealers	n/a	n/a	779	**779**
Total		**62**	**6 026**	**4 008**	**10 096**

111. Despite the addition of two new sectors in 2012-2013 (MSBs and securities), the total number of CARs has dropped from 6,026 to 4,008. This is partly due to an extensive coverage of the accounting and real estate sectors in 2011/12.

112. *Desk Examinations*. Canada indicates that FINTRAC has developed new approaches to conducting compliance examinations, including desk reviews, which were implemented in 2009. The requirement to provide information for a desk review is covered by the compliance measures under Section 63.1 of the PCMLTFA and failure to provide information for a desk review is subject to the Administrative Monetary Penalties (AMP) regime.

113. Canada informs that FINTRAC applies examination types (desk/onsite) commensurate with such factors as risk, complexity, and type of reporting entity. Canada reports that the desk examination initiative has allowed FINTRAC to optimize the use of its resources, tailored its compliance enforcement activities, and helped increase the total number of examinations conducted in a given fiscal year, while not decreasing the value of examinations and findings.

114. *New IT tools*. Canada reports that as of January 2012, IT systems have been put in place to support the examination program, CAR program, and the distribution of compliance workload.

115. *Compliance Research Laboratory*. Canada informs that FINTRAC has established a dedicated research environment used to develop and maintain a compliance risk model, which is used to direct the allocation of resources in the most efficient manner. Ongoing development focuses on further increasing the quality of incoming report data to support the intelligence function. This includes an enhancement of the validation rules for incoming reports (May 2014), and the implementation of a facility through which the agency can monitor large volumes of incoming reports and directly address issues with volumes, timing and data quality (August 2014).

116. *Major Reporters Team*. In July 2013, FINTRAC announced the creation of a major reporters team within its National Compliance Program. The team will be responsible for managing FINTRAC's relationship with the largest of the reporting entities in the banking sector. Given their economic footprint and the volume of transactions they facilitate, major reporters play a unique and important role in the detection, deterrence and prevention of money laundering and terrorist financing. For Canada, it represents an important milestone in FINTRAC's ongoing efforts to monitor and enhance compliance.

Table 3. **Overview of FINTRAC's compliane activities**

Compliance Activities by FINTRAC		Fiscal Year					
		2008/09	2009/10	2010/11	2011/12	2012/13	Total
Enforcement Activities	Money Services Business Registration Actions *	799	240	568	396	778	**2 781**
	Compliance Assessment Reports (CAR) Sent	n/a	n/a	62	6 026	4 008	**10 096**
	Examinations **	455	691	684	1 069	1 157	**4 056**

Compliance Activities by FINTRAC		Fiscal Year					
		2008/09	2009/10	2010/11	2011/12	2012/13	Total
	Administrative Monetary Penalties - Notices of Violations Issued ***	n/a	14	7	7	13	**41**
	Non-Compliance Disclosures	19	3	1	4	0	**27**
Other Key Compliance Activities	General Inquiries ****	6 445	3 728	4 365	6 763	5 993	**27 294**
	Policy Interpretations	n/a	n/a	258	450	245	**953**
	Reports Returned for Further Actions	2 115	2 283	1 537	48	630	**6 613**
	FINTRAC's Outreach Presentations	524	141	39	27	23	**754**
Total		**10 357**	**7 100**	**7 521**	**14 790**	**12 847**	**52 615**

* This includes initial registrations, registration renewals, registration denials, and registration revocations.
** This includes desk and on-site examinations conducted by FINTRAC.
*** FINTRAC has the authority to issue administrative monetary penalties since December 30, 2008.
**** This reflects only the volume of calls received by FINTRAC's Call Centre.

117. Canada reports that in 2012-13, FINTRAC completed 1,157 compliance examinations. This was a 69% increase from 684 examinations completed in 2010-11. This significant increase was due, in large part, to both the recruitment of additional resources to meet the Government of Canada Budget 2010 commitments and to the implementation of the new risk-based compliance strategy.

118. Canada also mentions that CARs, the newly introduced Compliance Assessment Reports (see paragraph 106), were not designed to be used for all sectors as they are not always the most appropriate method. For example, all casinos undergo an on-site examination on a regular cycle. Therefore, CARs have not been used for this sector. In 2012–2013, 4008 CARs were issued across several sectors in order to help assess compliance regime obligations.

Table 4. **Overview of FINTRAC's examinations**

Sector	Activity Sector	N° of reporting entities in Fiscal 2012/13 (primary population*)	FINTRAC Examinations**					
			2008/09	2009/10	2010/11	2011/12	2012/13	Total
Accountants	Accountants	3 829	21	48	20	0	25	114
BC Notaries	BC Notaries	289	0	0	0	0	16	16
Casinos	Casinos	39	12	12	12	5	10	51
Dealers in Precious Metals and Stones	Dealers in Precious Metals and Stones	642	0	0	0	10	166	176
Financial Entities	Banks***	80	0	1	1	6	2	10

Sector	Activity Sector	N° of reporting entities in Fiscal 2012/13 (primary population*)	FINTRAC Examinations**					
			2008/09	2009/10	2010/11	2011/12	2012/13	Total
	Credit Unions/ Caisses populaires	736	69	172	205	432	301	1,179
	Trust & Loan Companies***	75	3	5	4	9	3	24
Life Insurance***	Life Insurance (including agents and brokers)	89	28	70	52	5	13	168
Money Services Businesses	Money Services Businesses	788	220	210	200	426	222	1 278
Real Estate	Real Estate	20 784	62	90	70	40	270	532
Securities Dealers	Securities Dealers	3 829	40	83	120	136	129	508
Total		**31 180**	**455**	**691**	**684**	**1 069**	**1 157**	**4 056**

* The reporting entities' population can be separated into the primary and secondary reporting entities populations. The difference between the primary population and the secondary population lies in the fact that the Act is structured in such a way that there are instances where both an employer and an employee will be subject to the provisions of the Act; in such case, the employer is seen as the primary reporting entity and the employee as the secondary. These instances occur in the accountant, BC notary, dealers in precious metals and stones, life insurance, real estate and securities sectors.
** Does not include other compliance enforcement activities, such as CARs. The number of examinations conducted may include multiple examinations on the same reporting entity.
*** Does not include FRFIs assessed by OSFI.

119. Canada specifies that, as recommended in the MER, FINTRAC has launched a more intensive compliance review of the money services business (MSB) and credit unions/*caisses populaires* sectors:

- the number of examinations in the MSB sector was stable from 2008 to 2010 (an average of 210 examinations each year). Due to the evaluated risks, the number of examinations of the sector considerably increased in 2011/2012 when 426 examinations were conducted on MSBs and was brought back to 222 in 2012/2013 (this includes both desk and on-site examinations). FINTRAC also launched CARs to the MSB sector (50 in 2013).
- FINTRAC has also increased the examinations of the credit unions/*caisses populaires* sector (more than 4 times higher in 2012/2013, as compared to 2008/2009, with a peak in 2011/2012). Canada indicates that the number of on-site visits is proportional to the assessed risk in the credit union/*caisses populaires* sector.

120. As for the decrease in the number of examinations in the life insurance sector (from 28 in 2008/2009 to 5 in 2011/2012, and then 13 in 2012/2013), Canada explains that this is correlated to the level of risk of the sector. Canada adds that life insurance has nevertheless been subject to continuing appropriate supervisory activities including:

- examinations of key market players/companies, including Canada's top financial conglomerates' life insurance companies by OSFI;
- a number of "broker/intermediary" examinations by FINTRAC;
- CARs being issued to the entire sector, including agents, brokers/intermediaries, and companies. Table 2 shows that the number of CARs sent to life insurance providers reached 1,559 in 2011/2012 and 829 in 2012/2013, as compared to 33 in 2010/2011.

OSFI (Office of the Superintendent of Financial Institutions) – primary regulator of banks and other federally-regulated financial institutions (FRFIs):

121. OSFI is a member of the Basel Committee on Banking Supervision and the International Association of Insurance Supervisors, and applies their Core Principles of supervision throughout its supervisory activities, including AML/CFT supervision. As discussed more fully in the MER, OSFI has been conducting AML/CFT supervision in the FRFI sector since 2004.

122. Canada informs that since the MER on-site, OSFI's AML supervisory unit has been transferred to OSFI's Supervision Sector and its assessment program more integrated into OSFI's overall supervisory framework. For example, in 2011-12, OSFI conducted 17 on-site AML/CFT assessments Three of these assessments were conducted at conglomerate financial groups with multiple FRFIs and other financial entities in each group (OSFI's supervisory expectations include a requirement to apply findings across financial groups, as applicable). The other 14 assessments were: 9 banks; 7 trust companies; and two loan companies. From April 2012 to March 2013, OSFI conducted 13 on-site AML/CFT assessments. Three of these assessments were conducted at conglomerate financial groups with multiple FRFIs and other financial entities in each group. The other 10 assessments were: 6 banks and 4 trust companies.

123. The FRFI sector includes Canada's largest banks and life insurance companies, which have a dominant market share domestically. They also have major banking and life insurance subsidiaries and branches in the USA, the Caribbean, Latin America and Asia. OSFI's AML/CFT assessment program is directed at these and other FRFIs which OSFI considers to be at the highest risk of ML and TF, and includes an assessment planning cycle[32]. OSFI applies its AML/CFT supervision to foreign branches and subsidiaries using a risk- based approach. FRFIs are assessed more frequently

[32] All FRFIs subject to the PCMLTFA (i.e. banks, trust companies, loan companies and life insurance companies) have been risk-rated according to inherent risk exposures to ML and TF of business activities, location of business activities and business strategies and structures. This inherent risk rating is used to determine OSFI's AML/ATF assessment planning cycle. The methodology groups FRFIs into three risk categories as follows:

- Higher (A) inherent risk – assessed every 3 years (including all conglomerate banking groups)
- Medium (B) inherent risk – assessed every 4 years (including all conglomerate life insurance groups)
- Lower (C) inherent risk – assessed every 5 years

than the planned cycle, irrespective of risk rating, when, for instance, a FRFI's program is found to have major deficiencies and it is determined that a re-assessment may be warranted outside of the assessment planning cycle.

124. Under the MOU with FINTRAC, OSFI provides FINTRAC with a copy of its examination (findings) letters, as well as the responses to them by FRFIs, and also reports to FINTRAC on all follow-up work. OSFI consults FINTRAC on an on-going basis to ensure that any concerns FINTRAC has are factored in to the monitoring program applied to the FRFI.

125. There were 59 low to very low risk FRFIs which were assessed by FINTRAC during 2011-2012 using their compliance assessment reports process.

126. In 2010, FINTRAC announced it would commence direct compliance examinations of FRFIs supervised by OSFI. This program began in 2011 but was discontinued. Despite attempts to reduce any potential or perceived burden on entities, the results of this approach in 2012 were unsatisfactory, as they evidenced a duplication of supervisory and compliance efforts. In 2013, OSFI and FINTRAC signed a concurrent assessments/examination framework,. Under this approach, OSFI will continue to focus on risk management processes and controls needed to ensure compliance; and FINTRAC will focus on the quality, volume and timing of reports submitted by FRFIs as part of their PCMLTFA obligations

General structure of the AML/CFT supervisory regime

127. In considering Canada's compliance with Recommendation 23 (and subsequently with Recommendation 24), the MER questioned the choice made by Canada to very much concentrate the AML/CFT supervisory functions in FINTRAC, considering the high number of reporting entities to be covered in the context of a federal state and different financial sectors. However, aside from the concurrent examination approach between OSFI and FINTRAC, and a list of MOUs signed by FINTRAC and provincial regulators[33], no further information has been provided by Canada.

128. One suggestion in the MER was that FINTRAC should delegate formally its compliance examination authority[34] to its MOU partners and other primary regulators (essentially to leverage existing examination resources and avoid possible duplication of compliance inspections). This was considered but not undertaken due to the importance for Canada to ensure consistent application of the regulations and legislation by reporting entities, and ensure clear accountability by retaining FINTRAC as the lead responsible competent authority with appropriate and specific Administrative Monetary Penalties (AMPs) powers under the PCMLTFA.

129. The MOU between FINTRAC and OSFI enables the two agencies to achieve coordinated supervision of FRFIs. Current arrangements and the new concurrent assessment approach substantially increase efficiency and reduce the regulatory burden on those businesses with reporting obligations. FINTRAC currently has 18 Memoranda of Understandings with provincial

33 See Annex 1 to the Fifth follow-up report.

34 As permitted under Section 43(5) of the PCMLTFA.

regulators[35] which enable the sharing of their examination findings at agreed upon intervals. These results can influence the scope of subsequent FINTRAC examinations.

130. **Conclusion**: from the various elements provided by Canada, it can be concluded that this deficiency has been largely addressed. FINTRAC has strengthened its compliance staff in charge of supervising reporting entities, which is a positive step to improve the balance of supervision between all sectors. At the same time though, the scope of reporting entities under the responsibility of FINTRAC has expanded. FINTRAC should therefore ensure that its resources develop in relation to its specific needs. It has to be noted that the application of a risk-based compliance approach as well as the development of new and better suited compliance tools should also enable FINTRAC and sector supervisors to better target the institutions posing higher risks and requiring enhanced supervision and onsite-examinations.

131. However, risk assessments of each of the reporting sectors would be needed to get a comprehensive view on the nature and level of risks to which Canada is exposed, and to make sure that FINTRAC's compliance resources and activities are optimally applied to the different reporting sectors. This would in particular give a stronger basis to evaluate if, overall, the sectors and institutions presenting higher risks benefit from the required level of attention from FINTRAC, including through onsite examinations.

132. Canada informed the Secretariat that FINTRAC conducts risks assessments for each reporting sector and these exercises inform the compliance activities conducted. Canada adds that it is currently working on a broader risk assessment of these sectors. An interdepartmental Risk Assessment Working Group led by the Department of Finance has been established and the Terms of Reference were approved in Spring 2013. In addition, the Department of Finance has initiated the development of an ML/TF threat assessment as an initial step towards a complete risk assessment. The interdepartmental Risk Assessment Working Group has met 4 times to date and will be meeting on a regular basis until the project is completed. The results of this ML/TF risk assessment will further inform FINTRAC's risk-based compliance program, as well as inform all other public and private sector organizations contributing to Canada's AML/CFT regime.

133. On the basis of the information available, with particular regard to sectors identified in the MER as appearing insufficiently supervised:

- As a result of a risk evaluation of the money services business activities, the number of desk and on-site examinations doubled in 2011/2012.
- As far as credit unions/*caisses populaires* are concerned, progress has been made with a number of on-site examinations in 2011/2012 6 times higher than in 2008/2009. FINTRAC has conducted 878 examinations over 4 years for a reporting sector that includes 870 reporting entities. It better reflects the level of risk of the sector.
- Based on the overall level of risk of life insurance, the sector has been subject to other, more appropriate compliance activities than examinations,

[35] See Annex 1 to the Fifth follow-up report.

including the extensive issuance of CARs. In addition, key life insurance market participants were subject to examinations.

c) "Fit and proper" requirements are not comprehensive - at the time of the on-site visit, there was no specific obligation for FRFIs to implement screening procedures for persons who are hired, or appointed to the Board after the initial incorporation or authorisation procedures are concluded.

134. OSFI Guideline E-17 – *Background Checks on Directors and Senior Management of FREs*[36] came into effect in January 2009 and requires FRFIs supervised by OSFI to implement on-going fit and proper standards for directors and senior officers of FRFIs. E-17 sets out screening requirements including criminal background checks that must be done prior to appointment. The guidance also requires each FRFI to have policies for updating all fit and proper assessments of senior officers and directors at regular intervals (no longer than 5 years).

135. OSFI's authority to require FRFIs to conduct screening procedures for those who are hired, or appointed to the Board, after the initial incorporation or authorisation procedures are concluded, lies in its prudential mandate under federal financial sector legislation in Canada. All the OSFI AML assessments referred to above contained a module focussing on compliance with E-17, and remedial measures were required by OSFI in most cases, in order to ensure that FRFIs were implementing the measures contained in the guideline.

136. **Conclusion**: Canada has not taken any further action to ensure that market entry rules among the different provinces and sectors are compliant with FATF requirements[37]. The MER points out the lack of harmonisation of the requirements in terms of market entry among the federal and provincial levels and among the different provinces. This deficiency has not been addressed.

d) There is currently no registration regime for MSBs.

137. Canada implemented a federal registration regime for MSBs which has been in force since June 2008. Money services providers have to register with FINTRAC. The registration obligation applies to businesses engaged in foreign exchange dealing activities, remitting or transmitting funds by any means or through any person, entity or electronic funds transfer network; or issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments (except for cheques payable to a named person or entity). It also applies to alternative money remittance systems (such as Hawala, Hundi or Chitti).

138. Applicants for registration have to provide identifying information as well as other specific business information (location of the business, organisational structure of the business, information about the compliance officer, about the agents etc) to FINTRAC. Any change to that information has to be notified to FINTRAC within 30 days and the registration has to be renewed every two years.

36 www.osfi-bsif.gc.ca/Eng/Docs/E17_final.pdf and Mutual evaluation report of Canada, 2008, paragraph 1076.

37 Mutual evaluation report of Canada, 2008, paragraph 1163.

Table 5. **Number of MSBs that have registered**

Year	2008/09	2009/10	2010/11	2011/12	2012/13
# of MSBs registered	803	954	955	890	788

Note. Canada informs that the variation in the number of registered MSBs from year to year is primarily attributable to market-related dynamics in a sector where entry and exit are relatively frequent.

139. Canada also mentions that FINTRAC has developed and published a pamphlet that explains the legal obligations of MSBs in eight languages (Arabic, Chinese, Farsi, Punjabi, Spanish and Vietnamese, as well as French and English) to better communicate with this important business sector.

140. **Conclusion**: This deficiency has been addressed.

Recommendation 23 – Overall conclusion

141. From the various elements provided by Canada, it seems that FINTRAC has strengthened its compliance staff in charge of supervising reporting entities, which is a positive step to better balance the level of supervision between all sectors falling under the remit of FINTRAC. At the same time though, the scope and number of reporting entities under the responsibility of FINTRAC has expanded in terms of sectors covered (to dealers in precious metal and stones, and BC notaries)[38]. FINTRAC should therefore ensure that its resources continue to be sufficient in relation to its specific needs.

142. It has to be noted that the application by FINTRAC of a risk-based compliance approach as well as the development of new and better suited compliance tools and the conclusion of an agreement with OSFI to improve supervisory coordination should also enable FINTRAC to better target institutions posing higher risks and requiring enhanced supervision and onsite-examinations.

143. Regarding the particular sectors identified in the MER as appearing insufficiently supervised: as a result of a risk evaluation of the money services business activities, the number of desk and on-site examinations doubled in 2011/2012. As far as credit unions/*caisses populaires* are concerned, progress has been made with a number of on-site examinations in 2012/2013 4 times higher than in 2008/2009. Based on the overall level of risk of life insurance, the sector has been subject to other, more appropriate compliance activities than examinations, including the extensive issuance of CARs.

144. The deficiency regarding the "fit and proper" requirement has not been addressed, as Canada has not taken any further action to ensure that market entry rules among the different provinces and sectors are compliant with FATF requirements.

145. Canada has implemented a federal registration regime of MSBs since June 2008.

146. This means that Canada has implemented Recommendation 23 at an adequate level of compliance.

[38] The comparison in terms of number of reporting entities between the situation at the time of the MER and 2011/2012 is difficult to make as it seems that the distinction between primary and secondary reporting institutions (see table 4) was not applied in 2007/2008.

Recommendation 26 – description and analysis

*a) FINTRAC has insufficient access to intelligence information from administrative and other authorities (especially from CRA [Canada Revenue Agency], CSIS [*Canadian Security Intelligence Service*] and CBSA [Canada Border Services Agency]).*

147. Canada indicates that in 2008, FINTRAC obtained access to the Canadian Police Information Centre (CPIC) database. CPIC is a national repository of police information that amounts to a shared resource within Canadian law enforcement. Currently, CPIC handles in excess of 120 million queries and stores 9.6 million records in its investigative data banks.

148. In 2009, FINTRAC took part in Canada's National Integrated Interagency Information (N-III) initiative, which focused on improving the access, collection, use and distribution of information among federal, provincial and municipal partners involved in public safety and security. The N-III initiative included the development of a Police Information Portal (PIP) that facilitates information sharing among police agencies across the country. It also introduced the Public Safety Portal (PSP)), which allows federal departments and agencies to query law enforcement databases in accordance with their legislated mandates. FINTRAC obtained access to national law enforcement databases under the N-III initiative in February 2010. FINTRAC analysts utilize the CPIC and the PSP through the identification of individuals, their criminal involvement/activities, known associates and to assist in identifying additional financial intelligence that is relevant to FINTRAC disclosure recipients. Canada informs that access to these databases allows analysts to search data from over 40 000 contributors from police agencies across Canada.

149. Canada states that FINTRAC connection to these new information sharing tools is a positive step to facilitate access to information used by law enforcement authorities such as the RCMP or the CBSA.

150. Canada adds that FINTRAC successfully negotiated access to additional law enforcement and security databases that will provide valuable new sources of information to further assist the FINTRAC's financial intelligence products in the detection, prevention and deterrence of money laundering and the financing of terrorist activities.

151. **Conclusion**: several positive steps have or are being taken, and the deficiency has been substantially addressed. FINTRAC's expanded connections with law enforcement authorities has broadened its access to intelligence information, especially in the field of law enforcement and national security. FINTRAC now has indirect access to the CSIS database through a querying process which allows FINTRAC to determine whether CSIS has information on individuals or entities that may pose a terrorist financing threat. The positive or negative results of such queries assist FINTRAC in reaching or not reaching their disclosure threshold. FINTRAC will also get access to similar information as the CBSA.

152. No information was provided regarding FINTRAC's direct or indirect access to the CRA database, as recommended in the MER.

b) FINTRAC is not allowed by the PCMLTFA to gather additional financial information from reporting entities.

153. Canada advises that the Canadian Constitutional framework does not permit FINTRAC to go back to reporting entities and ask for additional information on the STR they have filed. However, Canada considers that in most cases, the STR provides clear and comprehensive information, and requests for additional elements would not be applicable.

154. Canada indicates that within FINTRAC, a formal framework of information exchange is in place between the department responsible for compliance issues and the department in charge of analyzing information from reporting entities, called the analytical sector. Under this mechanism, the analytical sector provides awareness-raising information on compliance issues. Canada also informs that since June 2010, FINTRAC's analytical sector has issued Intelligence Notices to its compliance sector. These notices range from non-compliance issues involving data quality and missing information to suspicions of non-reporting by reporting entities. These notices can be submitted on any of the following types of reports that FINTRAC receives: Suspicious Transactions Reports (STRs), Large Cash Transaction Reports (CAD 10,000/USD 9,548 or more in cash in the course of a single transaction), Electronic Funds Transfers Reports (EFTRs), Terrorist Property Reports, and Casino Disbursements Reports (of CAD 10,000 or more whether paid in cash or not, in the course of a single transaction).

155. An Intelligence Notice can be issued for individual reports or a block of reports. Intelligence notices help inform the prioritization of Compliance Program activities.

156. Canada considers that this framework assists FINTRAC's compliance sector in improving the quality and completeness of reports received from reporting entities, and further strengthening the report database.

157. **Conclusion**: the information sharing mechanism put in place by FINTRAC seems to be a useful tool to enhance coordination which may help improve the quality and usefulness of information provided by reporting entities, which in turn could help limit further the need for additional information on STRs. However these measures are indirect and there is still no possibility for FINTRAC to collect additional financial information from the reporting entity. The deficiency has not been adequately addressed.

c) Effectiveness - the number of staff dedicated to the analysis of potential ML/FT cases is low especially in comparison with the amount of reports coming in, which may have an impact on the number of cases that FINTRAC generate.

158. The total number of employees at FINTRAC has increased significantly since the 2008 MER. FINTRAC counted 384 full-time employees in 2012/2013, as compared to 271 in 2007/2008. FINTRAC staff working on tactical analysis (responsible for developing cases and disclosures) amounted to 71 full-time employees as of September 2013, as compared to 36 at the time of the MER.

159. In 2012/2013, FINTRAC received 79 294 STRs, as compared to 50 354 in 2007/2008[39]. It made 919 disclosures in 2012/2013, as compared to 210 in 2007/2008[40]. A disclosure can contain multiple STRs, information from the several other reports FINTRAC receives, and information from the various databases and open source materials available to FINTRAC to undertake value-added analysis.

Table 6. **Number of STRs received each year by FINTRAC**

Year	Number of STRs received
2007-08	50 354
2008-09	67 740
2009-10	64 240
2010-11	58 722
2011-12	70 392
2012-13	79 294

Sources: FINTRAC Annual Reports 2012 and 2013

160. **Conclusion**: This deficiency has been largely addressed. FINTRAC's analytical capacities have been doubled, while in the same period, the number of STRs received by FINTRAC has gone up by 57% and the number of disclosures is more than 4 times higher in 2013 than in 2008. This shows that the substantial increase in staff number led to considerable progress in the Centre's quantitative contribution to investigations.

161. General conclusions on the number of cases generated by FINTRAC have to be drawn in relation not only to the number of disclosures made by FINTRAC but also to the use of STRs received by FINTRAC, the added value of FINTRAC's disclosures in investigations and the ML or TF convictions based on FINTRAC disclosures. Given the limited scope of this desk-based follow-up report, it is not possible to draw final conclusions regarding progress made by FINTRAC to generate cases.

162. In any event, Canada should ensure that its resources always meet its actual needs and that activities related to the analysis of potential ML/FT cases are in the hands of an adequately staffed agency.

d) Effectiveness - feedback from law enforcement authorities outlines the relatively limited added value of FINTRAC disclosures in law enforcement investigations.

163. Canada mentions that FINTRAC has used feedback from its disclosure feedback forms (DFF) to improve disclosures, and has strengthened relationships through continued outreach and regular

39 FINTRAC Annual Report 2013 www.fintrac-canafe.gc.ca/publications/ar/2013/1-eng.asp#s8.4 – The other reports included Electronic Funds Transfers Reports (EFTRs), Large Cash Transaction Reports (LCTRs), Cross-Border Currency Reports/Cross Border Seizure Reports.

40 FINTRAC Annual Report 2013 www.fintrac-canafe.gc.ca/publications/ar/2013/1-eng.asp#s8.4.

dialogue at all levels (from analysts to Director) with the RCMP, CRA, CBSA and other law enforcement or national security agencies across Canada. From 2008-2009 to 2012-2013, FINTRAC received 2106 disclosure feedback forms from domestic and international disclosure recipients and within this time period the response rate for disclosure feedback forms increased from 17% (2008-2009) to 32% (2012-2013). These have highlighted areas in which FINTRAC can take steps to strengthen its disclosure products.

164. Partners have for example indicated in the past that a detailed, narrative overview of the financial transactions in a case is very useful. Based on this feedback, FINTRAC indicates that it now provides a comprehensive narrative overview of the transactions and designated information with the majority of cases disclosed to law enforcement. Based on the feedback from partners, FINTRAC also includes a relationship chart of the parties to the transactions which disclosure recipients find very useful. FINTRAC also provides its partners with an enhanced disclosure package, containing multiple document formats.

165. Canada states that FINTRAC receives positive feedback from law enforcement and security partners on the usefulness, relevance and timeliness of case disclosures. Increasingly, law enforcement agencies are providing the Centre with information concerning their highest priority investigations. This enables FINTRAC to assist in cases that are of the highest priority to its investigative partners and to be of greater assistance to their work.

166. Canada indicates that a number of initiatives have been taken to improve FINTRAC's ability to produce high quality intelligence to be used in investigations and prosecutions. Examples of initiatives taken to specifically improve the quality of disclosures include:

- Legislative provisions in force since June 2008 allow disclosures to be enriched with a greater range of information on financial transactions. Additional reporting sectors (Dealers of Precious Metals and Stones, British Columbia Notaries) and report types (Casino Disbursement Reports) have increased the range of information disclosed to FINTRAC's partners;
- FINTRAC has developed additional augmented disclosure products that increase the focus and timeliness of disclosures to its partners, resulting in improved communication with disclosure recipients. FINTRAC has streamlined its disclosure process, primarily through changes to its case approval process[41];
- FINTRAC continues to conduct operational meetings and discussions with disclosure recipients to discuss investigative priorities, analytical processes,

[41] Previously, all disclosures were approved in a five-step process in the following order: Manager of Analysis, Legal Services, Assistant Director Financial Analysis and Disclosures and Deputy Director and final approval by the Disclosure Committee (usually meeting once a week). FINTRAC has now adopted a risk-based approach regarding the decision-making process involved for disclosures. Disclosures are approved by the Manager and Assistant Director, Financial Analysis and Disclosures in low-risk cases. Compulsory legal review of each case and final approval by Disclosure Committee is no longer mandatory, resulting in faster dissemination. If required, disclosures may still be forwarded to Legal Services for review and only when the disclosure is considered a high-risk, the Disclosure Committee will have final approval.

the development of indicators, and to provide assistance regarding the use of FINTRAC disclosures.

167. Canada underlines that FINTRAC ensures alignment with law enforcement and national security regime partners' priorities through participation in the Canadian Association of Chiefs of Police and its committees dealing with organized crime and national security, as well as the Canadian Integrated Response to Organized Crime committee. A highlight for FINTRAC in past years was the formal recognition by the Canadian Association of Chiefs of Police that FINTRAC's financial intelligence "*should be made an integral part of all organized crime investigations*." For Canada, this endorsement is indicative of the role that FINTRAC has played in these types of cases in recent years. It also reinforces the important role of financial intelligence in certain types of complex investigations.

168. *Disclosures to the RCMP* - Canada states that the RCMP has noted that initiatives undertaken by FINTRAC since the MER (including streamlined approval process and more direct ongoing dialogue with partners) have enhanced the value-added of FINTRAC's disclosures to the RCMP and others. Canada indicates that FINTRAC has disclosed useful intelligence and new leads on persons or businesses of interest to the RCMP. Regarding their partnership with FINTRAC, the RCMP states that: *"FINTRAC is considered a key partner and has provided valuable financial intelligence on an ongoing basis that contributed to terrorist financing investigations." FINTRAC through their disclosures identified new linkages/nexus between entities and/or individuals through financial transactions which surfaced new avenues of investigation. FINTRAC has always responded in a timely fashion to our priority Voluntary Information Records."* - RCMP Anti-Terrorist Financing Team, National Security Criminal Operations, Headquarters, Ottawa[42]

Table 7. **FINTRAC disclosures to the RCMP**

Year	Number of distinct disclosures	Number of disclosure packages* (includes disclosures sent to multiple RCMP recipients)
2008-2009	392	710
2009-2010	363	617
2010-2011	459	883
2011-2012	494	914
2012-2013	580	1,088
Total	2 288	4 212

*Note that the number of disclosure packages sent to the RCMP includes disclosures being sent to multiple individual recipients within the RCMP. Individual cases may therefore have been disclosed a number of times.

42 Quoted in FINTRAC's Annual Report 2012 www.fintrac-canafe.gc.ca/publications/ar/2012/1-eng.asp?a=5#s5.

Table 8. **FINTRAC disclosures to other domestic law enforcement and national security agencies**

Year	Municipal Police	Provincial Police	CRA	CSIS	CBSA
2008-2009	164	58	157	59	82
2009-2010	136	119	125	78	42
2010-2011	143	162	136	120	82
2011-2012	153	167	136	107	89
2012-2013	182	198	150	164	144
Total	**778**	**704**	**704**	**528**	**439**

169. *Disclosures to the CRA* - Canada states that based on the MER recommendations and after tax evasion was made a predicate offense in 2010/2011, FINTRAC has been able to build more cases for disclosure to the CRA. According to information from Canada, the CRA notes that the information provided in disclosures received since April 2008 is detailed, timely and very useful.

170. The majority of the disclosures received from FINTRAC were reviewed and assessed by the Special Enforcement Program (SEP), a group responsible for auditing those suspected of being involved in illegal activities. Until March 2013 compliance action on FINTRAC referrals was completed by the SEP. Due to organizational changes, the SEP has been discontinued and this work is now being completed by auditors within the Small and Medium Enterprises Directorate (SMED). The Criminal Investigations Program (CIP) continues to receive and analyze all FINTRAC disclosures for intelligence and potential criminal investigations before referring them to the SMED workload development area.

171. *Disclosures to the CSIS.* Canada indicates that CSIS has noted that the quality of the information and analysis contained in disclosures - 164 in 2012/2013 - reflects the growing number of reporting entities, case complexity, and FINTRAC's maturity as an organization.

172. *Disclosures to CBSA*. Canada quotes the CBSA expressing their satisfaction on FINTRAC disclosures (144 received in 2012/2013): "*As a result of the information provided, we were able to recommend to Citizenship and Immigration Canada that our subject be deemed inadmissible to Canada based on s. 37(1) of the Immigration and Refugee Protection Act. We have also indicated that the subjects who are permanent residents be scrutinized further should they apply for citizenship.*" – *CBSA*[43]

173. **Conclusion**: information and data provided by Canada reflect that coordinated measures have been taken by FINTRAC to enhance the overall quality of its disclosures and better support law enforcement and national security investigations: use of feedback from disclosure recipients, better tailored disclosure process, dialogue with law enforcement authorities about their expectations and alignment with their priorities, better use of financial intelligence etc. This has resulted in a general

[43] Quoted in FINTRAC Annual Report 2012 www.fintrac-canafe.gc.ca/publications/ar/2012/1-eng.asp?a=5#s5.

level of satisfaction expressed by some law enforcement and national security authorities about FINTRAC's contribution to their investigations. This deficiency has been substantially addressed.

e) Effectiveness - the timeliness of FINTRAC disclosures to law enforcement authorities was raised as an issue at the time of the on-site visit.

174. Canada indicates that FINTRAC has significantly improved the timeliness of disclosures: since the MER, the average case disclosure turnaround time has decreased by approximately 84%. FINTRAC's broad review and revision of its disclosure process has allowed for routine disclosures to be approved more quickly, provided access to new data sources, increased the number of analysts, and led to more effective information systems and adjustments made in response to feedback from partners.

175. FINTRAC has also developed disclosure feedback forms (DFFs)[44], which it sends with each disclosure. Recipients of FINTRAC's disclosures have indicated on the DFFs that the information provided was timely and useful. For example, the RCMP says that *"FINTRAC provided us with timely information. The information helped us identify the financial institutions and the bank accounts that were used by the subjects. This information will be used to obtain judicial authorizations".* - [Translation] – RCMP, "C" Division, POC [45]

176. **Conclusion**: based on the information provided by Canada, it seems that progress made with regard to the timeliness of FINTRAC disclosures to law enforcement authorities has been confirmed. This deficiency has been addressed.

f) Effectiveness - 80% of the disclosures made by FINTRAC result from voluntary information from law enforcement; only 20% result from STRs which raises serious concerns with respect to the capability of FINTRAC to generate ML/TF cases on the basis of STRs or other reports it receives from the private sector.

Table 9. **FINTRAC disclosures and the number of reports received since 2008/2009**

Years	2008-2009	2009-2010	2010-2011	2011-2012	2012-2013
Number of disclosures	556	579	777	796	919
Number of reports received (all types of reports) *	24 264 077	24 826 336	19 266 541	18 529 956	19 746 005

*. STRs, LCTRs, EFTRs, Terrorist Property Reports, and Casino Disbursements Reports, see paragraph 153.

Variation in reporting volumes can be due to many factors, which, among others, include economic trends, market share of various reporting entities and the fact that two reporting entities changed their process with respect to EFT reporting.

44 See paragraph 163.

45 Quoted in FINTRAC Annual Report 2012 www.fintrac-canafe.gc.ca/publications/ar/2012/1-eng.asp?a=5#s5.

Table 10. **Number of STRs used in disclosures since 2008/2009**

	2008-09	2009-2010	2010-2011	2011-2012	2012-2013
STR	4 060	4 100	4 339	4 273	4 739

178. These figures show that the number of FINTRAC disclosures has significantly increased between 2009 and 2013 (+65%), but the number of STRs used has not evolved in the same proportions (+16%).

179. It should be noted that, in addition to STRs, FINTRAC receives many other types of reports which provide value added when conducting analysis and making disclosures.

Table 11. **Distribution of case originators per fiscal year**

Originator	2008-2009	2009-2010	2010-2011	2011-2012	2012-2013
Proactive					
Open Source	3%	3%	3%	1%	2%
Report Profiling	5%	3%	0.4%	1%	0%
STR	13%	8%	8%	9%	8%
Total Proactive	**21%**	**14%**	**11%**	**12%**	**10%**
VIR (Voluntary Information Record)	**59%**	**63%**	**65%**	**64%**	**69%**
FIUQ (Foreign FIUs queries)	**20%**	**22%**	**24%**	**24%**	**21%**
Other	**0%**	**1%**	**0.3%**	**0%**	**0%**

Note: the total of each column will not always equal 100% due to the rounding of numbers.

180. In 2012/2013, 69% of the disclosures made by FINTRAC resulted from voluntary information provided by law enforcement authorities, and 8% from STRs. At the time of the MER, the proportions were respectively 80% and 14%. The proportion of VIRs (Voluntary Information Records) started decreasing after the MER which seemed to reflect a better balance between the different sources of cases, but it is now increasing again and represents more than two third of total disclosures. In addition, the proportion of proactive disclosures stemming from STRs has also gone down, and has decreased since the MER (from 14% to 8% in 2012/2013), while the proportion of proactive disclosures in total has also halved since 2008-09.

181. **Conclusion**: on the basis of the figures provided, it seems that further efforts have to be developed to ensure that initial progress made during the period 2008/2009 can be further enhanced. FINTRAC has reviewed its approach to STRs, and ensured that the processes and capabilities in place have and will continue to lead to an effective use of STRs on a continuous basis, resulting in more cases being generated from this category of reports. The deficiency has been partially addressed.

182. Canada advises that STRs, Electronic Funds Transfers Reports (EFTRs), Large Cash Transaction Reports (LCTRs), and other reports and information received by FINTRAC are an extremely valuable source of financial intelligence. A total of 407,835 of those reports were included in cases disclosed between 2007 and 2011. Of that number, 60% were EFTRs, followed by LCTRs at 36%, STRs at 33%, Cross-Border Currency Reports (CBCRs) at 0.6% and Casino Disbursement Reports (CDRs) at 0.5%. Interestingly, the percentage of cases containing at least one STR is similar to the percentage of cases including at least one EFTR or LCTR. This is significant since the volume of the STRs submitted to FINTRAC is much lower than that of EFTRs and LCTRs. STRs are particularly useful for providing additional information related to individual behaviour and transactional activity[46].

183. Approximately 88% of the total STRs submitted to FINTRAC between November 2001 and August 2010 were from three main business sectors: banks and trusts/loans, money services businesses (MSBs) and credit unions/*caisses populaires*[47]. Although high volumes of STR reporting does not necessarily correlate to high quality STRs, it could be useful to consider launching further initiatives to raise awareness of reporting entities with low reporting volumes, explain the importance and the benefits of their contribution to the process, and encourage them to fill STRs reports, as and when appropriate.

g) Effectiveness - so far, very few if any convictions for ML or TF have resulted from a FINTRAC disclosure which is an additional factor to consider when looking at FINTRAC's ability to produce intelligence to be used in criminal investigations and prosecutions.

184. As noted above (par 165 and s.), the RCMP and CSIS have informed that FINTRAC disclosures are making significant contributions to new and ongoing investigations for money laundering and terrorist financing, and these disclosures are increasing significantly. Law enforcement indicates that FINTRAC disclosures provide information that advance investigations. Canada reports that of the disclosures produced proactively by FINTRAC in 2012/2013, 84% were considered relevant to an investigation and 72% were considered useful.

185. Canada reports that the RCMP receives the most significant number of FINTRAC's case disclosures of financial intelligence and that FINTRAC intelligence contributes to AML/CFT investigations by the RCMP. Canada adds that it is now standard procedural practice for all RCMP investigative bodies in Canada to use FINTRAC intelligence[48]. In addition, Canada informs that civil forfeiture is another avenue used by federal, provincial and municipal police forces in Canada.

186. **Conclusion**: Based on information provided by Canada, it seems that FINTRAC intelligence, is used in cases of ML/TF investigation. However, and in the context of this desk-based review, it is not possible to check the degree and the extent to which FINTRAC intelligence is used by investigation

46 Trends in Canadian Suspicious Transaction Reporting, April 2011 www.fintrac-canafe.gc.ca/publications/typologies/2011-03-eng.asp#s2.

47 Trends in Canadian Suspicious Transaction Reporting, April 2011 www.fintrac-canafe.gc.ca/publications/typologies/2011-03-eng.asp#s2.

48 See Toronto Police Service in FINTRAC Annual Report, 2013 p. 17

agencies, and there is no information available as to ML or TF convictions resulting from a FINTRAC disclosure. The deficiency has been partially addressed.

Recommendation 26 – conclusion

187. Based on the information provided by Canada, it seems that FINTRAC has expanded its access to information from other national authorities, especially CSIS and CBSA. But there was no progress made regarding FINTRAC's ability to require additional information from reporting entities.

188. As far as effectiveness of FINTRAC is concerned, given the limited scope of this desk-based follow-up report, it is not possible to draw final conclusions regarding progress made by FINTRAC to generate cases. In any event, Canada should ensure that its resources always meet its actual needs and that activities related to the analysis of potential ML/FT cases are in the hands of a sufficiently staffed body.

189. FINTRAC has taken measures to enhance the overall quality of its disclosures and better support law enforcement investigations. Although satisfaction is expressed by some law enforcement authorities, it seems difficult to draw some general conclusions as to the extent to which FINTRAC's disclosures positively contributed to the success of the investigations. Further efforts will be needed to ensure that initial progress on the proportion of STRs used by FINTRAC to generate ML/FT cases will be sustained. It is hoped that over time positive progress will be reported on the level of ML/TF convictions resulting from a FINTRAC disclosure.

190. This means that Canada has implemented Recommendation 26 at an adequate level of compliance.

VI. SUMMARY OF KEY ACTIONS TAKEN BY CANADA TO ADDRESS THE DEFICIENCIES IN RELATION TO NON-CORE AND NON-KEY RECOMMENDATIONS RATED PC OR NC

191. The scope of the present 6th FUR report is limited to the progress made in relation to the core and key Recommendations that were rated as PC or NC in the MER, i.e. Recommendations 5, 23 and 26.

192. In the 2009 FUR, significant progress was acknowledged for Recommendations 6, 8, 12, 16, 17, 22, 24, 30, SR VI, and SR VII and more limited progress was noted for Recommendations 7, 9, 11, 21, 33, and 34.

193. In particular,

- requirements for financial institutions in relation to Politically Exposed Foreign Persons (PEFPs) were introduced in June 2008 through amendments to the PCMLTFA and PCMLTFR, and specified the enhanced customer identification and due diligence requirements for this category of clients;
- non face-to-face CDD measures were introduced by the PCMLTFR in June 2008;

- the amended PCMLTFA explicitly requires financial institutions to ensure that their subsidiaries and branches located in a country that is not a member of the FATF, develop and apply policies and procedures that are consistent with Canadian requirements for record keeping, verifying identity and maintaining a compliance regime when the local laws permit it;
- a federal registration regime for money service businesses (MSBs) has been in force since June 2008. Money services providers have to register with FINTRAC;
- new provisions to the PCMLFTA came into force in December 2008 and extended the scope of the AML/CFT regime:
    - British Columbia (BC) Notaries Public and notary corporations (hereafter referred to as BC Notaries) are subject to the PCMLTFA when they engage in any of the following activities on behalf of any person or entity: (a) receiving or paying funds, other than in respect of professional fees, disbursements, expenses or bail; or (b) giving instructions in respect of any activity referred to in paragraph (a);
    - Dealers in precious metals and stones (DPMS) are subject to the PCMLTFA if they engage in the purchase or sale of precious metals, precious stones or jewellery in an amount of $10,000 or more;
    - Credit union centrals have been brought under the PCMLTFR for all their activities;
- the PCMLTF Administrative Monetary Penalties (AMP) Regulations came into force in December 2008. The Regulations provide FINTRAC with the power to apply monetary penalties (civil penalties) to any financial institution and DNFBPs subject to the AML/CFT regime, for non-compliance with the PCMLTFA.

194. Since the 1st FUR, Canada has continued to take actions with a view to address the remaining deficiencies. However, in the context of this report, no further analysis has been conducted of measures taken to address the deficiencies in relation to other Recommendations rated PC (R.7, R.11, R.17, R.21,R.30, R.34), or NC (R.6, R.8, R.9, R.12, R.16, R.22, R.24, R.33, SRVI, SRVII). In October 2012, Canada provided updated information on initiatives taken to make progress on these Recommendations. A detailed description of those initiatives taken since the 2008 MER may be found in Annex 2.

195. Below is a short summary of the key measures taken by Canada.

Amendments to the PCMLTFR

196. While the amendments to the PCMLTFR which came into force on 1 February 2014 were largely aimed at addressing the remaining deficiencies in relation to Recommendation 5 and

customer due diligence requirements, Canada considers that these amendments will have positive implications for its compliance with a number of other non-core and key Recommendations. In particular, the regulations will positively impact Canada's compliance with Recommendations 6, 7, 8, 11, 12, 16, 21, 22, 33 and 34.

Scope of the AML/CFT regime

197. Canada reports that new provisions of the PCMLTFA came into force n July 2010 and extended the AML/CFT regime to credit union centrals. However TCSPs remain completely exempted from the AML/CFT framework as they were assessed as low risk[49].

198. With respect to legal counsel and legal firms[50], Canada advises that new Regulations imposing client identification due diligence and record-keeping obligations on legal counsel came into force on 30 December 2008. However, these provisions are currently inoperative as a result of a court ruling and related injunctions. In October 2013, the Supreme Court of Canada granted leave to appeal the ruling.

Sanctions regime

199. Canada reports that FINTRAC's criteria for public naming of reporting entities that have been subject to an administrative monetary penalty changed in June 2013. Under the new criteria, a person or entity subject to an administrative monetary penalty is named publicly if one of the following criteria is met: the person or entity has committed a very serious violation; or the base penalty amount is equal to or greater than CAD 250,000 (USD 233,987), before adjustments are made in consideration of the person or entity's compliance history and ability to pay; or repeat significant non-compliance on the part of the person or entity. Since 2009/2010, FINTRAC has issued 41 notices of violation, and made public on its website a list of 27 administrative monetary penalties, including 19 relating to money service businesses.

Resources of law enforcement and investigative authorities

200. Based on information provided by Canada, since 2008-2009 FINTRAC's resources has increased in the compliance section from 49 to 87 staff, and staff responsible for developing cases and disclosures amounted to 71 full-time employees in 2013, as compared to 36 in 2008[51]. FINTRAC also received additional funding in 2010 and part of this ongoing funding was specifically earmarked to enhanced FINTRAC's compliance programme.

201. Canada also states that:

- in July 2012, the RCMP Federal Policing adopted a new organisation model, to allow the Force to better align its resources to priorities and become more efficient and results-driven. Under this new model, the RCMP Federal

[49] Canada explains that the conclusion that the TSCP sector is low risk is made on the basis that the ML/TF risk is offset by tax laws that require all businesses to register and file company information to the CRA.

[50] Which include Quebec notaries.

[51] See table 1 and paragraphs 103 and 158.

Policing maintain specialized members to investigate money laundering and terrorist activity financing on operations undertaken in line with their National strategic priorities of Serious and Organized Crime, Financial Integrity and National Security;

- the Department of Justice's International Assistance Group regularly provides training to Canadian police forces and prosecutors in the area of mutual legal assistance (MLA), including a section devoted to MLA requests related to restraint and forfeiture of assets, either on behalf of foreign country regarding assets located in Canada, or on behalf of Canada regarding assets sought to be restrained/forfeited by a foreign state on Canada's behalf;
- since 2008, the Public Prosecution Service of Canada (PPSC) has undertaken training on ML and TF, including at the School for prosecutors where for one week in 2008, 2009, 2010, and 2011, lectures on different issues, including proceeds of crime and money laundering, were given to approximately 50 to 75 prosecutors. In September 2013, the PPSC's national and regional terrorism prosecutions co-ordinators (approximately 30) met for an intensive three day workshop to discuss legal and operational issues relating to the investigation and prosecution of terrorism offences in Canada. Finally, PPSC has an Integrated Proceeds of Crime e-mail network which allows for timely exchange of best practices and consideration of novel circumstances and recent jurisprudence on money laundering and terrorist financing.

G8 Action Plan on Transparency of Corporations and Trusts

202. In June 2013, the Government of Canada committed to a G-8 Action Plan on Transparency of Corporations and Trusts. Part of the Action Plan includes a commitment to consult publicly on the issue of corporate transparency, including with respect to bearer shares, nominee shareholders, the ability of competent authorities to access information on beneficial ownership, as well as the possibility of establishing a central registry for entities incorporated under the Canada Business Corporations Act (CBCA).[52]

[52] The action plan can be viewed here http://pm.gc.ca/eng/media.asp?id=5547.

REFERENCES

FATF (2008), Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism, Paris, France, www.fatf-gafi.org/countries/a-c/canada/documents/mutualevaluationofcanada.html.

FATF (2009),Third Round of AML/CFT Evaluations Processes and Procedures, Paris, France www.fatf-gafi.org/media/fatf/documents/process%20and%20procedures.pdf.

FINTRAC (n.c.), Guideline 6, Recording Keeping and Client Identification, www.fintrac-canafe.gc.ca/publications/guide/guide6/6-eng.asp.

FINTRAC (2011), Trends in Canadian Suspicious Transaction Reporting, April 2011, www.fintrac-canafe.gc.ca/publications/typologies/2011-03-eng.asp#s2.

FINTRAC (2012), Annual Report, Harnessing the Power of Financial Intelligence, www.fintrac-canafe.gc.ca/publications/ar/2012/1-eng.asp?a=5#s5

FINTRAC (2013), Annual Report 2013, www.fintrac-canafe.gc.ca/publications/ar/2013/1-eng.asp#s8.4

Canada's Economic Action Plan (2010), Budget 2010, Leading the Way on Jobs and Growth, Ottawa, Canada, www.budget.gc.ca/2010/pdf/budget-planbudgetaire-eng.pdf

Canada Gazette (2013), Canada Gazette Part II, Statutory Instruments 2013 SOR/2013-7 to 17 and SI/2013-3 and 5 to 12, Pages 280-384, Ottawa, Canada www.gazette.gc.ca/rp-pr/p2/2013/2013-02-13/pdf/g2-14704.pdf.

Canada Senate (2013), *Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really,* Report of the Standing Senate Committee on Banking Trade and Commerce, www.parl.gc.ca/Content/SEN/Committee/411/banc/rep/rep10mar13-e.pdf.

Capra International (2010), 10-Year Evaluation of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, Final Evaluation Report Presented to Department of Finance Canada, Cumberland ON, Canada www.fin.gc.ca/treas/evaluations/amlatfr-rclcrpcfat-eng.asp.

Justice Laws Website (2009), Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (SOR/2007-292), http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/index.html

Justice Laws Website (2010), Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (SOR/2002-184), http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/

Justice Laws Website (2010), Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (SOR/2002-184), http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/index.html.

Justice Laws Website (2012), Freezing Assets of Corruption Foreign Officials (Tunisia and Egypt) Regulations (SOR/2011-79), http://laws-lois.justice.gc.ca/eng/regulations/SOR-2011-78/index.html

Justice Laws Websites (2013), Proceeds of Crime (Money Laundering and Terrorist Financing Act (S.C. 2000, c. 17), http://laws-lois.justice.gc.ca/eng/acts/P-24.501/index.html.

Office of the Superintendent of Financial Institutions Canada (2008), Deterring and Detecting Money Laundering and Terrorist Financing, Ottawa, Canada, www.osfi-bsif.gc.ca/Eng/Docs/b8.pdf

Office of the Superintendent of Financial Institutions Canada (2008) Background Checks on Directors and Senior Management of FREs, Ottawa, Canada, www.osfi-bsif.gc.ca/Eng/Docs/E17_final.pdf

Prime Minister of Canada (2013), Canada's G-8 Action Plan on Transparency of Corporations and Trusts, Enniskillin, Northern Ireland, 18 June 2013, http://pm.gc.ca/eng/news/2013/06/18/canadas-g-8-action-plan-transparency-corporations-and-trusts

ANNEXES

Available upon request from the FATF Secretariat at contact@fatf-gafi.org

ANNEX 1 THIRD MUTUAL EVALUATION OF CANADA – 1ST FOLLOW-UP REPORT

ANNEX I – ANALYSIS OF MEASURES TAKEN TO ADDRESS DEFICIENCIES

ANNEX II – SET OF LAWS AND OTHER MATERIAL RECEIVED FROM CANADA

ANNEX 2 INFORMATION FROM CANADA ON MEASURES TAKEN SINCE THE 2008 MUTUAL EVALUATION REPORT WITH RESPECT TO NON-CORE AND NONKEY RECOMMENDATIONS RATED PC & NC

Appendix N:

FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016)

FATF

APG

Anti-money laundering and counter-terrorist financing measures

Canada

Mutual Evaluation Report

September 2016

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org**

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organisation, whose members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the FATF Recommendations.

For more information about the APG, please visit the website: **www.apgml.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This assessment was conducted under the responsibility of the International Monetary Fund, adopted by the FATF at its June 2016 Plenary meeting.

Citing reference:

FATF (2016), *Anti-money laundering and counter-terrorist financing measures - Canada,* Fourth Round Mutual Evaluation Report, FATF, Paris
www.fatf-gafi.org/publications/mutualevaluations/documents/mer-canada-2016.html

Photocredits coverphoto: © Thinkstockphoto

CONTENTS

Executive Summary

This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in Canada as at the date of the on-site visit (3-20 November 2015). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Canada's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

1. The Canadian authorities have a good understanding of most of Canada's money laundering and terrorist financing (ML/TF) risks. The 2015 Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (the NRA) is of good quality. AML/CFT cooperation and coordination are generally good at the policy and operational levels.

2. All high-risk areas are covered by AML/CFT measures, except legal counsels, legal firms and Quebec notaries. This constitutes a significant loophole in Canada's AML/CFT framework.

3. Financial intelligence and other relevant information are accessed by Canada's financial intelligence unit, FINTRAC, to some extent and by law enforcement agencies (LEAs) to a greater extent but through a much lengthier process. They are used to some extent to investigate predicate crimes and TF activities, and, to a much more limited extent, to pursue ML.

4. FINTRAC receives a wide range of information, which it uses adequately, but some factors, in particular the fact that it is not authorized to request additional information from any reporting entity (RE), limit the scope and depth of the analysis that it is authorized to conduct.

5. Law enforcement results are not commensurate with the ML risk and asset recovery is low.

6. Canada accords priority to pursing TF activities. TF-related targeted financial sanctions (TFS) are adequately implemented by financial institutions (FIs) but not by designated non-financial business and professions (DNFBPs). Charities (i.e. registered NPOs) are monitored on a risk basis.

7. Canada's Iran and Democratic People's Republic of Korea (DPRK) sanction regime is comprehensive, and some success has been achieved in freezing funds of designated individuals, there is no mechanism to monitor compliance with proliferation financing (PF)- related TFS.

8. FIs, including the six domestic systemically important banks, have a good understanding of their risks and obligations, and generally apply adequate mitigating measures. The same is not true for DNFBPs. REs have gradually increased their reporting of suspicious transactions, but reporting by DNFBPs other than casinos is very low.

9. FIs and DNFBPs are generally subject to appropriate risk-sensitive AML/CFT supervision, but supervision of the real estate and dealers in precious metals and stones (DPMS) sectors is not entirely commensurate to the risks in those sectors. A range of supervisory tools are used effectively especially in the financial sector. There is some duplication of effort between FINTRAC and the Office of the Superintendent of Financial Institutions (OSFI) in the supervisory coverage of federally regulated financial institutions (FRFIs) and a need to coordinate resources and expertise more effectively.

10. Legal persons and arrangements are at a high risk of misuse, and that risk is not mitigated.

11. Canada generally provides useful mutual legal assistance and extradition. The authorities solicit other countries' assistance to fight TF and, to a somewhat lesser extent, ML. Informal cooperation is generally effective and frequently used.

Risks and General Situation

12. Canada has a strong framework to fight ML and TF, which relies on a comprehensive set of laws and regulations, as well as a range of competent authorities.

13. It faces an important domestic and foreign ML threat, and lower TF threat. As acknowledged in the public version of the authorities' 2015 assessment of Canada's inherent ML and TF risks (the NRA), the main domestic sources of proceeds of crime (POC) are fraud, corruption and bribery, counterfeiting and piracy, illicit drug trafficking, tobacco smuggling and trafficking, as well as (to a slightly higher level than assess) tax evasion. Canada's open and stable economy and accessible financial system also make it vulnerable to significant foreign ML threats, especially originating from the neighbouring United States of America (US), but also from other jurisdictions. The main channels to launder the POC appear to be the financial institutions (FIs), in particular the six domestic systemically important banks (D-SIBs) due to their size and exposure, as well as money service businesses (MSBs). While not insignificant, the TF threat to Canada appears lower than the ML threat. A number of TF methods have been used in Canada and have involved both financial and material support to terrorism, including the payment of travel expenses of individuals and the procurement of goods.

Overall Level of Effectiveness and Technical Compliance

14. Since its 2007 evaluation, Canada has made significant progress in bringing its AML/CFT legal and institutional framework in line with the standard, but the fact that AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries is a significant concern. In terms of effectiveness, Canada achieves substantial results with respect to five of the Immediate Outcomes (IO), moderate results with respect to five IOs, and low results with respect to one IO.

Assessment of Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33)

15. The authorities have a generally good level of understanding of Canada's main ML/TF risks. The public version of the 2015 NRA is of good quality. It is based on dependable evidence and sound judgment, and supported by a convincing rationale. In many respects, the NRA confirmed the authorities' overall understanding of the sectors, activities, services and products exposed to ML/TF risk. While the NRA's findings did not contain major unexpected revelations, the process was useful in clarifying the magnitude of the threat, in particular the threat affecting the real estate sector and emanating from third-party money launderers. The authorities nevertheless may be underestimating the magnitude of some key risks, such as the risk emanating from tax crimes and foreign corruption.

16. All high-risk areas are covered by the AML/CFT regime, with the notable exception of the legal professions other than British Columbia (BC) notaries, which is a significant loophole in Canada's AML/CFT framework, and online casinos, open loop prepaid cards, and white label ATMs.

17. While supervisory measures are generally in line with the main ML/TF risks, more intensive supervisory measures should be applied in some higher risk areas such as the real estate and DPMS.

18. AML/CFT cooperation and coordination appear effective at the policy level, but in some provinces, greater dialogue between LEAs and the Public Prosecution Service of Canada (PPSC) would prove useful.

19. While FIs generally appear adequately aware of their ML/TF risks, the same does not apply in some DNFBP sectors, in particular the real estate sector.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

20. Financial intelligence and other relevant information is collected and used to some extent only by competent authorities to carry out investigations into the predicate crimes and TF activities, and, to a more limited extent, to pursue ML. FINTRAC receives a range of information from REs and LEAs, which it adequately analyses. Some factors nevertheless hamper its ability to produce more comprehensive intelligence products, in particular, the fact that FINTRAC is not authorized to obtain from any RE additional information related to suspicions of ML/TF. FINTRAC's analysis and disclosures are mainly prepared in response to the requests made by LEAs in Voluntary Information Records (VIRs). LEAs use these disclosures mainly to investigate the predicate offense, rather than to carry out ML investigations. FINTRAC also produces strategic reports that address the LEAs' operational priorities and advise them on new ML/TF trends and typologies. Information resulting from cross-border transportation of cash and other bearer negotiable instruments is not exploited to its full extent. The FIU and the LEAs cooperate effectively and exchange information and financial intelligence on a regular basis and in a secure way.

21. LEAs have adequate powers and cooperation mechanisms to undertake large and complex financial investigations. This has notably resulted in some high-profile successes in neutralizing ML

networks and syndicates. However, current efforts are mainly aimed at the predicate offenses, with inadequate focus on the main ML risks other than those emanating from drug offenses, i.e. standalone ML, third-party ML and laundering of proceeds generated abroad. Some provinces, such as Quebec, appear more effective in this respect. LEAs' prioritization processes are not fully in line with the findings of the NRA, and LEAs generally suffer from insufficient resources and expertise to pursue complex ML cases. In addition, legal persons are not effectively pursued and sanctioned for ML, despite their misuse having been identified in the NRA as a common ML typology. Criminal sanctions applied are not sufficiently dissuasive. The majority of natural persons convicted for ML are sentenced in the lower range of one month to two years of imprisonment, even in cases involving professional money launderers.

22. Overall, asset recovery appears low. Some provinces, such as Quebec, appear more effective in recovering assets linked to crime. Falsely and undeclared cross-border movements of currency and other bearer negotiable instruments are rarely analysed by the FIU or investigated by the RCMP. As a result, the majority of the cash seized by the Canada Border Services Agency (CBSA) is returned to the traveller at the border.

Terrorist Financing and Financing Proliferation (Chapter 4 - IOs 9- 11; R.5-8)

23. The authorities display a good understanding of Canada's TF risk and cooperate effectively in CFT efforts. The intelligence services, LEAs and FINTRAC regularly exchange information, which notably contributes to support prioritization of TF investigations. Canada accords priority to investigations and prosecutions of terrorism and TF. There are a number of TF investigations, which resulted in two TF convictions. Canada also makes regular use of other disruption measures.

24. Implementation of TF-related targeted financial sanctions (TFS) is generally good but uneven. Large FIs implement sanctions without delay, but DNFBPs do not seem to have a good understanding of their obligations and are not required to conduct a full search of their customer databases on a regular basis. In practice, few assets have been frozen in connection with TF-related TFS, which does not seem unreasonable in the Canadian context.

25. Charities (i.e. registered NPOs) are monitored by the Canada Revenue Agency (CRA) on a risk basis, but the number of inspections conducted over the last few years does not reflect those TF risks. The NRA found the risk of misuse of charities as high, but only a small percentage of charities have been inspected. Nevertheless, to limit this risk, the CRA's charities division has developed an enhanced outreach plan which reflects the best practices put forward by the FATF.

26. Canada's framework to implement the relevant UN counter-proliferation financing sanctions is strong and, in some respect, goes beyond the standard, but does not apply to all types of assets listed in the standard. The current lists of designated persons are available on the OSFI websites, and changes to those lists are promptly brought to the attention of the FRFIs (i.e. banks, insurance companies, trust and loan companies, private pension plans, cooperative credit associations, and fraternal benefit societies). There is a good level of policy and operational cooperation between the relevant authorities including those involved in export control, border control, law enforcement and AML/CFT supervision. Some success has been achieved in freezing

funds of designated persons. None of the Canadian authorities has an explicit mandate to monitor FIs' and DNFBPs' implementation of their counter-PF obligations but, in practice, OSFI has examined implementation by FRFIs of TFS for both TF and PF, and has also identified shortcomings and requested improvements.

Preventive Measures (Chapter 5 - IO4; R.9-23)

27. AML/CFT requirements are inoperative towards legal counsels, legal firms and Quebec notaries. These requirements were found to breach the constitutional right to attorney-client privilege by the Supreme Court of Canada on 13 February 2015. In light of these professionals' key gatekeeper role, in particular in high-risk sectors and activities such as real-estate transactions and the formation of corporations and trusts, this constitutes a serious impediment to Canada's efforts to fight ML.

28. FRFIs, including the six domestic banks that dominate the financial sector, have a good understanding of their risks and AML/CFT obligations. Supervisory findings on the implementation of the risk-based approach (RBA) are also generally positive. The large FRFIs conducted comprehensive group-wide risk assessments and took corresponding mitigating measures. In an effort to mitigate some of the higher risks, a number of FRFIs have gone beyond the Canadian requirements (e.g. by collecting information on the quality of AML/CFT supervision in the respondent bank's country).

29. Nevertheless, some deficiencies in the AML/CFT obligations undermine the effective detection of very high-risk threats identified in the NRA, such as corruption. This is notably the case of the current requirements related to politically exposed persons (PEPs). The identification of beneficial ownership also raises important concerns. Although the legal requirements have recently been strengthened, little is done by FIs to verify the accuracy of beneficial ownership information. DNFBPs are not required to identify the beneficial ownership nor to take specific measures with respect to foreign PEPs.

30. Most DNFBPs are not sufficiently aware of their AML/CFT obligations. This is in particular the case of real estate agents. Extensive work has been conducted by FINTRAC with relevant DPMS trade associations, to increase the DNFBPs' awareness, which is leading to some improvement in compliance. REs have gradually increased the number of STRs and other threshold-based reports filed with FINTRAC but reporting remains very low. The fact that no STRs have been filed by accountants and BC notaries, and the low number of STRs received from the real estate sector raise concern.

Supervision (Chapter 6 - IO3; R.26-28, R. 34-.35)

31. FINTRAC and OSFI supervise FIs and DNFBPs on a risk-sensitive basis. FINTRAC should, however, apply more intensive supervisory measures to DNFBPs. There is good supervisory coverage of FRFIs, but FINTRAC and OSFI need to improve their coordination to share expertise, maximize the use of the supervisory resources available and avoid duplication of efforts. FINTRAC has increased its supervisory capacity in recent years. It adopted an effective RBA in its compliance

and enforcement program, but needs to further develop its sector-specific expertise and increase the intensity of supervision of DNFBPs, particularly in the real estate sector and with respect to DPMS, commensurate with the risks identified in the NRA.

32. There are good market entry controls in place to prevent criminals and their associates from owning or controlling FIs and most DNFBPs. There are, however, no controls for DPMS, and fitness and probity controls at the provincial level are not conducted on an ongoing basis (i.e. including after-market entry).

33. Supervisors appear generally effective. Remedial actions are effectively used and have been extensively applied by supervisors but the sanctioning regime for breaches of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the PCMLTFA) has not been applied in a proportionate and/or sufficiently dissuasive manner. Supervisors have demonstrated that their actions have largely had a positive effect on compliance by FIs and some categories of DNFBPs. They have increased guidance and feedback to REs in recent years but further efforts are necessary, particularly with regard to the DNFBP sector. The exclusion of most of the legal professions (legal counsels, legal firms and Quebec notaries) from AML/CFT supervision has a negative impact on the effectiveness of the supervisory regime as a whole.

Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)

34. Canadian legal entities and legal arrangements are at a high risk of misuse for ML/TF purposes and that risk is not mitigated. This is notably the case with respect to nominee shareholding arrangements, which are commonly used across Canada and pose real obstacles for LEAs.

35. Basic information on legal persons is publicly available, but beneficial ownership information is more difficult to obtain. Some information is collected by FIs and to a limited extent DNFBPs, the tax authorities and legal entities themselves, but is neither verified nor comprehensive in all cases. LEAs have the necessary powers to obtain that information, but the process is lengthy. Information exchange between LEAs and the CRA is also limited by stringent legal requirements.

36. The authorities have insufficient access to information related to trusts. Some information is collected by the CRA as well as by FIs providing financial services, but that information is not verified, does not always pertain to the beneficial owner, and is even more difficult to obtain than in the case of legal entities.

37. LEAs have successfully identified the beneficial owners in limited instances only. Despite corporate vehicles and trusts posing a major ML and TF risk in Canada, LEAs do not investigate many cases in which legal entities or trusts played a prominent role or that involved complex corporate elements or foreign ownership or control aspects.

International Cooperation (Chapter 8 - IO2; R. 36-40)

38. range of mutual legal assistance (MLA) provided by Canada is generally broad, and countries provided—through the FATF—largely positive feedback regarding the responsiveness and

quality of the assistance provided. Canada solicits other countries' assistance in relatively few instances in pursuit of domestic ML, associated predicate offenses and TF cases with transnational elements. Some concerns were nevertheless raised by some Canadian LEAs about delays in the processing of incoming and outgoing requests. The extradition framework is adequately implemented. Informal cooperation is effective. Cooperation between LEAs, FINTRAC, the CBSA and OSFI and their respective foreign counterparts is more fluid, and more frequently used than MLA. Nevertheless, some weaknesses in Canada's framework (e.g. the impossibility for FINTRAC to obtain additional information from REs, and the low quantity of STRs from DNFBPs) negatively affects the authorities' ability to assist their foreign counterparts.

Priority Actions

- Ensure that legal counsels, legal firms, and Quebec notaries engaged in the activities listed in the standard are subject to AML/CFT obligations and supervision. Bring all remaining FIs and DNFBPs in the AML/CFT regime.
- Increase timeliness of access by competent authorities to accurate and up-to-date beneficial ownership information - Consider additional measures to supplement the current framework.
- Increase timely access to financial intelligence – authorize FINTRAC to request and obtain from any RE further information related to suspicions of ML, predicate offenses and TF.
- Use financial intelligence to a greater extent to investigate ML and traces assets.
- Increase efforts to detect, pursue and bring before the courts cases of ML related to all high-risk predicate offenses, third party ML, self-laundering, laundering of POC of foreign predicate and the misuse of legal persons and trusts in ML activities.
- Ensure that asset recovery is pursued as a policy objective throughout the territory.
- Ensure compliance by all FIs with the requirement to confirm the accuracy of beneficial ownership in relation to all customers.
- Require DNFBPs to identify and verify the identity of beneficial owners and PEPs.
- Coordinate more effectively supervision of FRFIs by OSFI and FINTRAC to maximize the use of resource and expertise, and review implementation of the current approach.
- Ensure that FINTRAC develops sector-specific expertise, and applies more intensive supervisory measures to the real estate and the DPMS sectors.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings

IO.1 - Risk, policy and coordination	**IO.2 -** International cooperation	**IO.3 -** Supervision	**IO.4 -** Preventive measures	**IO.5 -** Legal persons and arrangements	**IO.6** - Financial intelligence
Substantial	**Substantial**	**Substantial**	**Moderate**	**Low**	**Moderate**

IO.7 - ML investigation & prosecution	**IO.8 -** Confiscation	**IO.9 -** TF investigation & prosecution	**IO.10 -** TF preventive measures & financial sanctions	**IO.11 -** PF financial sanctions
Moderate	**Moderate**	**Substantial**	**Substantial**	**Moderate**

Technical Compliance Ratings

R.1 - assessing risk & applying risk-based approach	**R.2** - national cooperation and coordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
LC	**C**	**C**	**LC**	**LC**	**LC**
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
LC	**C**	**C**	**LC**	**LC**	**NC**
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
LC	**C**	**NC**	**PC**	**PC**	**LC**
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
C	**PC**	**LC**	**NC**	**NC**	**PC**
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
NC	**LC**	**C**	**PC**	**PC**	**C**
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
LC	**LC**	**C**	**LC**	**LC**	**C**
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international cooperation		
LC	**LC**	**C**	**LC**		

C = Compliant
LC = Largely compliant
PC = Partially compliant
NC = Non-compliant

MUTUAL EVALUATION REPORT

Preface

This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in Canada as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Canada's AML/CFT system, and provides recommendations on how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology as updated at the time of the on-site. The evaluation was based on information provided by Canada, and information obtained by the evaluation team during its on-site visit to Canada from 3-20 November 2015.

The evaluation was conducted by an assessment team consisting of:

- Nadim Kyriakos-Saad (team leader),
- Nadine Schwarz (deputy team leader),
- Antonio Hyman-Bouchereau (legal expert, IMF),
- Katia Bucaioni (financial sector expert, *Unità di Informazione Finanziaria*, Italy),
- Anthony Cahalan (financial sector expert, Central Bank of Ireland),
- Carla De Carli (legal expert, Regional Circuit Prosecution, Brazil),
- Gabriele Dunker (IMF consultant),
- John Ellis (IMF consultant),
- Sylvie Jaubert (law enforcement expert, Directorate of Intelligence and Customs Investigations, France),
- Amy Lam (law enforcement expert, Hong Kong Police).
- The report was reviewed by Emery Kobor (US), Erin Lubowicz (New Zealand), Peter Smit (South Africa), Richard Berkhout (FATF Secretariat) and Lindsay Chan (Asia Pacific Group on Money Laundering—APG secretariat).

Canada previously underwent a FATF mutual evaluation in 2007, conducted according to the 2004 FATF Methodology. That evaluation concluded that Canada was compliant with 7 Recommendations; largely compliant with 23; partially compliant with 8; and non-compliant with 11. Canada was rated compliant or largely compliant with 13 of the 16 Core and Key Recommendations. Canada was placed in the regular follow-up process, and reported back to the FATF in February 2009, February 2011, October 2011, October 2012, and February 2013. The FATF February 2014 follow-up report found that overall, while some minor deficiencies remained, Canada had made sufficient progress with respect to the Core and Key Recommendations. Canada was therefore removed from the follow-up process in February 2014.

The 2008 mutual evaluation report (MER) and February 2014 follow-up report have been published and are available at www.fatf-gafi.org/countries/#Canada.

CHAPTER 1. ML/TF RISKS AND CONTEXT

39. Canada extends from the Atlantic to the Pacific and northward into the Arctic Ocean, covering 9.98 million square kilometres (3.85 million square miles) in total, making it the world's second-largest country by total area (i.e. the sum of land and water areas) and the fourth-largest country by land area. Canada is a developed country and the world's eleventh-largest economy as of 2015 (approximately USD1.573 trillion). As of 2015, the population of Canada is estimated to be 35 851 774. The foreign-born population of Canada represented 20.6% of the total population in 2011, the highest proportion among the G7 countries.[1]

40. Canada is a federation of ten provinces and three territories[2] in the northern part of North America. Ottawa, in the province of Ontario, is the national capital. Canada is a federal parliamentary democracy and a constitutional monarchy, with her Majesty Queen Elizabeth II being the Head of State. The Governor General of Canada carries out most of the federal royal duties in Canada as representative of the Canadian crown.

41. Canada's Constitution consists of unwritten and written acts, customs, judicial decisions, and traditions dating from 1763. The composition of the Constitution of Canada is defined in subsection 52(2) of the Constitution Act, 1982 as consisting of the Canada Act 1982 (including the Constitution Act, 1982), all acts and orders referred to in the schedule (including the Constitution Act, 1867 and the Charter of Rights and Freedoms), and any amendments to these documents.

42. All provinces and territories within Canada follow the common law legal tradition, except Quebec, which follows the civil law tradition. In addition, all federal laws also follow the common law legal tradition and are applicable in every province and territory (Quebec's civil tradition only applies to provincial laws).

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

43. Canada faces important ML risks generated both domestically and abroad. Estimates of the total amount of POC generated and/or laundered in Canada vary: the Criminal Intelligence Service Canada (CISC) estimated in 2007 that POC generated annually by predicate crimes committed in Canada represent approximately 3-5% of Canada's nominal gross domestic product (GDP), or approximately USD47 billion. The RCMP estimated in 2011 that the amount of money laundered annually in Canada to be somewhere between USD 5 billion and USD 15 billion. The NRA indicates that profit-generating criminal activity generates billions of dollars in POC that might be laundered.

[1] Statistics Canada (2011), Immigration and Ethnocultural Diversity in Canada – National Household Survey, 2011, www12.statcan.gc.ca/nhs-enm/2011/as-sa/99-010-x/99-010-x2011001-eng.cfm.

[2] The 10 provinces are Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Quebec, and Saskatchewan. The three territories are Northwest Territories, Nunavut, and Yukon.

1

44. Organized Criminal Groups (OCGs) pose the greatest domestic ML risk, as they are involved in multiple criminal activities generating large amounts of POC. There are over 650 OCGs operating in Canada. The public version of the NRA does not include a detailed analysis of the risks associated with the methods and financial channels used to raise, collect or transfer funds for TF, due to reasons of national security. The classified version of the NRA includes specific ratings for the TF risks represented by each of the terrorist groups. However, this could not be shared and therefore not assessed by the assessors due to national security concerns.

45. Canada appears to be moderately exposed to PF risks, due primarily to the size of the Canadian financial sector. Canada produces a range of controlled military and dual-use goods, and while no estimates were provided regarding the value and volume of goods exported, they are understood to be relatively large. In addition, Canada appears vulnerable to being used as a transshipment or transit point for military controlled and dual-use goods produced in the US. There are no estimates of the financial flows between Canada and either Iran or the DPRK, but, due to the number of restrictions in place (see R.7 and IO.11), are understood to be low.

ML/TF Threats

46. POCs in Canada are mainly generated from: human smuggling, payment card fraud, tobacco smuggling and trafficking, mass marketing fraud, mortgage fraud, capital markets fraud, illicit drug trafficking, counterfeiting and piracy, corruption and bribery, and commercial trade fraud. Canada is exposed to very high ML threats of both local and foreign origin: (i) Fraud, including capital markets fraud, trade fraud, mass marketing fraud, and mortgage fraud, is a major source of POC in Canada.(ii) The proceeds of drug trafficking laundered in Canada are also significant, and derive predominantly from domestic activity controlled by OCGs. (iii) Third-party ML has started to pose a significant threat in recent years. The NRA found, and discussions on-site confirmed that large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve professional money launderers[3] (i.e. individuals specialized in the ML of POC who offer their services for a fee), nominees or money mules. It also found that, of the three, professional money launderers pose the greatest threat both in terms of laundering domestically generated POC as well as laundering, through Canada, of POC generated abroad.[4]

47. The threat emanating from other countries is significant but less easily definable. While some countries have been identified as being the main source of POC laundered in Canada, the authorities' assessment of the foreign ML threat is less detailed and comprehensive than their analysis of the domestic threat.

48. The TF threat was assessed in relation to the terrorist organizations and associated individuals that have financing or support networks in Canada. In particular, the TF threat posed by the actors associated with the following ten terrorist groups and foreign fighters was

[3] It is suspected that criminally-inclined real estate professionals, notably real estate lawyers, are used to facilitate ML. OCGs involved in mortgage fraud appear to launder funds through banks, MSBs, legitimate businesses and trust accounts.
[4] Public version of the NRA, Department of Finance Canada (2015), Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, p.22, www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp

assessed: Al Qaeda in the Arabian Peninsula; Al Qaeda Core; Al Qaeda in the Islamic Maghreb; Al Shabaab; Hamas; Foreign Fighters/Extremist Travellers; Hizballah; Islamic State of Iraq and Syria; Jabhat Al-Nusra; Khalistani Extremist Groups; and Remnants of the Liberation Tigers of Tamil Eelam. Using rating criteria and currently available intelligence, the terrorist groups were assessed as posing a low, medium or high TF threat in Canada. The sectors and products exposed to very high TF risks are corporations, domestic banks, national full-service MSBs, small family-owned MSBs and express trusts. The NRA indicates the possible existence of TF networks in Canada suspected of raising, collecting and transmitting funds abroad to various terrorist groups.[5] The only domestically listed terrorist organizations that pose a TF threat to Canada are those that have financing or support networks in Canada.[6] Terrorism and TF have been increasing in the last two years and more resources were therefore shifted by the authorities to address these threats. As resources remain limited, these issues are putting additional pressures on the AML/CFT regime, and in particular LEAs. Additional funding for AML/CFT activities was authorized in Budget 2015, but these new resources have yet to be fully deployed.

Vulnerabilities

49. Canadian banks offer a number of inherently vulnerable products and services to a very large client base, which includes a significant amount of high-risk clients and businesses. In addition, banks are exposed to high-risk jurisdictions that have weak AML/CFT regimes and significant ML/TF threats. The main channels to launder the POC appear to be the FIs, in particular the D-SIBs due to their size and exposure, as well as MSBs. Terrorist financiers mostly use international and domestic wire transfers to move funds within Canada and/or abroad.

50. The legal profession in Canada is especially vulnerable to misuse for ML/TF risks, notably due to its involvement in activities exposed to a high ML/TF risk (e.g. real estate transactions, creating legal persons and arrangements, or operation of trust accounts on behalf of clients).[7] Following a 13 February 2015 Supreme Court of Canada ruling legal counsels, legal firms and Quebec notaries are not required to implement AML/CFT measures,[8] which, in light of the risks, raises serious concerns.

51. Businesses that handle high volumes of cash are highly vulnerable to ML/TF as they are attractive to launderers of drug proceeds. These include brick and mortar casinos, convenience

[5] The TF methods that have been used in Canada include both financial and material support for terrorism, such as the payment of travel expenses and the procurement of goods. The transfer of suspected terrorist funds to foreign locations has been conducted through a number of methods including the use of MSBs, banks and NPOs as well as smuggling bulk cash across borders.

[6] Organizations posing a terrorist threat to Canada do not necessarily pose a TF threat to Canada. In such cases, the level of threat may not be the same.

[7] The use of trust accounts by lawyers has been recognized by the Department of Finance as a high vulnerability. See: Standing Senate Committee on Banking, Trade and Commerce (2013), Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not really, p. A-26- Lawyers and legal firms, www.parl.gc.ca/Content/SEN/Committee/411/BANC/rep/rep10mar13-e.pdf.

[8] See Judgements of the Supreme Court of Canada (2015), Canada (Attorney General) v. Federation of law societies of Canada, 2015 SCC 7, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14639/index.do.

1

stores, gas stations, bars, restaurants, food-related wholesalers and retailers, and DPMS (notably in the diamonds sector).[9]

52. The real estate sector is highly vulnerable to ML, including international ML activities, and the risk is not fully mitigated, notably because legal counsels, legal firms and Quebec notaries (who provide services in related financial transactions) are not required to implement AML. The sector provides products and services that are vulnerable to ML and TF, including the development of land, the construction of new buildings and their subsequent sale. Also, the real estate business is exposed to high risk clients, including PEPs, notably from Asia[10] and foreign investors (including from locations of concern).

53. Other activities, such as the mining of diamonds, dealing in high value goods, virtual currencies and open loop prepaid cards, are subject to higher ML/TF vulnerability.[11][12] The NRA classifies the virtual currency sector as having high vulnerability, in particular convertible virtual currencies due to the increased anonymity that they can provide as well as their ease of access and high degree of transferability. White-label automated teller machine (ATM) operators are vulnerable to ML/TF. According to the RCMP, OCGs use white-label ATMs to launder POC in Canada. The money withdrawn has previously been deposed into a bank accounts controlled by OCGs through third parties.

54. Legal persons and legal arrangements are inherently vulnerable to misuse for ML/TF purposes to a high degree. There is no legal requirement for legal persons and entities to record and maintain beneficial ownership information. Accordingly, companies and trusts can be structured to conceal the beneficial owner and can be used to disguise and convert illicit proceeds. Privately-held corporate entities can also be established relatively anonymously in Canada. Express trusts have global reach; Canadians and non-residents can establish Canadian trusts in Canada or abroad.

55. Full-service MSBs are vulnerable to ML/TF as they are widely accessible and exposed to clients in vulnerable businesses or occupations, and clients conducting activities in locations of concern. Drug traffickers are particularly frequent users of MSBs.[13]

[9] Ibid. p. 63.
[10] For example, there are cases of Chinese officials laundering the PoC through the real estate sector, particularly in Vancouver, and the Chinese government has listed Canada as a country that it wishes to target for recovering the proceeds of Chinese corruption. Canada may be particularly vulnerable to such laundering, as there is no extradition treaty with China.
[11] See FATF (2013), ML and TF through Trade in Diamonds, pp. 30 and 41, www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf.
[12] See "Developing a ML/TF Risk Assessment Framework for Canada," updated by the Public-Private Sector Advisory Committee (PPSAC) in May 2014. In this regard, AML/CFT requirements have not been extended to the other sectors (i.e. luxury goods, automobile, antiquities) when they engage in any cash transaction with a customer equal to or above a designated threshold.
[13] APG (2013), Yearly Typologies Report, www.apgml.org/includes/handlers/get-document.ashx?d=e92a27b8-42d8-4f8e-bea0-6289dcb30b9b .

International Dimension of ML/TF Vulnerabilities

56. Some of Canada's key attributes (e.g. political and economic stability, well-developed international trade networks, cultural environment, and highly developed financial system and regulatory environment)[14] also make it attractive to those seeking to launder money or finance terrorism. Canada's appeal as an investment setting also makes it an attractive destination for foreign POC.

57. Canada and the US share the longest international border in the world, at over 8 800 kilometers. Some passages are unguarded and provide opportunity for criminals to move easily between both countries. OCGs in Canada and the US actively exploit the border for criminal gain. Both countries endeavour to tackle this vulnerability through close cooperation and careful monitoring of threats.

58. Outflows of POC generated within Canada appear to be moderate in comparison with the inflows of POC. Illicit proceeds from cocaine sales in Canada are often smuggled into the US. Canadian individuals and corporations use tax havens and offshore financial centres to evade taxes, in particular those located in the Caribbean, Europe and Asia.

59. Canada's multiethnic and multicultural character also leaves the country vulnerable to exploitation by OCGs seeking to launder POC or terrorist organizations looking to conceal themselves within law-abiding diaspora communities to finance and promote terrorist activities. Some terrorist groups have also been known to use extortion to gain power over individuals to further their objectives, including by extorting funds from diaspora communities in Canada.[15] Moreover, informal diaspora remittances are open to criminal interference because they circumvent exchange controls and can therefore facilitate ML.

Country's risk assessment & Scoping of Higher Risk Issues

60. The Canadian authorities recently undertook a comprehensive ML/TF NRA. They prepared a classified, restricted NRA report that was shared within the government, as well as a shorter, public version that was published in July 2015.

61. The NRA weighs ML/TF threats against the inherent vulnerabilities of sectors (i.e. to assess the likelihood of ML/TF) and then maps those inherent potential risk scenarios using ratings (i.e. very high, high, medium, low) of individual threat and vulnerability profiles. The threats analysed included some related to sectors that are not currently subject to the PCMLTFA (e.g. check cashing businesses, closed-loop pre-paid access, financing and leasing companies). Ratings serve to illustrate the relative importance of various factors/elements/components relevant to ML/TF.

[14] In response to such threats, Canada created the Illicit Financing Advisory Committee (IFAC) in September 2010. IFAC is responsible for advising the Department of Finance and its Minister about high-risk jurisdictions, and provides a formal mechanism to share information among Canadian government departments and AML/CFT agencies in order to identify and assess the ML/TF threats posed by foreign jurisdictions and entities to Canada.

[15] Department of Finance Canada (2015), Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (NRA), p. 26, www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp.

1

Metrics were based on judgments and were heavily reliant on subject-matter experts' input and readily available information. Based on this approach, all assessed sectors and products were found to be potentially exposed to inherent ML risks while a more limited number of them were found to be exposed to inherent TF risks.

62. While the NRA findings did not contain major unexpected revelations regarding inherent ML or TF threats, the authorities reported that the exercise revealed the magnitude of the threat affecting the real estate sectors and arising from third-party money launderers.

a) Scoping of Higher Risk Issues

63. The assessment team gave increased attention to the following issues which it considered posed the highest ML/TF risk in Canada or warranted more thorough discussions:

- Third-party money launderers (e.g. professional money launderers): The NRA found that large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve professional money launderers;
- Exposure of the Canadian economy to international ML/TF activities (i.e. deposit taking sector, real estate sector, and illicit outflows from Canada to so-called tax haven jurisdictions): A number of sectors are highly vulnerable to ML/TF linked to foreign countries, notably due to the openness of the Canadian economy, the volume of international migrants and visitors, a large and accessible financial system, and a well-developed international trading system;
- Inflows and outflows of POC (including with respect to fraud, corruption, OCG and tax evasion): A better understanding of the nature and magnitude of the inflows and outflows of POC was sought to analyse how Canadian regulators and banks are mitigating the risks of the banking system and to evaluate the effectiveness of international cooperation efforts;
- Sanctioning of ML activities (i.e. all ML offenses) and confiscation of POC: The team gathered information on the number and nature of investigations, prosecutions, sanctions imposed and confiscations related to ML and the main predicate offenses in order to analyse trends since the 2008 mutual evaluation report (MER).; and
- Transparency of legal persons and trusts: The high level of vulnerability of Canadian legal persons and arrangements is reflected by the high level of threat of third-party ML, the inoperativeness of AML/CFT requirements to legal counsels, legal firms and Quebec notaries, and the frequent use of front companies by OCGs.

Materiality

64. Canada has a large and diversified economy, with assets totalling about 500% of GDP.[16] In 2014, 70% of the economy was devoted to services, while manufacturing and primary sectors accounted for the remaining 30%.[17] International trade represents more than 60% of Canada's GDP. Most of Canada's trade is with the US (74% of export and 64% of import) followed by China and Mexico.[18]

65. Canada's financial system plays a key role in the Canadian economy and the global financial system. Canadian FIs provide substantial services to non-residents. The financial system is dominated by banks that total 42% of the financial sector assets, and by a handful of players in most sectors. The D-SIBs hold 93% of bank assets. The IMF's 2014 Financial Sector Assessment Program (FSAP) found that Canada's regulatory and supervisory framework demonstrates strong compliance with prudential international standards. Responsibility for supervision of FIs and markets is divided among federal and provincial authorities. The majority of the prudential supervision of the financial sector is regulated at the federal level by OSFI, though a significant segment is subject to provincial regulation.[19] In regard to prudential and business conduct, financial supervision is generally well coordinated across the federal oversight bodies.

Financial Sector and DNFBPs

66. There are approximately 30 000 REs subject to the PCMLTFA.

Table 1. **Entities by Sector (as of November 2015)**

Sector	Number of Entities	Subject to PCMLTFA (Y/N)
Domestic Systemically Important Banks (D-SIBs)	6	Y
Domestic Banks (other than D-SIBs)	22	Y
Foreign Bank Subsidiaries	24	Y
Foreign Bank Branches	29	Y
White-Label ATM Operators (Non-bank or financial institution)	43 100 (est.)	N
Mortgage Lenders	Not available	N
Leasing Companies	Over 200 (est.)	N
Life Insurance Companies	73 federal and 18 provincially-regulated	Y
Independent Life Insurance Agents And Brokers[1]	154 000 agents and 45 000 brokers (est.)	N

[16] Canada is one of the 29 jurisdictions whose financial sectors are considered by the IMF to be systematically important: *Press Release NO 14/08* of 13 January 2014.

[17] See Canada's National Risk Assessment, p.27.

[18] CIA World Factbook, 2015.

[19] For more information on the financial sector, see IMF 2014 Financial Sector Stability Assessment of Canada (www.imf.org/external/pubs/ft/scr/2014/cr1429.pdf). Canada's NRA states that the banking sector is highly concentrated and holds over 60% of the financial system's assets.

Sector	Number of Entities	Subject to PCMLTFA (Y/N)
Trust and Loan Companies	63 federally-regulated trust companies and loan companies and 14 provincially-regulated	Y
Securities Dealers	3 487 (The D-SIBs own six of the securities dealers, accounting for 75% of the sector's transaction volume)	Y
Credit Unions and *Caisses Populaires* (CU/CPs)	696 CU/CPs9 that are provincially-regulated; 6 Cooperative Credit Associations and 1 Cooperative Retail Association that are federally-regulated	Y
Money Services Businesses (MSBs)	850 registered MSBs	Y
Check cashing businesses	Not available	N
Provincially-Regulated Casinos	39	Y
Ship-based casinos	0	N
Real Estate Agents & Developers	20 784	Y
Dealers in Precious Metals and Stones	642	Y
British Columbia Notaries	336	Y
Accountants	3 829	Y
Legal Professionals	104 938 lawyers, 36 685 paralegals and 3 576 civil law notaries	N (to legal counsels, legal firms and Quebec notaries)
Trust & Company Services Providers	8	N
Registered Charities	86 000 federally registered charities	N

1. While independent insurance agents and brokers are not directly covered under the PCMLTFA, life insurance companies may use agents or brokers to ascertain the identity of clients on the basis of a written agreement or arrangement, which must conform to the requirements of PCMLTFR, s.64.1.

67. The broader deposit taking sector includes trust and loan companies. Canada's largest trust and loan companies are subsidiaries of major banks. Some trusts have provincial charters and are regulated at that level of government. Credit unions and *caisses populaires* are provincially incorporated and may not operate outside provincial borders. Relative to banks, these entities are minor participants in the deposit-taking sector. However, *caisses populaires* represent a large portion of the deposit-taking sector in the province of Quebec.

68. The insurance industry is an important player in the financial services sector, providing almost one-fifth of all financing to Canadian companies. Canadian-owned insurers take in more than 70% of total Canadian premium income. Canadian companies are also active abroad, especially in south-east Asia, generating more than half of their premium income from foreign operations.

Structural Elements

69. The key structural elements for effective AML/CFT controls are present in Canada. Canada is generally considered to be a very stable democracy. Political and institutional stability,

accountability, the rule of law and an independent judiciary are all well established. There also appears to be a high-level political commitment to improve the effectiveness of Canada's AML/CFT regime, as evidenced by the Economic Action Plans 2014 and 2015.[20-21] However, LEAs' resources are generally insufficient to pursue complex ML cases.

70. Canada has an independent, efficient, and transparent Justice System. The judicial process is widely trusted and effective, as well as relatively quick.

71. Canada has a comprehensive legal framework that governs the protection of personal information of individuals in both the public and private sectors. The primary source of constitutionally enforced privacy rights is Section 8 of the Canadian Charter of Rights and Freedoms. The Office of the Privacy Commissioner (OPC) oversees compliance with both federal privacy laws (see Box 1 below). Every province has its own privacy law and the relevant provincial act applies to provincial government agencies instead of the federal legislation. The Canadian regime is implemented while seeking an appropriate balanced between privacy and security considerations. In that regard, in 2012 the OPC issued guidance for REs regarding reporting suspicions to FINTRAC, in light of their customers' privacy rights.[22]

[20] Budget 2014 announced the Government's intention to take action to address the need to enhance the AML/CFT framework. As a result, the Government introduced in 2015 legislative amendments and regulations aiming to strengthen Canada's AML/CFT regime and improve Canada's compliance with international standards. This reform was based on the five-year review of the PCMLTFA undertaken by the Standing Senate Committee on Banking, Trade and Commerce in 2013. Economic Action Plan 2015 (Budget 2015) provides updates on these measures. The Government proposed to provide FINTRAC up to CAD 10.5 million over five years and up to CAD 2.2 million per year subsequently. The Government also proposed to provide up to CAD 12 million on a cash basis over five years to improve FINTRAC's analytics system. This allocation intends to better meet the needs of Canadian law enforcement and other regime partners. See Budget 2014, www.budget.gc.ca/2014/docs/plan/pdf/budget2014-eng.pdf

[21] Includes additional allocation of CAD 292.6 million over five years in intelligence and law enforcement agencies for additional investigative resources to counter terrorism. See www.budget.gc.ca/2015/docs/plan/budget2015-eng.pdf.

[22] Office of the Privacy Commissioner of Canada (2012), Privacy and PCMLTFA: How to balance your customers' privacy rights and your organization's anti-money laundering and anti-terrorist financing reporting requirements, www.priv.gc.ca/information/pub/faqs_pcmltfa_02_e.asp.

1

Box 1. **Legal Framework for Information and Data Protection in Canada**

The primary source of privacy rights is Section 8 of the Canadian Charter of Rights and Freedoms, which provides protection against unreasonable search and seizure by authorities. This means, generally, that in situations where the person concerned has a reasonable expectation of privacy in relation to an object or document, in order for the state (i.e. government authorities such as LEAs) to have access to these items, prior judicial authorization will need to be obtained. Where such access is sought for the purposes of a criminal investigation, LEAs will generally seek to obtain a search warrant or a production order from a Canadian court. The latter is typically used for access to financial information held by a third party, such as a FI. "Reasonable grounds to believe" that an offense has been committed is the legal standard of proof in Canadian Law for the court to issue the appropriate order. In addition, it is necessary to demonstrate that evidence of the offense is to be found in the place to be searched. In certain cases, such as in relation to certain types of financial information, a lower legal standard of "reasonable grounds to suspect" applies.

At the federal level, Canada has two different privacy acts which are enforced by the Office of the Privacy Commissioner of Canada. The Privacy Act regulates the handling of personal information by federal government departments and agencies. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to the commercial transactions of organizations that operate in Canada's private sector. PIPEDA applies to all private sector entities in Canada, except in provinces that have enacted substantially similar legislation. Every Canadian province and territory has its own privacy law and the relevant provincial act applies to provincial government agencies instead of the federal legislation.

The Privacy Act lists13 uses and disclosures that might be permissible without the consent of the individual (e.g. national security, law enforcement, public interest). Canadian law provides for lawful access to law enforcement and national security agencies to legally intercept private communications and the lawful search and seizure of information, including computer data, without the consent of either the sender or receiver to investigate serious crimes, including ML and threats to national security, such as terrorism. Lawful access is provided for in the CC, the CSIS Act, the Competition Act and other acts.

The Anti-Terrorism Act (ATA) provides law enforcement and national security agencies powers to obtain electronic search warrants. The ATA also allows Canadian intelligence agencies to intercept communications of Canadians in Canada, and allows the Attorney General to prevent the disclosure of information on the grounds of national security.

Under the PCMLTFA, FINTRAC receives detailed personal information through reports from REs, which can then be provided to the CRA (in cases which include tax matters), CSIS, CBSA, Citizenship and Immigration Canada (in cases which include immigration matters) or to LEAs (e.g. when the information is relevant to the investigation and prosecution of ML or TF offenses).

Background and other Contextual Factors

72. Canada ranks among the highest in international measurements of government transparency, civil liberties, quality of life, economic freedom, and education. It enjoys a high rate of financial inclusion, with 96% of the population having an account with a formal FI. Canadian banks and other FIs operate an extensive network of more than 6 000 branches, and around 60 000 ATMs of which about 16 900 are bank-owned (the rest are white-label ATMs).[23]

73. The authorities have identified corruption as a high-risk issue for ML. Recent assessments of Canada's implementation of international anti-corruption conventions indicate a rather moderate range of positive outcomes in identifying and sanctioning cases of corruption and implementing structures and systems to prevent corruption.[24] Nevertheless, corruption does not appear to hinder the implementation of the AML/CFT regime. Canada is ranked as 9 out of 168 countries in Transparency International's 2015 Corruption Perception Index (with a score of 83/100).[25]

Overview of AML/CFT strategy

74. As formulated in Budget 2014, the Government's priority in regards to AML/CFT is to improve the ability to trace and detect criminal funds in Canada. Besides law enforcement goals, this priority also aims to protect the tax base by supporting the Government's efforts to ensure tax compliance. Addressing this priority requires improving corporate transparency.

75. Canada does not have formal 'stand-alone' AML, CFT or PF strategies. There is, however, a set of relevant policies and strategies: the National Identity Crime Strategy (RCMP 2011); National Border Risk Assessment 2013–2015 (CBSA); 2014–16 Border Risk Management Plan (CBSA); Enhanced Risk Assessment Model and Sector profiles (FINTRAC); AMLC Division AML and CFT Methodology and Assessment Processes (OSFI); Risk Ranking Criteria (OSFI); RBA to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals (CRA) and CRA- RAD Audit Selection process. The RCMP recently developed its National Strategy to Combat ML.[26] These AML strategies and policies are linked to the *Canadian Law Enforcement Strategy on Organized Crime* adopted by senior police officials across Canada in 2011.

---

[23] In Canada, "white label" or "no name" ATMs are those run by independent operators and not by major financial institutions. They are usually located in local small establishment retailers such as gas stations, bars/pubs, and restaurants and do not display labels from financial institutions on the machine.
[24] See 2014 review of the implementation by Canada of the Inter-American Convention against Corruption; 2013 Phase 3 report on implementation of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transaction and the 2009 Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions.
[25]Transparency International (2015), 2015 Corruption Perception Index, www.transparency.org/cpi2015.
[26] Royal Canadian Mounted Police (nd), Royal Canadian Mounted Police 2015–16 Report on Plans and Priorities, www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-2015-16-report-plans-and-priorities, this strategy was finalized in 2016.

1

76. The Government's other main AML/CFT concerns are reflected in Finance Canada's Annual Report on Plans and Priorities,[27] which describes the AML/CFT regime's spending plans, priorities and expected results. Canada's CFT strategy policy guidance is derived from its 2012 Counter-terrorism Strategy.[28] This comprehensive Strategy guides more than 20 federal departments and agencies to better align them to address terrorist threats, including in regard to CFT activity and initiatives. The Minister of Public Safety and Emergency Preparedness, in consultation with the Minister of Foreign Affairs, is responsible for the Strategy's implementation. Similarly, the country's PF strategy forms part of the broader strategy to counter the proliferation of chemical, biological, radiological and nuclear weapons.

Overview of the legal & institutional framework

77. Canada's AML/CFT regime is organized as a horizontal federal program comprised of a large number of federal departments and agencies. Finance Canada is the domestic and international policy lead for the regime, and is responsible for its overall coordination, including guiding and informing strategic implementation of the RBA. It chairs the four main governing bodies of Canada's AML/CFT regime, namely:

- The interdepartmental Assistant Deputy Minister (ADM) Level Steering Committee, which was established to direct and coordinate the government's efforts to combat ML and TF activities. The ADM Committee and its working group consists of representatives of all partners;[29]
- The Interdepartmental Coordinating Committee (ICC), which provides a forum for government working-level stakeholders[30] to assess the operational efficiency and effectiveness of the regime;
- The National ML/TF Risk Assessment Committee (NRAC) provides a forum for regime and *ad hoc* partners to exchange information on risks and discuss about ML/TF risks in Canada and their mitigation; and
- The Public Private Sector Advisory Committee (PPSAC) which is a discussion and advisory committee, with membership from (federal public sector) regime partners and private sector REs, as well as provincial law enforcement.[31]

[27] Department of Finance Canada (2014), Report on Plans and Priorities 2014–15, www.fin.gc.ca/pub/rpp/2014-2015/index-eng.asp.
[28] Public Safety (2012), Building Resilience Against Terrorism – Canada's Counter-Terrorism Strategy, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-eng.aspx.
[29] The ADM Committee is composed of the following agencies: Finance Canada; Justice Canada; PPSC; Public Safety Canada; CRA; FINTRAC; RCMP; CBSA; OSFI; and CSIS.
[30] The ICC is composed of the following agencies: Finance Canada; PPSC; Public Safety Canada; CRA; FINTRAC; RCMP; CBSA; CSIS; OSFI; Privy Council Office (PCO); and Global Affairs Canada.
[31] This Committee consist of approximately 30 members, with more than half of the members coming from the private sector. The public sector participants generally consist of members who already participate in the Interdepartmental Steering Committee on this topic. The private sector participants will consist of participants from sectors covered by the PCMLTFA. This includes financial entities, life insurance companies, securities

78. The AML/CFT regime operates on the basis of three interdependent pillars: (i) policy and coordination; (ii) prevention and detection; and (iii) investigation and disruption. On this basis, the following are the primary ministries, agencies, and authorities responsible for formulating and implementing Canada's AML/CFT policies (i.e. the regime partners):

Policy and Coordination:

- **Finance Canada** is the lead agency of the regime, responsible for developing AML/CFT policy related to domestic and international commitments.
- **Department of Justice Canada (DOJ)** is responsible for the drafting and amending of statutory provisions dealing with criminal law and procedure, and to negotiate and administer mutual legal assistance (MLA) and extradition treaties.
- **Global Affairs Canada (GAC)**[32] is responsible for the designation of entities and individuals in Canada associated with terrorist activities listed by the United Nations 1267 Sanctions Committee or under Resolution 1373 of the United Nations Security Council. GAC also chairs the Counter-Proliferation Operations Committee, coordinating responses to threats within Canada.
- **Public Safety Canada (PSC, previously known as Public Safety and Emergency Preparedness)** chairs the Threat Resourcing Working Group and ensures coordination across all federal departments and agencies responsible for national security and the safety of Canadians, including on terrorist financing matters. It is responsible for the listing of terrorist entities under the Criminal Code and co-chairs the Interdepartmental Coordinating Committee on Terrorist Listings.

Prevention and Detection:

- **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** is Canada's financial intelligence unit. It is also responsible for supervising and monitoring all REs' compliance with the PCMLTFA.
- **Office of the Superintendent of Financial Institutions Canada (OSFI)** prudentially supervises FRFIs.
- **Innovation, Science and Economic Development Canada (ISED, former Industry Canada)** collects information about business corporations, including the business name and address, and information about the directors.

---

dealers, money service businesses, accountants, the notarial profession, the real estate sector, casinos, dealers in precious metals and stones, and home builders.

[32] Global Affairs Canada's Anti-Crime and Counter-Terrorism Capacity Building programs (ACCBP and CTCBP) funding has been used to support the Regime's AML and CFT projects in a number of regions.

1

- **Office of the Privacy Commissioner of Canada (OPC)** ensures that the necessary safeguards protecting privacy are upheld. The Privacy Commissioner has the ability to audit the public (e.g. FINTRAC) and private sector to ensure privacy laws are respected. The OPC is required to conduct a privacy audit of FINTRAC every two years.

Investigation and Disruption:

- **Royal Canadian Mounted Police (RCMP)** is Canada's main law enforcement agency (LEA) responsible for investigating predicate offenses, ML and TF.
- **Public Prosecution Service of Canada (PPSC)** is responsible for prosecuting criminal offenses under federal jurisdiction. It also provides legal advice to the RCMP and other LEAs over the course of their investigations, and for undertaking any subsequent prosecutions.
- **Canada Revenue Agency (CRA)**—the CRA's Criminal Investigations Directorate (CID) investigates cases of suspected tax evasion/tax fraud and seeks prosecution through the PPSC where warranted. The CRA also has responsibility for administering the registration system for charities under the Income Tax Act through its Charities Directorate.
- **Canada Border Services Agency (CBSA**) enforces the physical cross-border reporting obligation.
- **Canadian Security Intelligence Service (CSIS)** collects, analyses and reports to the Government of Canada information and intelligence concerning threats to Canada's national security.
- **Public Services and Procurement Canada (PSPC, previously Public Works and Government Services Canada)**, under the Seized Property Management Directorate (SPMD), is responsible for managing assets seized or restrained by law enforcement in connection with criminal offenses and for disposing and sharing the proceeds upon court declared forfeitures.

79. The AML/CFT regime is also supported by a number of other partners including: provincial, territorial and municipal LEAs, provincial and territorial financial sector regulators, and self-regulatory organizations.

80. Canada's AML/CFT framework is established in the PCMLTFA, supported by other key statutes, including the Criminal Code (CC). The Parliament of Canada undertakes a comprehensive review of the PCMLTFA every five years. The Government announced a series of measures to enhance the AML/CFT regime in Budget 2014, which received Royal Assent in June 2014. Accordingly, amended Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR) were released in draft form for consultation by the Government on 4 July 2015.

Proliferation Financing

81. The principal legislation governing Canada's export control system is the Export and Import Control Permits Act (EIPA), which provides for the requirements for exporters to report goods to the Government of Canada and for the enforcement of national control lists. The Customs Act and Canada Border Services Agency Act provide the CBSA with the authority to enforce Canada's export legislation. The country's efforts to combat the proliferation of weapons of mass destruction and, to some extent, its financing, are carried out by the following agencies: PSC (coordination of counter-proliferation policy and main operational partner); Global Affairs Canada (lead on international engagement on non-proliferation and disarmament and chairs the Counter-Proliferation Operations Committee); CBSA (law enforcement regarding the illicit export and proliferation of strategic goods and technology); Canadian Nuclear Safety Commission (licensing of nuclear-related activities); PWGSC (administers the Controlled Goods Program); FINTRAC (discloses financial intelligence that can assist in investigations and prosecutions); RCMP (enforces the counter-proliferation regime, investigates related criminal offenses, collects and analyses evidence to support prosecutions in court); the Public Health Agency of Canada (national authority on biosafety and biosecurity for human pathogens and toxins); and Finance (responsible for safeguarding Canada's financial system from illegitimate use, through the PCMLTFA and associated regulations, and the overall coordination of Canada's AML/CFT regime domestically and internationally).

Overview of preventive measures

82. The legal framework relevant to the preventive measures includes the PCMLTFA, the OSFI Act and the FRFIs' governing legislation (i.e. the Bank Act, Trust and Loan Companies Act, the Cooperative Credit Associations Act and the Insurance Companies Act). The PCMLTFA is applicable to most of the financial activities and DNFBPs.

Overview of legal persons and arrangements

83. Canada's company law consists of federal, provincial and territorial frameworks. Legal entities may be established at the federal level under the Canada Business Corporation Act (CBCA); the Canada Not-for-Profit Corporations Act (NFP Act), or the Canada Cooperatives Act (CCA). A federally incorporated entity is entitled to operate throughout Canada. However, provincial and territorial law requires federal entities to register with the province or territory in which the entity is carrying out business. Incorporation on the federal level is carried out by Innovation, Science and Economic Development Canada (ISED, formerly Industry Canada) is responsible for the incorporation of federal corporate entities, while each province has its own system for incorporating and administering legal entities.

84. There are over 2.6 million corporations incorporated in Canada, including almost 4 000 publicly-traded companies. About 91% of corporations are incorporated at the provincial or territorial levels and the remaining 9% at the federal level. Bearer shares are permitted in most provinces and at the federal level, but seem to be rarely used. There is also a relatively small market for stock warrants. All companies are obliged to file tax returns with the CRA on an annual basis.

1

Provincial legal entities incorporated in Alberta and Quebec must also file tax returns with the provincial tax authorities.

85. Partnerships are created under provincial law only and, other than limited partnerships, are created under the rules of the common law although subject to laws that codify and regulate certain aspects of the partnership. In contrast, limited partnerships are created under statute and subject to ongoing registration requirements.

86. The only form of legal arrangement that exists in Canada is the trust in form of testamentary or *inter vivos* trust. There is no general requirement for trusts to be registered, but Canadian resident trusts and certain foreign-resident trusts are subject to obligations to file information under the income tax laws. Specific-purpose trusts such as unit or mutual fund trusts are also subject to the securities laws of the relevant province. Trusts created under the laws of Quebec are required to register in some instances. According to the NRA, the total number of Canadian trusts is estimated in the millions. As of 2007, only 210 000 trusts filed tax returns with the CRA.

International Context for Legal Persons and Arrangements

87. According to the UNCTAD 2014 World Investment Report, Canada ranks amongst the top ten countries both with respect to inflowing and outflowing foreign direct investment, with much of the activity taking place in the manufacturing and oil and gas sectors. Canada received over USD 53 billion of foreign direct investment in 2014 coming mostly from the EU, the US, and China. On the outflow, Canada invested approximately USD 52 billion abroad in 2014, mostly in the EU and the US. While detailed figures are not available with respect to foreign ownership of Canadian companies, the statistics provided by the UNCTAD leads to the conclusion that foreign ownership of Canadian legal entities is significant. Canada is not perceived as an international centre for the creation or administration of legal persons or arrangements.

Overview of supervisory arrangements

88. Financial regulation is shared by a number of government bodies in Canada. The Bank of Canada has overall responsibility for financial stability, as well as for the conduct of monetary policy and the issuance of currency. As mentioned above, OSFI supervises and regulates FRFIs (banks and insurance companies, trust and loan companies, cooperative credit associations, fraternal benefit societies, and private pension plans). All banks, including branch operations of foreign banks, are regulated solely at the federal level. The securities sector including in respect of mutual funds, is currently regulated on a province by province basis with connections between the provinces through the Canadian Securities Administrators Association. Markets for securities and collective investments are overseen by provincial securities commissions, which co-ordinate their activities through the Canadian Securities Administrators.[33]

[33] Canada is currently developing a Cooperative Capital Markets Regulatory System (CCMRS), a new joint federal and provincial initiative. Under this system, the provinces and the federal government would delegate

89. In March 2013, FINTRAC and OSFI entered into an agreement to conduct concurrent examinations to improve the effectiveness and cohesion of supervision and allocation of resources, and to reduce the regulatory burden on FRFIs. FINTRAC and OSFI thus concurrently assess FRFIs' AML/CFT compliance and risk management regimes using a RBA. FINTRAC and OSFI mutually share information under a Memorandum of Understanding (MOU) was signed in 2004 with respect to FRFIs. At the provincial level, FINTRAC conducts AML/CFT supervision on non-FRFIs with the cooperation of other national and provincial supervisors under various MOUs.

their regulatory functions to the CCMR, which may be useful in regard to the identification of systemic risk and criminal enforcement.

1

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

The Canadian authorities have a good understanding of the country's main ML/TF risks and have an array of mitigating measures at their disposal. Canada's NRA is comprehensive, and also takes into account some activities not currently subject to the AML/CFT measures.

All high-risk areas are covered by AML/CFT measures, except activities listed in the standard performed by legal counsels, legal firms and Quebec notaries, which is a significant loophole in Canada's AML/CFT framework, and online casinos, open loop prepaid cards, and white label ATMs.

FIs and casinos have a good understanding of the risks. Other DNFBPs, and in particular those active in the real estate sector, do not have a similarly good understanding.

Law enforcement action focus is not entirely commensurate with the ML risk emanating from high-risk offenses identified in the NRA.

Cooperation and coordination are good at both the policy and operational levels, except, in some provinces, in the context of the dialogue between LEAs and the PPSC.

Communication of the NRA findings to the private sector was delayed, but is in progress.

Recommended Actions

Canada should:

- Mitigate the risk emanating from legal counsels, legal firms, and Quebec notaries in their performance of the activities listed in the standard.
- Strengthen policies and strategies to address emerging ML risks (in particular white label ATMs and online casinos).
- Review LEAs' priorities in light of the findings of the NRA.
- In the context of the update of the NRA, examine more closely ML linked to tax evasion, corruption, legal persons and arrangements, third-party ML and foreign sources of POC and use results to implement mitigating actions.

The relevant Immediate Outcome considered and assessed in this chapter is IO1. The recommendations relevant for the assessment of effectiveness under this section are R1-2.

Immediate Outcome 1 (Risk, Policy and Coordination)

90. As indicated in Chapter 1 above, Canada completed in 2015 a national assessment of the inherent ML/TF risks that it faces. The process and main findings of the NRA are described above.

Country's understanding of its ML/TF risks

91. The authorities' understanding of ML/TF risks has been forged through the development of several national threat and risks assessments undertaken by different governmental agencies over the past decade on related matters (see Criterion 2.1). The Parliament's Standing Senate Committee on Banking, Trade and Commerce undertakes a comprehensive review of the PCMLTFA every five years. As a result of the most recent review (completed in 2013),[34] the Government introduced legislative amendments in 2014 to address the Committee's recommendations (e.g. including measures to strengthen customer due diligence (CDD) requirements, improve compliance, monitoring and enforcement and enhance information sharing). The authorities demonstrated a sound understanding of the issues highlighted in Chapter 1, including a good understanding of the linkages between the threats and inherent vulnerabilities of the different sectors and the domestic and foreign offenses that are a source of most of the ML/TF[35] in the country. The NRA process has also contributed to a deeper understanding of the powers, resources and operational needs of all regime partners. NRAC ensures that all regime partners generally have a similar level of understanding of the ML/TF risks.

92. Following the publication of the NRA in July 2015, the NRAC concluded a gap analysis in September 2015 to categorize the residual risks (i.e. the risk remaining after the mitigation of the identified threats and inherent vulnerabilities) and identify and prioritize the actions required to mitigate the risk. The review and updating of the NRA is expected to be finalized by the fall of 2016. The authorities indicated that as new, improved controls are put in place, the residual risk will be an indicator of the areas that remain pending to be addressed. As of the date of the on-site visit, it was not possible to establish if the publication of the NRA has led to improvements of the RE's level of compliance with AML/CFT requirements.

National policies to address identified ML/TF risks

93. The adjustment of the national policies and strategies related to the identified ML/TF risks is in its early stages and no updates have been completed. The authorities have been addressing the inherent risks identified in different ways including through ongoing policy coordination through NRAC, the discussion of draft amendments to the PCMLTF Regulations, adjusted supervisory priorities, more focused police investigations, and amendments to the law regarding the seizure of illicit assets, among others.

---

[34] Standing Senate Committee on Banking Trade and Commerce (2013), Follow The Money: Is Canada Making Progress In Combatting Money Laundering And Terrorist Financing? Not Really, www.parl.gc.ca/Content/SEN/Committee/411/banc/rep/rep10mar13-e.pdf.

[35] As elaborated in Chapter 1, the classified version of the NRA, which was not shared with the assessment team, ranks in greater detail the TF risks associated with terrorist groups.

94. On the basis of the NRA, a package of regulatory amendments was issued in July 2015 for public comment. The government is now moving forward with final publication and the Regulations will come into force one year after registration of the regulations. Canada is preparing a second package of regulatory amendments based on the NRA, including measures to cover pre-paid payment products (e.g. prepaid cards), virtual currency as well as money service businesses without a physical presence in Canada in the AML/CFT Regime. The authorities are also revisiting the PCMLTFA provisions relating to legal counsels, legal firms and Quebec notaries, in order to bring forward new provisions for the legal professional that would be constitutionally compliant. Furthermore, also informed by the NRA results, FINTRAC and OSFI are reviewing their RBA to supervision, the RCMP developed its Money Laundering Strategy, and the CBSA is reviewing its Cross-Border Currency Reporting program.

95. As discussed in Chapter 1, Canada's CFT strategy policy guidance is derived from its 2012 Counter-Terrorism Strategy. The PS coordinates Canada's counter-proliferation policy approach across the government, which includes PF.

Exemptions, enhanced and simplified measures

96. Canada's AML/CFT framework does not provide for simplified CDD measures, but the PCMLTFR provide a small number of exceptions to REs based on the risk circumstances and products (see Criterion 10.18). These exemptions correspond to lower-risk scenarios that are consistent with the NRA findings in regard to FIs (i.e. in regard to life insurance companies, brokers, or agents).

Objectives and activities of competent authorities

97. FINTRAC and OSFI objectives and activities are largely consistent with the ML and TF risks in Canada, as detailed in the NRA. With the exception of the legal professions (other than BC notaries), the supervisory coverage is adequate.

98. Law enforcement action is focused on LEAs current priorities, which include drug-related offenses and OCGs, but is not commensurate with the ML risk emanating from these and other types of offenses.

99. In terms of the resources required, the Government's Economic Action Plans for 2014 and 2015 included a commitment to ensuring that law enforcement and security agencies have the investigative resources and tools to address the threats presented by OGCs, ML and terrorism and to further their understanding of Canada's ML/TF risks. Nevertheless, the authorities advised the assessors that all regime partners are under significant pressures at the working level given the increased terrorist threats and combined with the increased threat of professional ML with transnational organized crimes and the number competing priorities.

National coordination and cooperation

100. AML/CFT policy cooperation and coordination to address Canada's ML/TF risks is adequate—with the exception of the dialogue between LEAs and the PPS in some provinces, which is currently insufficient- and constitutes an essential strength of the Canadian AML/CFT framework, as evidenced by the organization and process of the NRA. Canada has wide-ranging arrangements in place for AML/CFT coordination and cooperation at both the policy and operational levels, including with respect to strategic and tactical information sharing (See R.2). Coordination and cooperation at the policy design platform is exceptional.

101. The NRA has allowed the identification and inclusion of new partners for AML/CFT (e.g. Defence Research and Development Canada and Environment Canada), and to reconsider the roles and responsibilities of traditional partners that gained a more prominent role in the fight of ML/TF over the years given enhanced understanding of ML/TF risks (e.g. Industry Canada). Overall, the public version of the NRA is of good quality and is drafted in an accessible language. Moreover, the assessment process has yielded reasonable findings that broadly reflect the country's ML/TF context and risk environment.

Private sector's awareness of risks

102. The public version of the NRA had not been circulated widely at the time of the on-site visit, due to a broader prohibition on the federal public service undertaking consultations with private sector stakeholders during the August to October 2015 federal election campaign. However, the public NRA has been made available on Finance Canada's, OSFI's and FINTRAC's website since July 2015.[36] The report was also shared with the PPSAC. As of the dates of the on-site visit, the authorities had not formally presented the results of the communication strategy for the broader private sector, but were in the process of reaching out to selected FIs. FINTRAC also provides access to guidelines, Interpretation Notices reports on current and emerging trends and typologies in ML and TF on its website to assist FIs and DNFBPs.

Overall Conclusions on Immediate Outcome 1

103. **Canada has achieved a substantial level of effectiveness for IO.1.**

[36] The NRA has since been made available on several websites (e.g. OSFI, Investment Industry Organization of Canada, among others).

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

IO.6

Financial intelligence and other relevant information are accessed by FINTRAC to some extent, and by LEAs to a greater extent but through a much lengthier process.

They are then used by LEAs to some extent to investigate predicate crimes and TF, and, to a more limited extent, to investigate ML and trace assets.

FINTRAC receives a wide range of information, which it uses adequately to produce intelligence. This intelligence is mainly prepared in response to Voluntary Information Records (VIRs; i.e. LEAs' requests) and used to enrich ongoing investigations into the predicate offenses. FINTRAC also makes proactive disclosures to LEAs, some of which have prompted new investigations.

Several factors significantly curtail the scope of the FIU's analysis—and consequently the intelligence disclosed to LEAs—in particular: the impossibility for FINTRAC to request from any RE additional information related to suspicions of ML/TF or predicate offense, the absence of reports from some key gatekeepers (i.e. legal counsels, legal firms, and Quebec notaries), and the inability for FINTRAC to access to information detained by the tax administration. This is compensated by LEAs in their investigations to some extent only due to challenges in the identification of the person or entity who may hold relevant information.

FINTRAC also produces a significant quantity of strategic reports that usefully advise LEAs, intelligence agencies, policy makers, REs, international partners, and the public, on new ML/TF trends and typologies.

FINTRAC and the LEAs cooperate effectively and exchange information and financial intelligence in a secure way.

IO.7

Canada identifies and investigates ML to some extent only. While a number of PPOC cases are pursued, overall, the results obtained so far are not commensurate with Canada's ML risks.

LEAs have the necessary tools to obtain information, including beneficial ownership information, but the process is lengthy.

In some provinces, such as Quebec, federal, provincial, and municipal authorities are relatively more effective in pursuing ML.

Nevertheless, overall, as a result of inadequate alignment of current law enforcement priorities with the findings of the NRA and of resource constraints, LEAs' efforts are aimed mainly at drug offenses and fraud, with insufficient focus on the other main ML risks (corruption, tobacco smuggling, standalone ML, third-party ML, ML of foreign predicate offenses). In addition, investigations generally do not focus on legal entities and trusts (despite the high risk of misuse), especially when

more complex corporate structures are involved.

There is a high percentage of withdrawals and stays of proceedings in prosecution.

Sanctions imposed in ML cases are not sufficiently dissuasive.

3

IO.8

Canada has made some progress since its last evaluation in terms of asset recovery, but the fact that assets of equivalent value cannot be recovered hampers Canada's recovery of POC.

Confiscation results do not adequately reflect Canada's main ML risks, neither by nature nor by scale.

Results are unequal, with some provinces, such as Quebec, being significantly more effective, and achieving good results with adequately coordinated action (both at the provincial level and with the RCMP) and units specialized in asset recovery.

Administrative efforts to recover evaded taxes appear more effective.

Sanctions are not dissuasive in instances of failure to properly declare cross-border movements of currency and bearer negotiable instruments.

Recommended Actions

Canada should:

IO.6

- Increase timely access to financial intelligence. Authorize FINTRAC to request and obtain from any RE further information related to suspicions of ML, predicate offenses and TF in order to enhance its analysis capacity.
- Use financial intelligence to a greater extent to investigate ML and trace assets.
- Analyse and, where necessary, investigate further information resulting from undeclared or falsely declared cross-border transportation of cash and bearer negotiable instruments.
- Ensure that LEAs and FINTRAC can identify accounts and access records held by FIs/DNFBPs in a timely fashion.
- Consider granting FINTRAC access to information collected by the CRA for the purposes of its analysis of STRs.

IO.7

- Increase efforts to detect, pursue, and bring before the courts cases of ML related to high-risk predicate offenses other than drugs and fraud (i.e. corruption and tobacco smuggling), as well as third-party ML, self-laundering, laundering of POC of foreign predicate offenses, and the misuse of legal persons and trusts in ML activities.
- Ensure that LEAs have adequate resources (in terms of number and expertise) for ML

investigations.

- Engage prosecutors at an earlier stage for securing relevant evidence for ML/PPOC prosecutions in order to limit instances where charges are dropped at the judicial process and minimize waste of resources in ML investigations.
- Ensure that effective, proportionate, and dissuasive sanctions for ML are applied.

IO.8

- Ensure that asset recovery is pursued as a policy objective throughout the territory.
- Make a greater use of the available tools to seize and restraint POC other than drug-related instrumentalities and cash (i.e. including other assets, e.g. accounts, businesses, and companies, property or money located abroad), especially proceeds of corruption, including foreign corruption, and other major asset generating crimes.
- Amend the legal framework to allow for the confiscation of property of equivalent value.
- Consider increasing the sanctions and seizures related to falsely declared or undeclared cross-border movements of currency and bearer negotiable instruments.

The relevant Immediate Outcomes considered and assessed in this chapter are IO6-8. The recommendations relevant for the assessment of effectiveness under this section are R.3, R4 & R29-32.

Immediate Outcome 6 (Financial intelligence ML/TF)

Use of financial intelligence and other information

104. Financial intelligence derives from a wide range of information collected by LEAs and received by FINTRAC. Both processes are closely linked. FINTRAC's main financial intelligence product takes the form of disclosures made in response to LEAs' requests (i.e. voluntary information records, VIRs). FINTRAC also disseminates information to LEAs spontaneously (i.e. through "proactive disclosures").

105. LEAs request and obtain financial information held by the private sector either through a court warrant or a production order, when they can establish (as per the CC) that assets are POC. To obtain this judicial authorization, LEAs must identify the FI/DNFBP or entity that holds the information (i.e. account or assets owned or controlled, financial transactions or operation). Various methods are available (see TCA criterion 24.10) and used in practice, such as "grid searches," VIRs to FINTRAC, and consultation of other sources of information as well as use of a range of investigative activities. In Ontario (where the major D-SIBs have their headquarters), "grid searches" are frequently conducted: LEAs send a request to the six D-SIBs (as they dominate about 80% of the deposit-taking market) inquiring whether a particular person is amongst their customers. If there is indication that this person is in business relationships with another FI or with a DNFBP, a request will be sent to that RE as well. Once a D-SIB (or other RE) confirms that a specific person is its

customer, the LEAs apply for a court order requiring the D-SIB to produce the relevant account and beneficial ownership information, as well as transaction records. If necessary, the production is staged to expedite the procedure (i.e. the specific information stated in the order is produced first, and the remainder of the information is provided at a later stage). Nevertheless, the D-SIBs typically take up to several weeks to provide basic and beneficial ownership information to the LEA. As result of the time required at the initial stage (i.e. identification of the relevant RE that may hold the information), as well as the time imparted to implement the production order, it frequently takes 45-90 days before LEAs can obtain the initial transaction records of potential POCs. If the culprit uses numerous layering techniques before integration, it takes LEAs several months or even years to trace POCs. The outlined process is useful only if the persons under investigation bank with the D-SIBs or one of the other large FIs. In cases where a targeted person or entity is in a business relationship with a smaller FI or a DNFBP, the tracing of assets is far more burdensome; given the size of Canada and its financial and non-financial sectors, it is not possible for LEAs to check with each FI and DNFBP individually whether it holds relevant information. In these instances, the identification of the relevant FI or DNFBPs relies on other potentially lengthier methods (e.g. surveillance).

106. LEAs frequently obtain financial information and intelligence from FINTRAC, with or without prior judicial authorization. Most often, they request the information by sending VIRs (which do not require prior judicial authorization). This provides LEAs with a quicker access to the information they need to obtain the judicial authorization (but timeliness of production of requested information remains a challenge). The number of VIRs has increased steadily over the years.[37] This indicates a greater appetite for and appreciation of FINTRAC's reports.[38] Most LEAs expressed their satisfaction with the richness of FINTRAC's responses to VIRs and mentioned that these responses adequately supplement their ongoing investigations.[39] In 2011, the Canadian Association of Chiefs of Police also recognized the contribution of financial intelligence, and called on all Canadian LEAs to include financial intelligence in their investigations and share their targets with FINTRAC.[40]

107. FINTRAC also provides information to LEAs on a spontaneous basis, through proactive disclosures, both in instances linked to ongoing investigation and in cases that identify new potential targets. Between 1 January 2010 and 31 November 2015, the RCMP received 2 497 FINTRAC

[37] Number of VIRs received: 2010–2011: 1 186; 2011–2012: 1 034; 2012–2013: 1 082; 2013–2014: 1 320; 2014–2015: 1 380.
[38] The Canadian authorities were not able to provide additional information regarding the proportion of predicate offense investigations that lead to a VIR.
[39] The Canadian authorities provided examples of written testimonies of some agencies' satisfaction with FINTRAC's response to their VIRs. E.g. "*The disclosure was very impressive in its detail and scope. Shortly after receiving it, our General Investigation Service Unit generated a file resulting in a large seizure of drugs. The individuals mentioned in the disclosure were identified as involved*" (RCMP 'G' Division Federal Investigations Unit); "*The information obtained led us to start a new investigation focused on the money trail—namely the illegal means used by the accused to launder the money they obtained in this case*"(*Sûreté du Québec*); "*Quick turnaround time was appreciated. The disclosures provided new information of potential interest along with account numbers not previously known. The Service was further able to identify additional relationships, which assisted our national security investigation. The information in the electronic funds transfers was found to provide valuable intelligence*" (Canadian Security Intelligence Service).
[40] Canadian Association of Chiefs Police (Resolution #06-2011).

disclosures, 867 of which were proactive.[41] Of these proactive disclosures, the authorities indicated that 599 generated a new investigation.[42] Very few resulted in ML charges (see IO.6.3 and IO.7). The cases communicated to and discussed with the assessors highlighted that FINTRAC information (in response to VIRs and/or shared proactively) is used by LEAs mainly as a basis for securing search warrants, aiding in the selection of investigational avenues (including the identification of targets, associates, and victims) and providing clarification of relevant domestic and international bank accounts and cash flows.

108. Additional relevant information is used to varying degrees: (i) The RCMP and other LEAs receive relevant information from provincial Securities Commissions and recognize the value of such information in combating ML/TF in the context where corporations are identified as very highly vulnerable to be abused for ML/TF. In Toronto and Montreal, the RCMP now includes personnel from the Securities Commission (Joint Securities Intelligence Unit—SIU) to facilitate intelligence gathering, analysis, and dissemination functions. The Canadian authorities provided examples of the use of information communicated to LEAs by the "*Autorité des marches financiers*" (AMF) (including Project Carrefour detailed below, as well as projects Convexe, Jongleur, Incitateur, and Ilot). In these cases, the financial intelligence was used to develop the financial part of the investigation into the predicate offense, not to investigate potential ML activities. (ii) The CRA-CID also uses financial intelligence to identify potential tax evasion. (iii) The CBSA forwards to FINTRAC and to the RCMP all Cross-Border Currency reports (CBCRs) submitted by importers or exporters. It also forwards seizure reports to FINTRAC. It seems that both FINTRAC and the RCMP use the CBSA information to supplement ongoing analysis and investigations[43] and that they analyse or, in the case of LEAs, investigate the CBSA information to a very limited extent, namely only when it has no link to existing cases (see IO.7). Two cases originating from this intelligence have been communicated to the assessors, including project Chun (see Box 4 in IO.7).

[41] FINTRAC also makes disclosures to other LEAs.
[42] According to the authorities, 297 completed feedback forms indicated that FINTRAC proactive disclosures prompted a new investigation in 53 cases between 1 January 2008 and 31 November 2015. In 92 cases a proactive disclosure provided the names of, or leads on, previously unknown persons or businesses/entities, 90 provided new information regarding persons or businesses of interest, 53 triggered a new investigation and 17 provided intelligence that may generate a future investigation. Only one of the 53 new investigations prompted following a proactive disclosure was shared with the assessors.
[43] RCMP indicated that of all ML, PPOC and TF investigations, cross-border currency reporting have been used in 331 cases.

3

Box 2. **Project Carrefour**

In December 2008, the Montreal Integrated Market Teams (IMET) Program[44] initiated an investigation based on an AMF referral. The AMF is mandated by the government of Quebec to regulate the province's financial markets and provide assistance to consumers of financial products and services. The referral indicated that individuals' Registered Retirement Savings Plans (RRSPs) and other types of retirement savings accounts were being emptied using methods that avoided attention from regulatory and fiscal authorities. The scheme consisted of attracting the attention of investors, through classified ads, with RRSPs and/or other types of retirement savings accounts looking for financial aid. In order for the investors to receive that aid, they had to give up full control of their accounts. The operators of the schemes would then empty those accounts to use the funds to transact on a variety of publicly traded companies under their control, hence engaging in market manipulation. On 15 February 2011, eleven Montréal and Toronto residents were charged with various fraud related offenses committed against 120 investors. They were also charged with fraudulent manipulation of stock exchange transactions estimated at USD 3 million.

109. In sum, financial intelligence is used to some extent to develop evidence and trace criminal proceeds. While a great deal of information provided by REs and others (i.e. in STRs and CBCRs) is used by FINTRAC for tactical analysis, strategic analysis, and to take supervisory action, a large part of this information is not further used by its partners for tactical cases, until it appears relevant for an ongoing investigation. Moreover, a relatively small portion of the intelligence is used for the specific purpose of pursuing ML activities.

110. Financial intelligence and other relevant information are, however, more frequently used to pursue TF. FINTRAC, in consultation with some of the other competent authorities, published advisories that assisted the FIs in their efforts to identify potential ISIL and TF-related activities and funding. Financial intelligence is accessed and used in TF investigation (see below and IO.9), and the on-site discussions as well as the authorities' submissions indicate that FINTRAC's proactive disclosures and responses to VIRs are appreciated by LEAs in their TF efforts.[45]

STRs received and requested by competent authorities

111. FINTRAC receives a significant quantity of information in various reports (see table below), which it uses to develop its financial intelligence.

[44] The objective of the IMET program is to effectively enforce the law against serious criminal capital market fraud offenses in Canada. The authorities involved in the program are the RCMP, ODPP, DOJ, and Finance Canada.

[45] "*FINTRAC is considered a key partner and has provided valuable financial intelligence on an ongoing basis that contributed to "terrorist financing investigations." FINTRAC through their disclosures identified new linkages/nexus between entities and/or individuals through financial transactions which surfaced new avenues of investigation. FINTRAC has always responded in a timely fashion to our priority VIRs*" (RCMP Anti-Terrorist Financing Team, National Security Criminal Operations, Headquarters, Ottawa. FINTRAC 2012 Annual Report, pg. 11, Document 102).

Table 2. **Types of Reports Received by FINTRAC (excluding terrorist property reports)**

	2010–2011	2011–2012	2012–2013	2013–2014	2014–2015
Large Cash Transaction Reports	7 184 831	8 062 689	8 523 416	8 313 098	8 445 431
Electronic Funds Transfer Reports	11 878 508	10 251 643	10 993 457	11 182 829	12 348 360
STRs	58 722	70 392	79 294	81 735	92 531
Cross-Border Currency Reports / Cross-Border Seizure Reports	40 856	35 026	31 826	42 650	47 228
Casino Disbursement Reports	102 438	109 172	116 930	130 141	155 185
Total	**19 265 355**	**18 528 922**	**19 744 923**	**19 750 453**	**21 088 735**

112. With respect to STRs, the authorities indicated that the quality of reporting has improved over the years—notably as a result of FINTRAC's efforts to reach out to REs—and that the information filed is particularly useful for the analysis of individual behaviours and transactional activity. Half of the STRs are sent by MSBs. Banks and credit unions and *caisses populaires* have submitted more STRs to the FIU in the last two years, but the number of STRs filed by DNFBPs other than casinos, while it has increased as a result of FINTRAC's outreach efforts, remains very low (278 in 2014–2015), including those filed by the real estate sector despite the very high ML risk that it faces.[46]

113. The wide range of systematic reports of transactions above CAD 10 000 that FINTRAC receives constitutes an important source of information which has allowed FINTRAC to detect unusual transactions, make links between suspected persons and/or detect bank accounts and other assets held by these persons.

114. Despite the important amount of information received, several factors limit the scope and depth of the analysis that the FIU can do, namely: (i) the fact that some REs listed in the standard are not required to file STRs (in particular legal counsels, legal firms and Quebec notaries) – as a result, FINTRAC does not receive information from key gatekeepers which would otherwise prove useful to its analysis and/or highlight additional cases of potential ML; (ii) the fact that some REs, such as those active in the real estate sector, file few STRs – as a result, information on some areas of high risks is limited; (iii) delays in reporting (FINTRAC supervisory findings seem to confirm that STRs are not filed promptly but within 30 days); and (iv) the fact that FINTRAC is not authorized to

[46] Regarding the real estate sector, the authorities indicated that an important part of STRs received from banks and credit unions and *caisses populaires* over the last three years related to suspicions of ML activities in real estate transactions. This compensates partially but not fully the lack of reporting from legal professionals—other than BC notaries (who, although subject to AML/CFT reporting requirements had not filed STRs at the time of the assessment)- who are directly involved in these transactions. Real estate brokers, sales representatives, and developers (when carrying out certain activities) have filed STRs but in very small numbers.

request additional information related to suspicions of ML, predicate offenses or TF from any REs – as a result, FINTRAC is largely dependent on what is reported. These factors entail that it is challenging for FINTRAC to follow the flows of potential POC in certain cases. For example, when an STR indicates that suspicious funds have been transferred to another FI, FINTRAC can only follow the trail of particular activities or transactions if other intermediaries and/or the final FI have also filed an STR or another report above the required threshold. This is particularly acute when the funds transferred are divided into multiple transfers below CAD 10 000. Enabling FINTRAC to request additional information from REs would considerably facilitate and strengthen the analysis and development of financial intelligence.

Operational needs supported by FIU analysis and dissemination

115. FINTRAC nevertheless provides a significant amount of financial intelligence to LEAs. Over the years, it has increased the number of disclosures sent to regime partners, both in response to VIRs and proactively. In 2014–15, the FIU sent 2 001 disclosures to partners including the RCMP, CBSA, CRA, CSIS, municipal and provincial police, as well as foreign FIUs. Of these, 923 were associated to ML, while 228 dealt with cases of TF and other threats to the security of Canada. 109 disclosures had associations with all three. Additional statistics provided showed that FINTRAC's disseminations of financial information are appropriately spread between the different provinces.

Table 3. **FINTRAC Disclosures to Regime Partners** [1]

Year	Municipal Police	Provincial Police	CRA	CSIS	CBSA	CSEC	RCMP	Total
2012–13	182	144	149	164	96	32	580	**1 347**
2013–14	207	135	153	243	139	33	703	**1 613**
2014–15	331	214	173	312	169	23	779	**2 001**

1. A number of disclosures may have been sent to more than one regime partner.

116. The main predicate offenses highlighted in the disclosures are drugs-related offenses (27% of the cases disseminated), frauds (30%), and tax evasion (11%). Between FY 2010–2011 and 2013–2014, the type of predicates was stable.[47] In FY 2014–2015, FINTRAC also provided information pertaining to potential other predicate offenses to ML (namely crimes against persons, child exploitation, prostitution, weapons and arms trafficking, cybercrimes, and illegal gambling).[48] These predicate offenses are in line with the main domestic sources of POC identified in the NRA, except corruption and bribery, counterfeiting and piracy and tobacco smuggling and trafficking. FINTRAC's disclosures have assisted LEAs in their ongoing investigations in a number of instances, such as in the case of project Kromite described below.

[47] The range of predicate offenses related to the cases disclosed were: drugs, fraud, "unknown," i.e. unspecified, tax evasion, corruption, customs/excise violations, theft, human smuggling/trafficking.
[48] The percentages were the following: crimes against persons, 4%; child exploitation, 1%; prostitution/bawdy houses, 1%; weapons/arms trafficking, 1%; cybercrimes, 0.3%; illegal gambling, 0.3%.

Box 3. **Project Kromite**

In May 2013, the RCMP participated in an international investigation which focused on significant amounts of heroin being imported from source countries (Afghanistan, Pakistan and Iran) to Tanzania and South Africa. The investigation determined that the heroin was transported through various methods to destinations in Europe, South America, the Far East, Australia, the United States, and Canada. Profits from the distribution and sale of illicit drugs were being collected in Canada and disbursed back to the criminal organization in South Africa and Tanzania.

The RCMP sent VIRs to, and received financial disclosures from FINTRAC. The disclosures were able to identify accounts, businesses owned by the subjects and transactions which led to the identification of relevant banking information and, ultimately, to the identification of targets. The financial intelligence was used by the RCMP to collaborate with the DOJ and the PPSC to draft and issue judicial authorizations. Authorizations took various forms including four MLATs, which were issued to three foreign jurisdictions to provide a formal release of information, and Production Orders and Search Warrants that were used to trace and seize POC, both assets and funds. Formal drug-related charges under the Canada's Controlled Drugs Substances Act were laid. The ML-related component of the investigation has been concluded and potential ML/PPOC-related charges were being prepared at the time of the assessment, but no charges had been laid.

117. FINTRAC tailors its analysis to the LEAs' operational priorities. It focuses mainly on answering the VIRs and also discloses intelligence related to LEAs' priorities. Regular operational meetings[49] and discussions are conducted with disclosure recipients to discuss investigative priorities, analytical processes, the development of indicators, and to provide assistance regarding the use of FINTRAC intelligence. The CSIS Financial Intelligence Center (FIC), which is in charge of all financial Intelligence related to national security investigations and linked notably to terrorism and proliferation, also interacts with FINTRAC on a regular basis.

118. FINTRAC's financial intelligence products include its analysis of all relevant information collected: the information contained in STRs, EFTRs, LCTRs, other reports and other information received or accessed by the FIU are all an integral part for developing case disseminations. As mentioned above, LEAs generally consider that FINTRAC's disclosures provide useful supplements to their investigations and generally meet their operational needs. FINTRAC also uses the information gathered in the exercise of its AML/CFT supervisory function, as well as information from a fair range of law enforcement and administrative databases maintained by—or on behalf of—other authorities, and information from open and public sources. While this broad range of information is undeniably useful, it does not necessarily provide FINTRAC with sufficient information about the suspected person's financial environment. In this context, it would prove particularly useful to ensure that FINTRAC has adequate access, for the purposes of the analysis of STRs, to information collected by the CRA, as this would assist FINTRAC with information that could

[49] Seventy-six meetings have been laid in 2014–2015 between FINTRAC and different LEAs agencies, including municipal, provincial and federal agencies, as intelligence services.

strengthen its analysis further, such as information about a person's or entity's income and assets, as well as information on trust assets and trustees (see IO.5).

119. In addition to disclosures in response to VIRs and proactive disclosures, FINTRAC produced from FY 2010/11 to 2014/15, 62 strategic intelligence and research products, which identify ML/TF methods and techniques used by listed terrorist groups and criminal networks, emerging technologies, as well as vulnerabilities in different sectors. These reports support the operational needs of competent authorities and many of them are developed in collaboration with the Canadian and international security, intelligence and law enforcement communities. FINTRAC's classified strategic financial intelligence assessments address the nature and extent of ML/TF activities inside and outside of Canada. Canadian authorities provided testimonies of some partners' satisfaction with FINTRAC's strategic intelligence reports.[50]

120. FINTRAC provides a significant amount of disclosures on TF to a variety of LEAs. FINTRAC sent 234 disclosures related to TF and other threats to the security of Canada in 2013-14, and 228 disclosures in 2014-15. These disclosures were communicated to a variety of partner agencies, including CBSA, CRA, CSIS, CSE and RCMP, as well as to municipal and provincial police, and other FIUs, and generated 40 new RCMP TF investigations in 2014 and 126 in 2015.. FINTRAC has increased its disclosures regarding TF to 161 for the first six months of FY 2015-2016, of which 82 were proactive disclosures. This increase in the number of disclosure shows the involvement of the FIU in analysing and disseminating information regarding TF.

Cooperation and exchange of information/financial intelligence

121. Most agencies adequately cooperate and exchange information including financial intelligence. FINTRAC meets with partners on a regular basis, as seen above, and the FIU focuses on priority investigations to support the LEAs' operational needs. In particular, VIRs constitute an important channel for cooperation and information sharing between FINTRAC and LEAs, as well as between LEAs. FINTRAC may send a single disclosure to multiples agencies simultaneously, which informs LEAs that another agency is working on a case. A LEA can further disseminate a disclosure that was based on another agency's VIR, provided that it obtains the permission from the source agency to further disseminate to the requester. In 2014-2015, FINTRAC was authorized by the source agency to disseminate further its disclosures to another LEA in some 41% of cases.

[50] FINTRAC's report, Mass Marketing Fraud: "*Money Laundering Methods and Techniques, is helpful to Canadian law enforcement and government agencies in understanding the complexity and international scope of mass marketing fraud impacting Canada. The CAFC has been able to leverage this report to provide insight into the prominent money laundering techniques used by criminal organizations engaged in mass marketing fraud*" (Canadian Anti-Fraud Centre); "*FINTRAC's report (on terrorism financing risks related to a particular group) … have contributed to AUSTRAC's understanding of the topic … FINTRAC and AUSTRAC have been able to collaborate on analytical products, supporting a multilateral approach to information sharing*" (Australian Transaction Reports and Analysis Centre) ; "*Public Safety Canada benefits from strategic financial intelligence reports on ML and TF provided by FINTRAC to inform the overall analysis of national security and organized crime issues. Strategic financial intelligence helps Public Safety to identify the nature and extent of money laundering and terrorism* financing and its potential links to *Canada, international conflicts, crimes, sectors and/or organizations, and the growing links between transnational organized crime and terrorism*" (Public Safety Canada).

122. In addition, FINTRAC has direct and indirect access to LEAs and Security (i.e. intelligence services) databases. The authorities indicated that FINTRAC regularly queries LEA databases in the course of its normal work. FINTRAC and LEAs have established privacy and security frameworks to protect and ensure the confidentiality of all information under FINTRAC's control (including information collected, used, stored and disseminated). In October 2013, FINTRAC strengthened its compliance policies and procedures to increase further the protection of the confidentiality of the information it maintains.

123. Where necessary, LEAs also share information indirectly via FINTRAC by highlighting the disclosures that should be disclosed to other agencies: In this respect, the RCMP has, in specific cases, flagged some files with cross border features to the FINTRAC for disclosure to the CBSA where cross border elements. Similarly, the CBSA has advised FINTRAC to disclose the results of certain VIRs to another regime partner where it determined that further investigations should be carried out.

124. Additionally, the CRA—Charities shares information with other government departments, including RCMP, CSIS and FINTRAC, when there are reasonable grounds to suspect the information would be relevant to an investigation of a terrorism offense or a threat to the security of Canada. Similarly, CSIS shares information on security issues with a range of domestic partners, including FINTRAC, on a regular basis. The sharing of intelligence includes financial intelligence.

Overall Conclusions on Immediate Outcome 6

125. **Canada has achieved a moderate level of effectiveness for IO.6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

126. ML cases are primarily identified from investigations of predicate offenses, human sources (e.g. informants, victims, suspects, informers, etc.), intelligence (including FINTRAC responses to VIRs), coercive powers, and, in fewer instances, FINTRAC's proactive disclosures, as well as referrals from other government departments without ML investigative powers. LEAs mentioned that they examine all cases with a financial component and assess whether a concurrent financial investigation is warranted. The decisions on whether to investigate a case and how much resources should be devoted to a specific investigation are guided by the LEAs' prioritization processes.[51] As a result, LEAs principally investigate the financial aspects of ML[52] or PPOC[53] occurrences in serious

[51] In the case of the RCMP: The Prioritization Process is designed to aid the judgment of RCMP management in the application of its investigative resources against the most important (priority) criminal threats and activities facing the country. It takes into consideration a series of variables designed to gauge the overall profile of the investigation (or project), its targets, the expected impact against those targets, as well as the expected cost in terms of investigative resources and the length of time they will be dedicated to the project. Prioritization criteria include: economic, political and social integrity of Canada, strategic relevance to RCMP, links to other GoC and partner priorities, etc. Investigations are scored in three tiers (Tier 1 being the highest priority). Highest priority files afforded resources as required to successfully conduct the investigations.
[52] ML encompasses the CC: ss. 462.31(1) and (2) for laundering property and proceeds of property.

and organized crime cases, and in less serious investigations pursue PPOC charges if proceeds are seized through the predicate investigation.

Table 4. **ML and PPOC-Related "Occurrences**[1]
(numbers extracted from all police services' records management systems across Canada)

	2010	2011	2012	2013	2014	Total
ML-Related Occurrences	684	716	596	593	608	3 197
PPOC-related Occurrences	42 261	38 796	38 638	37 521	36 012	193 228
Total	**42 945**	**39 512**	**39 234**	**38 114**	**36 620**	**196 425**

1. The basic unit of this data capture system is an "incident", which is defined as the suspected occurrence of one or more criminal offense(s) during one single, distinct event. During the on-site visit, authorities explained that the ML/PPOC related occurrences are classified when the offenses or incidents fall into the definitions of PPOC/ML under the CC. E.g. a simple theft case can be regarded as a PPOC incident; and if the thief further transfers the stolen good, it will be a ML occurrence.

Source: Statistics Canada's Uniform Crime Reporting Survey (2015)

Table 5. **ML/PPOC Occurrences Handled by the RCMP**

	2010	2011	2012	2013	2014	Total
ML-Related Occurrences	945	844	692	619	664	3 764
PPOC-Related Occurrences	12 753	11 408	11 573	12 299	14 177	62 210
Total	**13 698**	**12 252**	**12 265**	**12 918**	**14 841**	**65 974**

Source: RCMP

127. The ML/PPOC occurrences handled by RCMP (unlike the numbers provided in the table for all police forces) include 1 599 ML- and 13 179 PPOC-related "assistance files," i.e. cases where the RCMP rendered assistance to foreign agencies. In practice, requests from foreign counterparts are used to a limited extent to identify potential ML cases in Canada. In particular, requests from foreign countries seeking information regarding Canadian bank accounts suspected of receiving or transferring POC are generally only acceded to and a ML investigation initiated when the account holder(s) is/are subject to ongoing investigation(s) in Canada, or there is clear indication of a predicate offense having been committed in Canada. Although Canada has identified third-party ML as one of the very high ML threat, it does not focus sufficiently on foreign requests that may reveal the presence, in Canada, of third-party launderers.

128. As mentioned in IO.6, FINTRAC provides a significant amount of information to LEAs. FINTRAC responses to VIRs (which constitute the majority of FINTRAC's disclosures) and proactive disclosures that have a link with an existing file and/or target are adequately used by LEAs. LEAs mentioned that due to time and resources considerations, in line with their prioritization process, fewer investigations are initiated on the basis of a proactive disclosure which has no link to an ongoing investigation. Between 2010 and 2014, FINTRAC made 867 proactive disclosures to the RCMP, of which 599 led to new ML/PPOC related occurrences for further investigations.

[53] PPOC includes CC s. 354 possession of property of proceeds obtained by crime.

129. While the CBSA may investigate fiscal crimes, it does not have the powers to investigate related ML/PPOC cases, and in instances where it considers that there are reasonable grounds to suspect that a person is or has been engaging in ML activities, it reports the case to the RCMP. The latter recorded that between 2010 and 2014 there were 444 ML/PPOC occurrences related to cross border currency reporting. The authorities provided one case ("Project Chun," described in the Box below) of a successful ML investigation started in 2002 on the basis of a CBSA referral. Whilst the assessment team was also shown several ML cases involving parallel investigations arising from CBSA's enquiries into smuggling or customs related offenses, no other cases arising from CBSA's cross-border declaration/seizure reports were provided. It therefore appears that, in practice, information collected at the border is analysed or investigated with a view to pursuing ML activities to a very limited extent only. The cross-border declaration system is not adequately used to identify potential ML activities.

Box 4. **Case study: Project Chun**

In October 2002, a male was intercepted at the Montreal International Airport with USD 600,000 cash in his hand luggage. In the absence of a valid explanation, the money was seized and the case was referred to RCMP which initiated an investigation to determine the source and destination of the money. Extensive enquiries unveiled that the male and his wife owned two currency exchange companies in Canada and in 2000 they made an agreement with a drug trafficker to assist the latter in laundering proceeds deriving from drug trafficking activities. The laundering included use of various financial services and an elaborate scheme for the transfer of money to a bank in Cambodia that was owned and controlled by the couple. The precise amounts involved in these activities are estimated at more than CAD 100 million. Information received from FINTRAC indicated that the couple dealt in large sums of cash and that their bank account activities did not fit their economic profiles. Travel records of one of the accomplice money launderers were received from Cuba through MLAT requests. The accomplice, who was detained in custody in the US, was later transferred from the US to Canada to provide testimony for the prosecution. Canadian investigators had travelled to Israel and Cambodia for tracing after and restraining the crime proceeds. The couple applied delaying tactics during the prosecution and the Canadian authorities eventually convicted the couple with six counts of Money Laundering and seven counts of tax offenses. In March 2015, the couple was each sentenced to eight years of imprisonment and ordered to pay fines of CAD 9 million. Two real properties, USD 600 000 and the shares of a bank in Cambodia were forfeited.

130. Canada's main law enforcement policy objective is to prevent, detect and disrupt crimes, including ML, but in practice, most of the attention is focused on securing evidence in relation to the predicate offense and little attention is given to ML, as evidenced by the discussions held as well as by the case studies provided. LEAs focus on criminal actions undertaken by OCGs (i.e. mainly drug-related offenses and fraud). Cases studies and figures provided by LEAs demonstrated that they also investigate other high-risk offenses (e.g. corruption and tobacco smuggling), but to a limited extent only. Insufficient efforts are deployed in pursuing the ML element of predicate offenses and pursuing

ML without a direct link to the predicate offense (e.g. third-party/professional money launderers). Since 2010, when tax evasion became a predicate offense to ML, none of the tax evasion cases finalized by the CRA have included sanctions for ML. There are, however, ongoing investigations that contemplate the ML activities.

131. The various LEAs adequately coordinate their efforts, both at the strategic level and at the operational and intelligence levels, through working groups and meetings. Within the RCMP, a centralized database is used to minimize the risk of duplicative investigative efforts against the same groups or persons. Direct exchanges regularly occur during relevant LEAs meetings, as well as through specific joint projects: in particular, the CRA-CID and the RCMP have entered into special projects (i.e. Joint Forces Operations, JFOs) for a specific duration, to identify targets of potential criminal charges including ITA/ETA offenses. Between 2010 and 2015, 10 JFOs were conducted. In these cases, the JFO agreements do not supersede or override the confidentiality provisions of the ITA/ETA, but they, nevertheless, enable the CRA to provide tax information to the RCMP if this is reasonably regarded as necessary for the purposes of the administration and enforcement of the Acts.

132. LEAs regularly seek the production of a court order to obtain banking (or other relevant) information for the purposes of their investigations. However, as detailed in R 31.3 and IO6, the length of the process leading to the identification of relevant accounts considerably delays the tracing of POC in ML/PPOC investigations.

133. The LEAs also access tax information (outside JFOs) with prior judicial authorization. During the period 1 April 2013 to 31 December 2015, the CRA CID received in excess of 2 500 LEA requests for taxpayer information. One RCMP unit indicated that this information is obtained in all significant cases by way of letter under S241 of ITA when charges are laid or by CC authorization of Tax order. The RCMP sent 91 tax letters from 2010 to 2016.

134. LEAs also regularly consult public registries of land and companies, but the paucity of accurate basic and beneficial ownership information in these registries limit the usefulness of the information obtained. Investigations in Canada typically do not focus on complex ML cases involving corporate structures (and/or involving transnational activities). LEAs stated that, in the few cases where legal entities were under investigation, the beneficial ownership information was typically obtained from FIs, in particularly the D-SIBs. Investigators are aware of the risk of misuse of corporate entities in ML schemes, but, in some provinces, do not investigate such cases to the extent that they should mainly because of a shortage of adequate resources and expertise. As a result, some targets are not pursued or bank accounts investigated (e.g. in instances where multiple targets and accounts are involved), and LEA efforts are focused on easier targets where the chances of the investigations being cost effective are greater.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

135. According to the NRA, fraud, corruption, counterfeiting, drug trafficking, tobacco smuggling, and (although a recent phenomenon) third-party ML pose very high ML threats in Canada. The LEAs generally agreed with the NRA findings and have prioritized their resources on OCGs, which are

mostly involved in drug and fraud related offenses (see table below). As described above, LEAs, in particular the RCMP, have a prioritization process, which is continually evolving to address the current threats, taking into account a number of factors. At the time of the assessment, that process did not take the NRA's findings sufficiently into account.

Prosecuted ML-Related Cases	2010	2011	2012	2013	2014	Total	%
Money Laundering (CC s462.31)	88	86	130	108	114	526	51.2%
Fraud	12	27	57	61	53	210	20.4%
Drug Offenses	14	18	9	14	14	69	6.7%
Others	27	52	45	51	47	222	21.6%
Total	**141**	**183**	**241**	**234**	**228**	**1027**	**100.0%**

Source: Statistics Canada's Uniform Crime Reporting Survey (UCR) – all police services' records

Prosecuted ML-Related Cases	2010	2011	2012	2013	2014	Total	%
PPOC (CC 354, 355)	11930	11955	11179	10904	10292	56260	37.7%
Drug Offenses	4260	4351	4504	4020	3889	21024	14.1%
Fraud	3013	2690	2467	2352	2144	12666	8.5%
Others	13144	12602	12079	11656	9638	59119	39.7%
Total	**32347**	**31598**	**30229**	**28932**	**25963**	**149069**	**100%**

Source: Statistics Canada's Uniform Crime Reporting Survey (UCR) – all police services' records

136. The authorities provided in the above tables the number of prosecution cases, broken down by the most serious offense (MSO) of the case, in which at least one ML or PPOC charge was laid in 2010 to 2014. [54] This information does not distinguish third-party ML from self-laundering. These statistics show that high-threat predicate offenses, i.e. drug trafficking and fraud, account for 27.1% of ML or 22.6% of PPOC prosecutions only, which does not match the ML threats and risks identified in the NRA (which suggest that a higher percentage would be necessary to mitigate the risks). The figures provided do not show related prosecutions in the context of corruption, counterfeiting, and tobacco smuggling cases, but these cases could be embedded in the "others", "ML" or "PPOC" categories, when they were not the MSO. Canada provided further information to show that there were 68 counterfeiting related ML/PPOC cases, examples of tobacco smuggling related ML cases and one case (Project LAUREAT highlighted below) of a successful prosecution of corruption-related ML cases[55].

[54] RCMP also provided that between 2010 and 2014, it laid 130 630 PPOC charges against 35 600 persons and 1 904 ML charges against 503 persons.
[55] Two other corruption related ML cases, Project Ascendant and Project Assistance, were provided but both cases were under court proceedings.

Box 5. **Case study: Project LAUREAT**

In 2010, in order to obtain the CAD 1.3 billion contract of modernization of a Health Centre ("HC"), the president ("P") and vice-president ("VP") of an engineer company ("EC") had bribed the top officials, "Y" and "Z," of the HC to get the award. Upon the announcement of the award to EC, the VP transferred a total of CAD 22.5 million to the shell companies in foreign countries owned by Y and Z. Y further transferred the crime proceeds to the accounts of his wife's (Y's wife) shell companies. Numerous MLAT requests were executed and bank accounts in nine other countries, worth more than CAD 8.5 million, were blocked. Y, Z, P, VP were also extradited from other countries. The syndicate was charged with corruption, fraud, ML along with other offenses. For Y's wife, who has only been involved in laundering the CAD 22.5 million, was sentenced to 33 months of imprisonment.[1] Upon her conviction, seven buildings (value at CAD 5.5 million) were confiscated.

1. The sentence of Y's wife expires in December 2016, but she was granted full parole in September 2015.

137. While Project LAUREAT was relatively successful, overall, on the face of the statistics and cases provided as well as of the discussions held on-site, it was not established that Canada adequately pursues ML related to all very high-risk predicate offenses identified in the NRA.

138. As indicated in the statistics on standalone ML / PPOC prosecutions below, there were 35 (3.4%) and 14 271 (9.6%) standalone ML and PPOC concluded respectively in the last five years. As professional money launderers are mostly involved in ML (rather than PPOC) cases, the fact that Canada only led 35 prosecutions and obtained 12 convictions of single-charge ML cases in the last five years is a concern. It is possible and, according to the authorities, very likely that a professional money launderer would also be charged with another charge such as conspiracy, fraud, or organized crime in addition to ML, but the numbers nevertheless appear too low in light of the risk.

Table 6. **Results of Single Charge ML Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	2	2	4	3	1	12	34.3%
Acquitted	0	0	0	0	1	1	2.9%
Stayed	0	1	3	1	0	5	14.3%
Withdrawn	2	4	4	2	2	14	40.0%
Other decisions	0	0	1	0	2	3	8.6%
Total	**4**	**7**	**12**	**6**	**6**	**35**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 7. **Results of Single Charge PPOC Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	1332	1199	1108	1017	947	5603	39.3%
Acquitted	115	84	76	127	98	500	3.5%
Stayed	589	642	640	611	581	3063	21.5%
Withdrawn	1158	1077	1022	904	806	4967	34.8%
Other decisions	53	23	24	23	15	138	1.0%
Total	**3247**	**3025**	**2870**	**2682**	**2447**	**14271**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

139. Canada's NRA also identified very high ML vulnerabilities in the use of trusts and corporations. LEAs confirmed that corporate vehicles and trusts are misused to a relatively large extent for ML purposes. As the case study Dorade (below) indicates, the authorities have been successful in identifying the legal persons and arrangements involved in the ML schemes and in confiscating their assets in some instances. However, overall, it was clear from the discussions held with police forces and prosecutors that legal persons are hardly ever prosecuted for ML offenses, mainly because of a shortage of adequate resources and expertise. Investigators are nevertheless aware of the risk of misuse of corporate entities in ML schemes and that more focus should be placed on this risk.

Box 6. **Case study: DORADE**

During the investigation of a fraud syndicate, it was revealed that the director of a loan company had set up, with the assistance of various professional accomplices, foreign shell companies located in tax havens for receiving the crime proceeds and lending the sum back to loan company for its legitimate loan business, thereby facilitating the director to evade tax payment and recycle crime proceeds. It was estimated, between 1997 and 2010, a total of CAD 13 million of tax was evaded. With the assistance of MLAT requests, the syndicate members were identified and the proceeds, whether domestic or abroad, were restrained and eventually confiscated. The director and the professionals were convicted of fraud and ML and sentenced to 36–84 months of imprisonment. However, all the ML charges attracted an imprisonment term of less than 18 months and to be served concurrently with the Fraud sentence.

140. Overall, while there are exceptions, law enforcement efforts are not entirely in line with Canada's NRA risk profiles. As previously noted, LEAs' prioritization processes place strong attention to National Security investigations, OCGs, and, to a lesser extent, more recently third-party ML in an international context. Other instances of high threat predicate offenses, especially fraud, corruption, counterfeiting, tobacco smuggling, and related ML, as well as laundering activities in Canada of the proceeds of foreign predicate offenses, third-party ML and ML schemes involving corporate structures are not adequately ranked in the prioritization process and, consequently, are not pursued to the extent that they should.

3

Types of ML cases pursued

141. Different types of ML and PPOC cases are prosecuted, but there is insufficient focus on the types of ML that are more significant in Canada's context, i.e. ML related to high-risk predicate offenses. In addition, prosecutions of ML-related cases focus on the predicate offenses, with the ML charge(s) often withdrawn or stayed after plea bargaining and re-packaging of charges. The number of standalone ML cases is comparatively low, indicating few investigations and hence prosecutions of third-party ML and foreign predicate offenses despite their high ranking in the NRA. According to the authorities, as far as third-party ML is concerned, the low number of investigations and prosecutions is that the magnitude of the threat has only recently reached a high level. Finally, legal persons are frequently misused for ML purposes, but not often pursued for ML offenses. The tables below show the results of ML cases brought before the courts and the charges laid in these cases.

Table 8. **Results of ML-Related Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	82	108	140	136	146	612	59.6%
Acquitted	2	0	0	4	7	13	1.3%
Stayed	8	12	15	26	18	79	7.7%
Withdrawn	49	63	74	64	53	303	29.5%
Other Decisions	0	0	12	4	4	20	1.9%
Total	**141**	**183**	**241**	**234**	**228**	**1027**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 9. **Results of ML-Charges**

	2010	2011	2012	2013	2014	Total	%
Guilty	38	21	35	31	44	169	9.4%
Acquitted	5	1	8	6	9	29	1.6%
Stayed	17	26	144	45	31	263	14.6%
Withdrawn	132	190	366	327	294	1309	72.7%
Other Decisions	2	2	14	7	5	30	1.7%
Total	**194**	**240**	**567**	**416**	**383**	**1800**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

142. Between 2010 and 2014, a total of 1,800 ML charges were concluded in 1,027 cases. Although about 60% of these cases were led to convictions, only 169 ML charges (i.e. some 9%) resulted in a conviction. Some 87% of the ML charges were either withdrawn or stayed. The reasons provided for the withdrawal of the ML charges included insufficient evidence, the lack of public interest in the pursuit of the charges, the avoidance of overcharging, as well as repackaging of charges and plea bargaining (as the ML/PPOC charge will not normally add any additional sentence to the defendant and it is easier for the defendant to accept the guilty plea of the predicate offenses in order to contribute to a fair and efficient criminal justice system). The consultation with prosecutors at an earlier stage of the ML cases is clearly useful in securing the necessary evidence

and avoiding a waste of investigative efforts. The length of criminal proceedings in ML cases is also a concern. Proceedings may take a number of years during which the subjects of the investigation and prosecution may continue their unlawful businesses and dispose of the POCs (as was the case in Project Chun for example).

143. Over the last years, although 68.4% of PPOC cases resulted in convictions, 74.6% of the PPOC charges were withdrawn / stayed or dealt with by other means, and the defendants were only charged with and convicted of the predicate offenses.

Table 10. **Results of PPOC-Related Cases**

	2010	2011	2012	2013	2014	Total	%
Guilty	22 974	21 728	20 525	19 611	17 191	102 029	68.4%
Acquitted	388	349	339	404	391	1 871	1.3%
Stayed	2 769	3 193	3 157	3 148	2 857	15 124	10.1%
Withdrawn	5 961	6 140	6 021	5 606	5 380	29 108	19.5%
Other Decisions	255	188	187	163	144	937	0.6%
Total	**32 347**	**31 598**	**30 229**	**28 932**	**25 963**	**149 069**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 11. **Results of PPOC-Related Charges**

	2010	2011	2012	2013	2014	Total	%
Guilty	13 493	12 782	11 178	10 996	10 072	58 521	23.6%
Acquitted	736	715	1 716	674	817	4 658	1.9%
Stayed	9 178	9 715	9 183	9 132	6 894	44 102	17.8%
Withdrawn	28 776	28 388	27 402	27 375	25 130	137 071	55.2%
Other decisions	1 120	912	883	753	416	4 084	1.6%
Total	**53 303**	**52 512**	**50 362**	**48 930**	**43 329**	**248 436**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

144. Overall, of the 1 027 ML-related cases and 102 029 PPOC-related cases that entered the court system, over 60% resulted in convictions, though most of the defendants were convicted of the predicate offenses rather than the ML or PPOC charges. This indicates that Canada is able to investigate and prosecute predicate offenses in ML/PPOC-related cases and disrupt some of the ML/PPOC activities. One hundred sixty-nine ML charges were led to a conviction in the past five years (i.e. 33.8 charges on average annually), which appears very low in light of the magnitude of the ML risks identified. Canada does not pursue the ML charges sufficiently.

Effectiveness, proportionality and dissuasiveness of sanctions

145. The totality principle[56] always applies in the sentencing, and a ML/PPOC sentence is usually ordered to be run concurrently with the predicate offenses. The statistics below indicate the sanctions imposed for ML in instances where the ML charges were the most serious offenses (MSO). The vast majority of natural persons (i.e. 89%) convicted for ML have been sentenced in the lower range of one month to two years of imprisonment or awarded non-custodial sentences.[57] This is proportionate with the type of ML activities most frequently pursued in Canada. However, although this is not made evident in the statistics provided, it is apparent from the case examples provided, and in Projects Dorade and Laurent mentioned above, that many sanctions imposed on money launderers are low even in the (relatively few) cases of complex ML schemes and/or of professional launderers brought before the courts. None of the PPOC convictions attracted a sentence of more than two years. In these circumstances, the sanctions applied do not appear to be of a level dissuasive enough to deter criminals from ML activities.

Table 12. **Sanctions in ML Cases Where ML was the Most Serious Offense, from 2010 to 2014**[1]

	Number	Percentage
Custodial Sentence	**80**	**55.2%**
• Less than 12 months	47	32.4%
• 12 to 24 months	17	11.7%
• More than 24 months	16	11.0%
Conditional sentence, probation, fine, restitution	**65**	**44.8%**
Total	**145**	**100.0%**

1. There are other undisclosed cases where the ML offense runs concurrently with another MSO.

Extent to Which Criminal Justice Measures are Applied Where Conviction is Not Applicable

146. Information provided under IO.8 reveals that non-conviction based forfeiture amounted to 17% of the total forfeiture. Whilst it is not encouraged to drop the criminal charges during the judicial process, Canada's use of civil confiscation is not to be discounted. Plea bargaining and repackaging of charges have also been used in the prosecution stage for shortening the length of court proceedings.

Overall Conclusions of Immediate Outcome 7

147. **Canada has achieved a moderate level of effectiveness for IO.7**.

[56] Totality principle is a common law principle, which applies when a court imposes multiple sentences of imprisonment. Section 718.2(c) of the CC stipulates that when a court that imposes a sentence shall take into consideration of, amongst others, where consecutive sentences are imposed, the combined sentence should not be unduly long or harsh.
[57] A breakdown of sanctions for third-party ML cases and against legal persons is not available.

Immediate Outcome 8 (Confiscation)

148. Since its last assessment, Canada improved its ability to collect information on seizures and confiscations and produce related statistics. It uses both criminal and civil (non-criminal based) proceedings to confiscate proceeds and property related to an unlawful activity. At the Federal level, there is an agency to manage seized and confiscated assets (SPMD). At the provincial level, the management of these assets rests with the prosecution services. Canada also confiscates with no terms of release any undeclared currency and monetary instruments from travellers entering and exiting the country when there is reasonable grounds to suspect they are from illicit origin or that the funds are intended for use in the financing of terrorist activities. It shares confiscated assets with countries with which it has a sharing agreement.

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

149. While confiscation of criminal proceeds and instrumentalities is a policy objective, that objective is pursued to some extent only. Canada is not able to confiscate property of equivalent value; instead, it imposes fines in lieu. As a result of the deficiencies described in IO.7 confiscation relate mainly to proceeds of criminal activities and offence related property conducted by OCGs, in particular drug offenses, fraud, theft, and to the proceeds of tax evasion.

150. Canada's Integrated Proceeds of Crime (IPOC) Initiative aims at the disruption, dismantling, and incapacitation of OCGs by targeting their illicit proceeds and assets. It brings together the CBSA, CRA, PPSC, Public Safety Canada, PSPC (more specifically, its Forensic Accounting Management Group, and the Seized Property Management Directorate), and the RCMP, which cooperate and share information to facilitate investigations. According to the authorities, the IPOC is a distinct program and a corner stone of the AML/CFT regime as a whole as modified in 2000. However, it is not identified as one of the key goals of the latest articulation of the AML/CFT program.

151. The RCMP's Federal Policing Serious and Organized Crime/Financial Crime Teams (which investigate ML cases) target the proceeds of organized crime for seizure. The return of frozen or seized POC and instrumentalities to the defendant is avoided in the context of a plea bargain; in line with the PPSC policy, both POC and instrumentalities must be sought.[58] According to the authorities, the accused normally agree with the confiscation request when they plead guilty. At the provincial level, measures aimed at tracing and seizing assets in view of confiscation are in some cases conducted jointly by the RCMP and the provincial LEA. In the province of Quebec, for instance, the cooperation between the RCMP and the relevant provincial police, i.e. the *Sûreté du Québec*, has shown a number of cases of successful recovery of assets. At the municipal level, the Service de Police of the City of Montreal has a unit specialized in the recovery of POC and in the investigation of ML (*Unité des produits de la criminalité*—Programme UPC-ACCEF). The priority of the investigations in Quebec and in Montreal in particular is clearly to identify assets for confiscation, especially in

[58] According to the PPSC Deskbook, Guideline issued by the Director under Section 3(3)(c) of the Director of Public Prosecutions Act, Chapter 5.3 Proceeds of Crime, in the context of ORP, "partial forfeiture is not a negotiation tool. If the facts justify and application for total forfeiture, Crown counsel may not, as part of negotiations, suggest partial forfeiture."

cases involving OCGs. These clear priorities and effective specialized units have resulted in greater recovery of POC and instrumentalities by criminal law means both in scope and in type of assets, including in more complex ML cases. Other provinces rely more on non-conviction based forfeiture, where roughly CAD 100 million have been confiscated, nationally, during the relevant period.

152. As a general rule, however, LEAs in other provinces and at the federal level do not seem to adopt a "follow the money" approach in practice, nor to initiate a parallel financial investigation, notably because of resource constraints. Overall, as a result of the shortcomings explained under IO.6 and IO.7, asset recovery is pursued to a limited extent only.

Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad

153. The total amounts recovered yearly have increased significantly since the previous assessment,[59] but, nevertheless, appear to be low in the Canadian context (see table below). This is likely to be due to the lack of focus on asset recovery mentioned above and the shortcomings mentioned in IO.6 and IO.7, as well as the length of time needed to bring cases to closure: The delays encountered (especially at the tracing stage) are likely to encourage and facilitate the flight of assets.

Table 13. **Amounts Forfeited in Canada**[1]
(in Canadian Dollars)

	Criminal Federal Forfeiture	Federal Fines in Lieu	CBSA Cash Forfeitures	Civil Forfeiture Results (Nationally)	Québec Criminal Provincial Forfeiture	Total
2009/10	46 368 327	101 600	5 277 676	7 600 000	---	59 347 604
2010/11	58 872 881	71 650	4 698 404	12 400 000	9 070 456	85 113 392
2011/12	77 698 566	31 700	1 960 038	18 900 000	10 905 959	109 496 264
2012/13	83 935 230	105 939	3 468 888	41 700 000	11 498 811	140 708 870
2013/14	75 997 602	312 178	4 054 089	18 900 000	12 453 244	111 717 114
2014/15	72 869 240	314 217	4 076 586	---	---	77 260 044
Total In CAD	415 741 848	937 285	23 535 683	99 500 000	43 928 471	583 643 289

The table is a consolidation of statistics maintained by different authorities, using different criteria and does not include forfeitures undertaken by federal departments that do not involve or are not reported to the SPMD. At the provincial level, figures were provided for Quebec only (federal criminal results for Quebec appear in the first column). They do not differentiate domestic from foreign predicate offenses (though IO.2 shows that there have been forfeitures based on the direct enforcement of foreign orders) and proceeds which have moved to other countries. According to the authorities, the link between seized and forfeited assets cannot easily be made, as these actions occur over multiple years.

154. Different types of assets are seized or restrained in federal criminal proceedings (see table below) but, overall, Canada does not restrain businesses, company shares—despite the high risk of misuse of legal entities—or property rights. [60] In general, Canadian authorities seem to be managing

[59] An average of Can$ 27 million a year were forfeited from 2000 to 2007 (2008 MER, page 62).
[60] The only exception appears to be a golf course seized on behalf of another country.

effectively the seized and confiscated assets on both federal and provincial levels. Assets are generally not sold before the conclusion of the criminal proceeding to maintain their value or reduce the costs of management of the property, unless they are rapidly depreciating or perishable, or the accused authorizes their disposal.

Table 14. **Federally Seized/Restrained Assets by Appraisal Value**
(in Canadian Dollars)

Asset Type	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015
Aircraft	108 000	-	15 000	-	250 000	0
Cash	20 878 443	21 456 803	22 665 264	28 833 075	18 036 703	21 680 932
Financial Instruments	365 247	961 557	5 938 052	732 443	26 924 056	723 834
Hydroponics	6 291	2 748	808	1 240	259	12
Other Property (incl. jewellery)	138 410	684 780	605 054	274 601	203 956	269 866
Real Estate	52 785 401	54 220 901	37 336 935	25 445 169	26 532 406	16 758 250
Vehicle	5 940 355	5 947 937	6 256 389	4 839 410	4 479 067	4 433 720
Vessel	311 200	156 101	79 296	121 661	39 700	518 000
Grand Total	**80 533 349**	**83 430 829**	**72 896 801**	**60 247 601**	**76 466 149**	**44 384 616**

155. Revenue agencies, both at the federal and provincial level, have been successful in recovering evaded taxes, including in instances where the monies were held offshore. In FY 2013/2014, Revenue Quebec alone recuperated over CAD 3.5 billion of evaded taxes, both by criminal sanctions and civil compliance actions. During the same period, FY 2013/2014 the CRA recuperated CAD 10.6 billion in its criminal and civil actions. As a result of the CRA's investigations into suspected cases of tax evasion, fraud and other serious violations of tax laws, and recommendations to the PPSC, Canada secured convictions for tax crimes for CAD 162.3 million and levied a total of CAD 70.7 million in criminal fines. However, it should be noted that these figures do not solely represent confiscations related to the proceeds of crime, and that the Canadian authorities were unable to provide such separate figures.

156. Between 2008 and 2015, in an effort to recover proceeds that have been moved to other countries, Canada sent 135 requests for tracing assets (bank or real estate records) to other countries 43 requests for restraint of funds or assets and 4 requests for forfeiture. Discussions with the authorities and the cases provided nevertheless established that the authorities pursue assets abroad to some extent only, notably because such actions require resources that are currently dedicated to other priorities. The fact that LEAs seem to have little expertise in pursuing complex international ML schemes or in the investigation of professional money launderers also explain the relatively low level of effort in seeking the recovery of assets abroad. Considering that there is no possibility for the authorities to seize property of equivalent value, when POC cannot be forfeited, fines in lieu are ordered, in addition to the custodial sentence. The total fines collected by the federal Crown are CAD 937 285.95 for 2009-2015. The authorities share parts of the confiscated assets with

their foreign counterparts, both in criminal and civil actions, when the property is in Canada, the foreign country assisted Canada in the case and there is a signed sharing agreement. This would be the case when the offense was committed partly or entirely abroad and laundered in Canada.[61] The major part of the sharing occurred with the US, which appears justified in the Canadian context, and property was also shared with Cuba and the UK.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

157. CBSA agents seize monies when there is a suspicion that the latter are POC or funds intended to be used to fund terrorism. As indicated in the table below, between 2009 and 2015, Canada seized about CAD 263 million at the border, of which less than 9% were confiscated and more than 91% were returned to the travellers. In the latter cases, according to the authorities, there was no suspicion of ML, TF, or other illicit activities; therefore, the monies were returned to the traveller and an administrative fixed fine (of CAD 250, CAD 2 500, or CAD 5 000) levied. In practice, however, falsely or undeclared cross-border movements of currency and other bearer negotiable instruments are analysed by the FIU, or investigated by the RCMP to a very limited extent, namely only when they pertain to an ongoing analysis or investigation (See IO.6). Moreover, the level of the sanctions for noncompliance with the obligation of disclosure of cross-border movements and the frequency which it is applied does not seem effective, proportionate nor dissuasive.

(in Canadian Dollars)

FY	Seized Amount	Returned at Seizure by CBSA	Final Penalty Amount Forfeited	Cash Seizures Forfeited	Amount Returned by SPMD[1]
2009/2010	99 430 742	94 448 985	2 150 500	5 277 676	731 782
2010/2011	12 447 605	6 277 108	223 000	4 698.404	1 458 233
2011/2012	4 361 463	1 871 650	50 750	1 960 038	522 035
2012/2013	28 273 318	23 949 256	545 500	3 468 888	853 173
2013/2014	52 508 920	47 564 857	1 340 000	4 054 089	873 782
2014/2015	65 989 388	61 808 579	1 732 000	4 076 586	1 328 046
Total	263 011 436	235 920 435	6 041 750	23 535 681	5 767 054

1. This column contains only the amounts for closed cases where an appeal or other legal means of challenging are no longer available to the travellers.

[61] Canada shared the following amounts: 2007/2008: CAD 199 390; 2008/2009: CAD 75 620; 2009/2010: CAD 357 844; 2010/2011: CAD 0; 2011/2012: CAD 93 013; 2012/2013: CAD 237 577; 2013/2014: CAD 244 846.

Consistency of confiscation results with ML/TF risks and national AML/CTF policies and priorities.

158. Law enforcement actions, including asset recovery efforts focus mostly on illicit drug trafficking, fraud, and theft.[62] While drug-related offense and fraud are identified as very high ML threats in Canada's NRA, theft is not. In addition, the recovery of proceeds of other very high threats identified in the NRA is pursued, but not to the same extent (this is notably the case for proceeds of corruption and bribery, third-party ML, and tobacco smuggling, although some success was achieved in a case of tax evasion perpetrated from 1991 to 1996 in relation to a large scale tobacco smuggling operation[63]).[64] As a result, Canada's confiscation results are not entirely consistent with ML/TF risks or national AML/CFT policy.

Overall Conclusions on Immediate Outcome 8

159. **Canada has achieved a moderate level of effectiveness in Immediate Outcome 8.**

[62] As stated in the Research Brief-Review of Money Laundering Court Cases provided by FINTRAC, p. 1 and the Authorities Submissions to IO.7, p. 12 and 13. This is consistent with the assessor's findings after the interviews with Canadian authorities during the on-site.
[63] Project Oiler, where charges of tax fraud (through smuggling) and the possession of proceeds of crime were laid in 2003 and ultimately a plea of guilty accepted for violations of the Excise Tax Act in 2008 and 2010. This case resulted in the imposition of criminal fines and penalties totalling CAD 1.7 billion.
[64] The authorities provided the assessment team with a table showing the seizures in relation to the offenses (Seizures by Act), from 2009 until 2015. The higher values are related to the Controlled Drug and Substance Act, followed by the offense of Possession of property obtained by crime, laundering of proceeds, PCMLTFA, tax offenses and conspiracy. The values seized in relation to bribery of officers are insignificant (except in one case where some CAD 4 million were confiscated). It is not possible to identify third-party ML in the statistics provided. Seizures for possession of tobacco appear only in fiscal years 2012/2013 and 2013/2014, and seizure for bribery of officers appear only in FY 2010/2011, 2011/2012 and 2013/2014. In FY 2009/2010, 2012/2013 and 2014/2015 the value of seizures in relation to bribery is zero.

3

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

IO.9

The authorities display a good understanding of TF risks and close cooperation in CFT efforts. The intelligence services, LEAs and FINTRAC regularly exchange information, which notably contributes to support prioritization of TF investigations.

Canada accords priority to pursuing terrorism and TF, with TF investigation being one of the key components of its counter-terrorism strategy.

The RCMP duly investigates the financial components of all terrorism-related incidents, considers prosecution in all cases and the prosecution services proceed with charges when there is sufficient evidence and it serves the public interest. Two TF convictions were secured since 2009. Sanctions imposed were proportionate and dissuasive.

Canada also makes frequent use of other measures to disrupt TF.

IO.10

Implementation of TF-related targeted financial sanctions (TFS) is quite effective for FIs but not for DNFBPs.

Canada takes a RBA to mitigate the misuse of NPOs (i.e. charities). A specialized division within CRA-Charities focuses specifically on concerns of misuse of organizations identified as being at greatest risk. In addition, CRA-Charities has developed an enhanced outreach plan, which reflects the best practices put forward by the FATF.

In practice, few assets have been frozen in connection with TF-related TFS.

IO.11

Canada's Iran and DPRK sanction regimes are very comprehensive and in some respects go beyond the UN designations.

Cooperation between relevant agencies is effective and some success has been achieved in identifying and freezing the funds and other assets belonging to designated individuals.

Large FIs have a good understanding of their TFS obligations and implement adequate screening measures but some limit their screening to customers only. DNFBPs, however, are not sufficiently aware of their obligations and have not implemented TFS.

There is no formal monitoring mechanism in place; while some monitoring does occur in practice, it is limited to FRFIs and is not accompanied by sanctioning powers in cases of non-compliance.

4

Recommended Actions

Canada should:

IO.9

- Pursue more and different types of TF prosecutions.

IO.10

- Require DNFBPs to conduct a full search of their customer databases on a regular basis.
- Consider increasing the instances of proactive notification of changes to the lists to REs other than FRFIs.
- Consider enhancing the number of seizures and confiscations related to TF offenses.

IO.11

- Monitor and ensure FIs' and DNFBPs' compliance with PF-related obligations.
- Conduct greater outreach. This should include information on the PF-risk that can be published without compromising Canada's security, as well as more detailed guidance on the implementation of TFS and indicators of potential PF activity.

The relevant Immediate Outcomes considered and assessed in this chapter are IO9-11. The recommendations relevant for the assessment of effectiveness under this section are R.5-8.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

160. The RCMP investigates all occurrences of TF. This includes investigations into a wide range of TF activities, such as the collection of funds and their movement and use by individual, entities or wider organizations. The RCMP lays TF charges when approved by PPSC based on sufficient evidence and when the prosecution would best serve the public interest. Between 2010 and 2015, charges were laid against one individual, resulting in a conviction for TF in 2010 (see Box 7 below). Charges were also laid in another case, but subsequently withdrawn for tactical and operational enforcement reasons.

Box 7. **R v. THAMBITHURAI 2008**

It came to the knowledge of the RCMP's Integrated Security Enforcement Team (INSET) that a man was in the process of collecting funds from his place of residence and businesses for the Liberation Tigers of Tamil Eelam (LTTE), a listed terrorist entity in Canada. The person was arrested in Vancouver. INSET found various materials in his possession, including donation forms for the LTTE which were used for a CAD 600 donation and a CAD 300 pledge. The accused was charged with four counts of "Providing or making available property for a terrorist organization" under CC 83.03, three of which were later withdrawn. He pled guilty in 2010 and was sentenced to six months of imprisonment.

161. LEAs actively pursue the threat of individuals radicalized to violence, and in particular, those seeking to travel abroad for terrorist purposes. The RCMP's priority is to pursue charges that are in the best interest of public safety, and to mitigate the possible threat of terrorist activity as efficiently as possible. TF charges are not always determined to be the most appropriate means to mitigate threat. In these instances, alternative measures are used. The below case showed that while a boy obtained funds by robbery for travel abroad to join a terrorist organization, RCMP had pursued terrorism and criminal charges instead of TF charges.

Box 8. **Young Foreign Terrorist Fighter**

In 2014, a 15-year-old boy who had become radicalized to violence became determined to travel abroad to join a terrorist organization. He had previously tried unsuccessfully to purchase an airline ticket for Syria with his father's credit card. In October 2014, the father discovered CAD 870, a knife, and a balaclava in the boy's backpack. Feeling suspicious of money might have been stolen, the father made a report to police. Investigation revealed that the boy had committed an armed robbery in order to purchase ticket for Syria. The boy was charged and convicted of armed robbery. Additional national security investigation by C-INSET resulted in the youth being convicted of attempting to leave Canada to participate in the activity of a terrorist group (CC 83.131) and commission of an offense for a terrorist group (83.2). He was sentenced to 24 months in youth custody plus one-year probation, consecutive to the sentence of armed robbery.

162. This and other cases discussed establish the authorities' ability to pursue TF activities. However the results obtained so far are not entirely commensurate with Canada's risk profile, which, as assessed in the NRA, points to more frequent and diverse TF occurrences. As a result, Canada has demonstrated to some extent that it pursues the different types of TF activities that it faces.

TF identification and investigation

163. The RCMP investigates the financial component of all terrorism-related incidents. It employs various avenues to identify and investigate potential TF activities including human source

or intelligence, referrals from international or domestic partners (e.g. the US Federal Bureau of Investigations (FBI), FINTRAC, CRA, and CSIS, direct reporting from Canadian FIs), and national security investigations.

164. FINTRAC regularly provides proactive disclosures and responses to VIRs on TF cases, which supports the prioritization of TF investigations. It mostly disseminates disclosures related to TF to CSIS, but also to the RCMP, CBSA, CRA, municipal and provincial police, and foreign FIUs. According to FINTRAC, roughly half of TF disclosures were proactive, and half in response to VIRs. The authorities do not keep figures on the results of TF investigations arising from proactive disclosures.

Table 15. **TF-Related VIRs and FINTRAC Disclosures (from and to RCMP only)**

	2010-11	2011-12	2012-13	2013-14	2014-15	Total
Number of TF Disclosures	100	110	125	188	206	729
Number of TF-Related VIRs	26	65	78	84	61	314

165. LEAs and FINTRAC accord priority to TF investigations, although there are exceptions where priority would be accorded to other terrorism files, as highlighted in the Project Investigation below. In urgent cases, FINTRAC provides TF-related financial intelligence to the RCMP within hours. In normal circumstances, it may take days or weeks to respond to the VIRs. In one of the cases provided, which dated back more than 10 years, timely intelligence from FINTRAC was instrumental in identifying domestic and foreign accounts, as well as in establishing the foundations for the necessary judicial authorization applications.[65] The CBSA also assists in the identification of an investigation into TF activities.

166. For example in the case of Project Investigation, a person was intercepted by the CBSA at a Canadian airport for carrying undeclared currency in excess of CAD 10 000. CBSA notified the RCMP, which assumed control of the investigation because of the nexus to TF. The investigation revealed that funds destined to a foreign country to support an organization listed by Canada as a terrorist entity had been collected across Canada by multiple individuals. Information received from FINTRAC resulted in the identification of the funding networks of the entity and of its key members. Due to operational and resource constraints imposed by higher priority national security investigations, the RCMP was unable to proceed further with the file. A different approach was therefore adopted: the suspect was charged under PCMLTFA for not reporting the importation or exportation of currency

[65] The case in question was the Project Saluki: In 2002, the RCMP conducted a TF investigation to determine whether monies were being raised in Canada by a front organization, the World Tamil Movement (WTM), for the LTTE in Sri Lanka. Financial Intelligence provided by FINTRAC and banking records from FIs obtained by a court order indicated that funds were being sent from a bank account in Canada to a bank account in a foreign country registered to a legal entity. With the assistance of the foreign country, the RCMP gathered the bank documents of the foreign account and identified the holders and the persons associated with or who maintained control over the account, which involved a private deed of trust as well as a list of the appointed trustees. RCMP officers went to the foreign country, interviewed the trustees and signatories of the foreign bank account and determined details of their involvement and position with the legal entity. No person was charged upon the conclusion of the investigation. The PPSC applied for civil forfeiture and in 2010 the Court ordered forfeiture of the WTM building in Montreal and other property under terrorism legislation.

or monetary instruments. He pleaded guilty and was fined CAD 5 000, and the funds previously seized were forfeited to the Crown.

167. All TF investigations are conducted by the RCMP's INSET field units. These units are located in Vancouver, Edmonton, Calgary, Toronto, Ottawa, and Montreal, and are comprised of officers deployed from other partners (including municipal and provincial LEAs and the CSIS) in numbers that fluctuate depending on operational needs. They are tasked by FPCO, which it is responsible for the prioritization of investigations. TF activities are investigated in proportion with their scope and complexity. As investigations become more complex and require more resources, the RCMP uses a management tool to ensure that investigations align with national security priorities. Between 2009 and 2013, it identified five investigations as major TF cases, which led to two charges being laid (see previous core issue).

Table 16. **TF Investigations**

	2010	2011	2012	2013	2014	Total
Assistance Files[1]	235	162	117	201	179	**894**
Participate/Contribute to Terrorist Group Activity	40	29	33	45	52	**199**
Provide/Collect Property for Terrorist Activity	31	26	17	21	9	**104**
Information Files[2]	30	31	15	25	34	**135**
Crime Prevention3	0	2	1	2	79	**84**
Facilitate Terrorist Activity	15	3	6	10	15	**49**
Make Available Property/Service for Terrorist Act	10	15	8	5	8	**46**
Suspicious Person/Vehicle/Property	0	1	6	9	2	**18**
Use/Possess Property for Terrorist Activity	4	1	2	1	0	**8**
National Security Survey Codes[4]	1	1	0	4	0	**6**
Instruct/Commit Act for Terrorist Group	2	3	0	1	3	**9**
Others (Criminal Intelligence, Fraud, etc.)	5	3	6	5	4	**23**
Total	**373**	**277**	**211**	**329**	**385**	**1 575**

1. An Assistance file is created when assisting domestic or foreign non-PROS/SPROS units or agencies.
2. Information File is information received, it is not a call for service, or the person or agency supplying the information does not expect police action.
3. Crime Prevention are activities directed toward the tangible objective of preventing a specific type of crime, e.g. breaking and entry, approved or accepted community-based policing program such as Drug Abuse Resistance Education (DARE).
4. National Security Survey Codes are the combined collection of two different survey types: Threat Assessments and VIP/Major Events.

TF investigation integrated with -and supportive of- national strategies

168. CFT is an integral part of Canada's strategy to combat terrorism. The RCMP confirms that it assesses the existence of a TF component in every national security investigation. Cases provided (including IRFAN-CANADA described in IO.10) showed that the authorities use TF investigations to identify the structures, key persons, and activities of terrorist organizations. TF investigations are integrated with, and used to support, national counter-terrorism strategies and investigations.

Effectiveness, proportionality and dissuasiveness of sanctions

169. Canada successfully pursued and convicted two individuals on TF charges. The first case (*R v. THAMBITHURAI* described above) only attracted a six-month imprisonment despite PPSC appealing against the sentence. In the second case (*R v. KHAWAJA*, see Box 9 below), the Court sentenced the defendant to two years imprisonment for TF and to life imprisonment for "developing a device to activate a detonator."

Box 9. **R v. KHAWAJA**

In 2004, Canada initiated an investigation into a Canadian citizen linked to a terrorist group under investigation in the United Kingdom (UK) for planning a fertilizer bomb attack targeting pubs, nightclubs, trains and utility (gas, water and electric) supply stations in the UK. The evidence collected indicated that the Canadian subject attended a training camp in Pakistan in July 2003 and transferred on three occasions a total of about CAD 6 800 to his associates in the UK with the help of a young woman to avoid suspicion of link. His parents were persuaded to evict tenants from their residence in Pakistan so that the subject may make the facility available for use by the group's members. He also planned 30 devices to strap explosives onto model airplanes with remote triggers. He was arrested by the RCMP in 2004, detained, and charged in 2008 with seven counts of offenses under the CC, including one count of TF under 83.03(a). MLA requests were sent to the US authorities for the subject's Internet Service Provider and payment records as well as the testimony of a US witness. In December 2010, upon the appeal by the PPSC, the subject was sentenced to life imprisonment for "developing a device to activate a detonator" and 24 years of imprisonment for the other offenses, including two years' imprisonment for TF.

170. While low, the number of instances prosecuted appears in line with Canada's threat profile and considering the alternative mitigating measures taken (see below). Sanctions applied appear to be proportionate with the amounts involved and dissuasive. No legal person has been convicted of TF offenses. No designations were made to the relevant UN bodies but Canada has been co-sponsor to a number of designations.

Alternative measures used where TF conviction is not possible (e.g. disruption)

171. Canada's primary goal in counter terrorism efforts is to maintain public safety, and Canada places a strong focus on disrupting terrorist organizations and terrorist acts before they occur. The RCMP defines disruption in national security matters as the interruption, suspension or elimination, through law enforcement actions of the ability of a group(s) and/or individual(s) to carry out terrorist or other criminal activity that may pose a threat to national security, in Canada or abroad. It includes disruption of TF activities

172. During national security investigations, activities of participants and peripheral participants may be tactically disrupted for a variety of reasons, including triggering reactions or behavioural changes of the main targets. TF investigations therefore do not always result in TF

charges, if other charges for terrorism or other offenses are being laid and the evidence is most cogent and appropriate or would best serve the public interest. The authorities shared several cases (including Project Smooth below) where despite clear evidence to substantiate a TF charge, other means were preferable to ensure the public interest.

Box 10. **Project SMOOTH**

In August 2012, CSIS reported to RCMP that a male ("CE") residing in Montreal had met another male ("RJ") in Toronto. RJ was known to the RCMP for recently distributing pro Al-Qaeda propaganda. Investigation, including the use of an undercover US FBI agent who had gained the trust of CE and RJ, revealed that the two men had plotted to cut a hole in a railway bridge to derail the Canadian Via Rail passenger train between Toronto and New York. The FBI agent had surreptitiously recorded their conversations, which made up the bulk of the case's evidence, including CE's description on the hierarchical structure and mode of communication of a terrorist group and that CE was receiving orders from Al Qaeda through a middleman. It was also unveiled during the investigation that CE had or intended to finance a total of CAD 4 200 to the terrorist group. In 2013, CE and RJ were arrested. CE and RJ were both charged with four offenses: conspiring to damage transportation property with intent to endanger safety for a terrorist organization, conspiring to commit murder for a terrorist group, plus two counts of participating or contributing to a terrorist. CE was found guilty of all four charges plus another he faced alone for participating in a terrorist group. RJ was convicted of all charges except that of "conspiring to damage transportation property with intent to endanger safety for a terrorist organization." In March 2015, both men were sentenced to life imprisonment.

173. In other cases, TF prosecutions were not possible, especially in cases based largely on intelligence that may fall short of the evidentiary threshold required by criminal courts. In instances where prosecution is not deemed to be the best avenue to protect the public or human sources, or is not possible, a wide-range of disruption techniques is employed. Such techniques typically include: arrests; search-and-seizure raids; "intrusive surveillance" (in which police make it obvious to the suspects that they are being watched); civil forfeiture; inclusion of specific persons in Canada's no fly list (which is particularly relevant considering the growing threat of foreign fighters); revocation of the charitable status of NPOs identified as having been used for TF purposes; listing of terrorist entity under the CC, barring of individuals who pose a threat to the security of Canada and prohibition from entering or obtaining status in Canada or from obtaining access to sensitive sites, government assets or information; and extradition. Canada frequently uses other criminal justice and administrative measures to disrupt TF activities when a prosecution for TF is not practicable.

Overall Conclusions on Immediate Outcome 9

174. **Canada has achieved a substantial level of effectiveness for IO.9**.

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

175. Canada implements UNSCR 1267 and UNSCR 1373 (and their successor resolutions) through three separate domestic listing mechanisms: the United Nations Al-Qaeda and Taliban Regulations (UNAQTR); the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST); and the CC. Canada plays an active role in co-sponsoring the listing of new terrorist entities, as appropriate, and delisting defunct entities. The lists of entities whose assets are to be frozen under UNSCR 1267 and its successor resolutions are automatically incorporated into Canadian law by reference through UNAQTR. Accordingly, UNSC decisions to list or delist an individual are given immediate effect in Canada; no additional action by Canadian authorities is needed to give legal effect to a designation. These decisions are rapidly brought to the attention of FRFIs, but not of other REs.

176. The CC is Canada's primary listing mechanism, and allows it to satisfy the obligations under UNSCR 1373. While the RIUNRST also satisfies UNSCR 1373, no listings have been added to the RIUNRST since 2006. In practice, this CC process entails a criminal intelligence report prepared by the RCMP or a security intelligence report prepared by the CSIS, which is subjected to a legal review by independent counsel to ensure that it meets the CC listing threshold (i.e. reasonable grounds to believe), as well as interdepartmental consultations. The authorities can list an entity to Canada's domestic list (under the CC) in an expedited manner if necessary.[66] The Canadian authorities provided a concrete example (IRFAN Canada, below) of the domestic listing of a NPO.

Box 11. **IRFAN-Canada**

In 2010, CRA-Charities suspended the receipting privileges of IRFAN-Canada. The suspension was based on the organization's failure to provide and maintain records, which interfered with CRA-Charities' ability to carry out the audit that began in 2009. CRA-Charities continued with the audit during the period of suspension and ultimately revoked IRFAN-Canada's charitable registration in 2011. It shared information regarding IRFAN-Canada's possible association with the listed organization, Hamas, with partner organizations, including the RCMP. A CRA-Charities analyst seconded to the RCMP was able to provide expertise to facilitate the sharing of information, as authorized by legislation. The RCMP collaborated with and received financial intelligence from FINTRAC.

In 2014, the RCMP officially opened the investigation, which resulted in an RCMP recommendation to PS Canada to have IRFAN-Canada listed as a terrorist organization. The financial intelligence provided by FINTRAC also served to inform deliberations on the listing of IRFAN. The RCMP, PS Canada, and the DOJ worked together to prepare the documentation required for the Government to make a decision as to the listing. In April 2014, IRFAN-Canada was listed as a terrorist entity by the Government of Canada. Following the listing, criminal investigations were initiated by the RCMP's INSETs in Ontario and Quebec, and were still ongoing at the time the assessment.

[66] Several factors may be considered, as for example: operational imperative to list more quickly to freeze known assets; nexus to Canada; national security concerns; allied concerns, etc.

177. Third-party requests from foreign jurisdictions are considered under the CC framework. Canada has received numerous requests from foreign jurisdictions since the establishment of the regime and has given effect to both formal and informal requests, though it does not keep records on the number of third-party requests for listing under the CC. The authorities also indicated that they were able to list an entity on an expedited manner when necessary, following third-party requests.

178. As of 7 April 2015, 54 entities were listed pursuant to the CC and 36 terrorist entities under the RIUNRST. Once an entity has been listed, PS issues a news release advising of the new listing and provides a notification on its sanctions website, and the listings are published in the Canada Gazette, approximately two weeks after listing. To assist FIs search their list of customers against these listed terrorist names, OSFI maintains on its website a database of all terrorist names (and known identifiers) subject to Canadian laws, and notifies FIs without delay by posting instantly a notification to its website and by notifying all its e-mail subscribers each time a new terrorist name is listed under Canadian law, or there are changes to existing information. FRFIs are also required to report to OSFI monthly that they have conducted the name screening and report any terrorist property that they have identified and frozen. FINTRAC also provides a link to OSFI's website on its own website, as well as guidance to REs on the reporting requirements related to terrorist property. Other than in the case of OSFI, the mechanism for informing the private sector about listed entities appears to be rather passive, as it relies on REs consulting the Official Gazette and the websites of the competent authorities and/or, when they are aware of this possibility, subscribing to RSS feeds (or the UN notification system).

179. The FRFIs met during the on-site had a good understanding of their screening obligation regarding targeted financial sanctions (TFS) and implemented sanctions without delay. DNFBPs, however, do not have a good understanding of their obligations (see IO.4). Furthermore, while they are required to check the listings at the beginning of a business relationship, they are not required to conduct a full search of their customer databases on a regular basis, which is a major limitation to an effective implementation of TFS.

180. Persons listed in Canada may apply for revocation of the designation under the framework detailed in R.6.[67] Examples of delisting were shared with the assessors. One entity was delisted in December 2012.

181. Canada has not proposed a designation to the UN Sanctions Committees, but acted as co-sponsor on several occasions.

Targeted approach, outreach and oversight of at-risk non-profit organisations

182. The Canadian NRA concluded that registered charities present a high risk of TF, due to the fact that a large number of the financial transactions that charities conduct may be performed via delivery channels with a high degree of anonymity and some level of complexity (i.e. multiple

[67] Under the Criminal Code regime, there are several ways an entity could be delisted. The Minister of Public Safety and Emergency Preparedness can recommend to the Governor in Council that an entity be delisted at any time, the entity could be recommended for delisting as part of the two-year review, or an entity can apply for delisting as per the process outlined under section 83.05(2).

intermediaries are involved). The NRA also highlights that the significant use of cash may make it difficult for the authorities to establish the original source of funds, and that it may be difficult to know how the funds or resources will be used once transferred to partner organizations or third parties.

183. Canada has implemented a targeted approach regarding the NPO sector vulnerability to TF. In 2015, the CRA, which regulates charities under the Income Tax Act, conducted a review in addition to the NRA, to examine the size, scope and composition of the NPO sector in Canada and to determine which organizations, by virtue of their activities and characteristics, were at greater risk of being abused for terrorist support purposes. The CRA found that, in Canada, the organizations at greatest risk of terrorist abuse because of the nature of their activities and characteristics are charities. As a result, the authorities concluded that, in the Canadian context, NPOs that fall within the FATF definition are charities. Four reports had previously been published regarding the sector, notably a "Non-profit Organisation Risk identification project" in 2009. Canada has a large NPO sector, comprising of approximately 180 000 organizations. The sector can be divided into two groups: charities and NPOs, depending on their legal structures. While both are exempt from paying taxes, federally registered charities (of which there are approximately 86 000) receive additional fiscal privileges and submit annual information returns, which include notably the names of the directors or trustee, a description of its activity and financial information, including sources of funding. Non-charity NPOs (of which there are approximately 94 000) having assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000 are not required to register, but must file an annual NPO Information Return with the CRA.[68] In addition, non-charity NPOs incorporated provincially or federally would be required to file certain information with the provincial or federal governments on an annual basis depending on the statute under which the organization is formed. This typically includes information related to address, directors, and the date of the last general meeting. In certain cases, organizations may have to provide detailed financial information depending on value of assets or fund received.

184. CRA-Charities reviews all applications for charitable registration and conducts audits of registered charities. From 2008–2014, CRA-Charities completed approximately 5 000 audits in total; 16 these audits comprised a national security concern, eight of which resulted in revocation of registration.[69] If an applicant charity does not meet the requirements of registration, e.g. due to terrorism concerns, the CRA denies its application.[70] Through its work, CRA-Charities may take administrative action to disrupt an organization's activities where it has identified a risk of terrorist abuse, and/or relay the information to LEAs. If a registered charity no longer complies with the requirements of registration, for any reason including connections to terrorism, the division can

[68] The annual NPO Information Return includes information about their activities, assets and liabilities.
[69] Two led to penalties totalling CAD 440 000; four led to compliance agreements with the charity involved and two resulted in education letters.
[70] The Income Tax Act requires that charities devote their resources to charitable purposes and activities. An organization that supports terrorism would be denied registration for carrying on activities contrary to public policy, which would not qualify as charitable. Additionally, the Charities Registration (Security Information) Act provides a prudent reserve power to deny or revoke registration when terrorist connections are suspected.

apply a range of regulatory interventions and, in the most the serious cases, may revoke the registration.

185. CRA-Charities conducts outreach to advise charities of their legislative requirements and how to protect themselves from terrorist abuse. This includes general guidance on topics related to sound internal governance, accountability procedures, and transparent reporting, as well as specific tools such as a checklist on avoiding terrorism abuse and a web page on operating in the international context. CRA-Charities will build on this existing outreach through its enhanced outreach plan. CRA-Charities has begun consultations with the sector to educate them on the risk of terrorist abuse and to gain a better understanding of their needs in terms of outreach and guidance.

186. National coordination has been enhanced. The CRA shares information with relevant partners where there are concerns that a charity is engaged in providing support to terrorism. If the division encounters information that is relevant to a terrorism investigation when carrying out its regulatory duties, it shares that information with national security partners and LEAs. The division shared information with domestic national security partners in support of their mandate in 47 cases. Similarly, the division received information from partners in 51 cases to assist with its analysis, in 2014/2015. In addition, to facilitate the sharing of information, a secondment program between the CRA and its partners has been instituted: CRA employees are seconded to the partner agencies and employees from the partner agencies are seconded to the CRA.

187. According to the CRA's NPO Sector Review of 2015 the 86 000 registered charities represent 68% of all revenues of the NPO sector and nearly 96% of all donations (see R.8). CRA registered charities also account for a substantial share of the sector's foreign activities as about 75% of internationally operating NPOs are registered as charities. In addition, as detailed above, all registered charities, regardless of the value of their assets, and all NPOs with assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000 must file an annual information return with the CRA, which includes the provision of financial information. In addition, registered charities with revenue in excess of CAD 100 000, and/or property used for charitable activities over CAD 25 000, and/or that have sought permission to accumulate funds, must provide more detailed financial information. The authorities identify charities as being the organizations falling under the FATF definition of NPOs and reviewed the NPO's sector (see Box 12).

Box 12. **Canadian NPO's Sector Review**

The national regulator of registered charities, i.e. the CRA, conducted a domestic review of the entire NPO sector in Canada in order to identify which organizations, by virtue of their activities and characteristics, were at greater risk of being abused for terrorist support purposes. The review aimed to ensure that Canada (i) is not taking an overly broad interpretation of the FATF definition of NPO, (ii) focuses on those organizations that are at greatest risk, and (iii) does not burden organizations that not at risk with onerous reporting requirements for TF purposes.

The CRA reviewed existing publications and research by governmental, academic, and non-profit organizations related to the non-profit sector, including reports by Statistics Canada on non-profit institutes, consultations on regulations affecting the sector, and studies on trends in charitable

giving and volunteering. In addition, it looked at existing laws and reporting requirements affecting NPOs. To determine where there is risk, NPOs were categorized based on shared characteristics such as purpose, activities, size and location of operation. The CRA compared those characteristics with the elements of the FATF definition of NPO. It also took into consideration the findings of the FATF typologies report Risk of Terrorist Abuse in NPOs to identify features that put organizations a greater risk.

The CRA found that, in Canada, the organizations at greatest risk of terrorist abuse are charities. As a result, the authorities concluded that, in the Canadian context, only charities fall within the FATF definition of NPO. While organizations at greatest risk are charities, not all charities are at risk. The insight obtained from the sector review allowed Canada to focus on charities as the starting point for its NRA.

Source: FATF (2015), Best practices paper on combating the abuse of NPOs—October 2015.

188. The registered charity met during the assessment is large and has a number of international connections. It has a good understanding of its vulnerability to TF and has implemented adequate measures to mitigate that risk, without disrupting legitimate NPO activities.

Deprivation of TF assets and instrumentalities

189. As of February 2015, the total amount of frozen assets belonging to designated entities is CAD 131 235 in 12 bank accounts, CAD 29 200 in six life insurance policies, nine house insurance policies, and one automobile insurance policy, totalling CAD 3 248 612 frozen. The number of entities that had their assets frozen was not provided.

190. Despite the high number of TF occurrences (see IO.9), no assets and instrumentalities related to TF were seized or confiscated in circumstances other than designations. There are several reasonable explanations for this. LEAs indicated that, in several cases, no assets or instrumentalities were found. In others cases, the lack of confiscation can be due to the fact that TF investigations do not always result in TF charges and other means of disruption (see IO 9). The authorities also provided cases of TF investigations unrelated to the UN designations where the RCMP seized some assets and instrumentalities,[71] but did not proceed to seek their confiscation.

Consistency of measures with overall TF risk profile

191. While the terrorist threat has grown in the recent years, in particular in light of an increased number of Canadian nationals who have joined terrorist groups abroad,[72] not all terrorist entities identified have financing or support in Canada. In October 2014, Canada was victim of two

[71] The assets seized included over CAD 10 000 in cash, in one case, and tractor trailers in another.
[72] As stated by the Director of CSIS following his appearance at the Senate Committee on National Security and Defence, as of the end of 2015, the Government was aware of approximately 180 individuals with Canadian a nexus who were abroad and suspected of engaging in terrorism related activities. The Government was also aware of a further 60 extremist travellers who had returned to Canada.

terrorist attacks in Saint-Jean-sur-Richelieu and Ottawa, perpetrated by two Canadian citizens who intended to travel abroad for extremist purposes, but had been prevented from doing so. The TF investigation related to these events was still ongoing at the time of the assessment. In other instances, the authorities detected the transfer of suspected terrorist funds to international locations. These transfers had been conducted through a number of methods, including the use of MSBs, banks, and NPOs, as well as smuggling bulk cash across borders.

192. Canada has demonstrated to some extent only that it pursues the TF threat that it faces (see IO.9). The system suffers from inadequate implementation of UNSCRs by DNFBPs. Nevertheless, it must also be noted that, in some respect, Canada goes beyond the standard—this in particular the case with respect to the CC terrorist list, which Canada reviews every two years to ensure that the legal threshold for listing continues to be met for each entity listed.

Overall Conclusions on Immediate Outcome 10

193. **Canada has achieved a substantial level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

194. Canada's framework to implement the relevant UN CFP sanctions relies on three main components: (i) a prohibition to conduct financial transactions to Iran and the DPRK, with a few regulated exceptions, (ii) an obligation to freeze assets of designated persons; and (iii) an obligation to notify the competent authorities of any frozen assets.

195. Canada implemented the UNSCR 1737 and 1718 obligations, including part of the freezing obligations, by issuing within the UN-requested timeline two regulations dealing with Iran and the DPRK respectively. Both regulations impose freezing obligations that are generally comprehensive (see R.7). The lead agency for their implementation is GAC. Canada also went beyond the standard by imposing additional unilateral sanctions under the Special Economic Measures Act (SEMA). As a result of its Controlled Engagement Policy towards both countries, the Canadian Government does not engage in active trade promotion with Iran and the DPRK, and, with almost all commercial financial transactions between Canada and Iran prohibited, the volume of existing bilateral trade with both countries has dropped considerably. Canada also ensured that the exceptions to the general prohibition of conducting financial transactions[73] do not apply with respect to designated persons and entities.

196. Decisions taken by the UNSC under 1737 and 1718 take immediate effect in Canada. The current lists of designated persons and entities are published on the OSFI website. To facilitate the

[73] Examples of these exceptions include: non-commercial remittances to the DPRK; financial banking transactions of CAD 40 000 and under between family members in Canada and family members in Iran; and other transactions permitted on a case-by-case basis, at the discretion of the Minister of Global Affairs. In practice, exceptions have been granted mainly in the case of prospective Iranian immigrants for the purposes of immigration fees and related transactions.

implementation of the TFS, guidance is provided on the GAC and OSFI website.[74] In addition, OSFI notifies the FRFIs of any changes to the lists on the same day as the changes occur, or on the day that follows the receipt of the note verbale. It also reminds FRFIs on a monthly basis of their screening and freezing obligations, either per web post or per email. Its guidance requires FRFIs to search their records for designated names in two ways: (i) by screening new customers' names against the official lists at the time such customers are accepted; and (ii) by conducting a full search of all customers' databases "continuously," which the guidance defines as "weekly at a minimum." No other authorities provide notifications to other REs of changes made to the lists. As a result, while the legal obligations to implement PF-related TFS are the same across the range of REs, swift action is actively facilitated in the case of FRFIs only. REs may nevertheless subscribe to the RSS feeds on the GAC website, or to the UN notification system, in order to be notified of changes to the Iran and DPRK regulations.

Identification of assets and funds held by designated persons/entities and prohibitions

197. Canada has had some success in identifying funds and other assets of designated persons, and preventing these funds from being used, as indicated in the table below. Two of the larger banks, as well as one provincial FI and two life insurers have identified assets of designated persons, frozen those assets (where available), and reported the case to the RCMP, OSFI, and FINTRAC. The assets were detected through timely screening of the FIs' customers' (but not other parties such as the beneficial owner, despite OSFI's guidance in this respect) against the UN lists. While the freezing are occurrences are low, they nevertheless indicate that FIs and in particular D-SIBs are taking measures to prevent their potential misuse for PF activities. No information was provided on the timing of the freezing measures.

Table 17. **Assets Reported Under the Regulations Implementing the United Nations Resolutions on both Iran and the DPRK, as of September 2015**

Reporting Entity	Number of Accounts/Contracts	Assets Frozen		Assets Reported but Not Frozen (no cash surrender value) in CAD
		CAD equivalent of amounts in foreign currencies	Amounts in CAD	
Bank X (DTI)	1		78 838	
Bank Y (DTI)	2	591.2	845	
Provincial FI	4		30 647	
Total re. Accounts	**7**	**591.2**	**110 330**	
Federal Life Insurer X	6			29 200
Life Insurer Y	10			3 248 612
Total re. Insurance Contracts	**16**			**3 277 812**

[74] See Global Affairs Canada (nd), Canadian Sanctions Related to Iran, www.international.gc.ca/sanctions/countries-pays/iran.aspx?lang=eng; Canadian Sanctions Related to North Korea, www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.

198. Canada went beyond the UN listings by investigating the financial components of proliferation activities detected on their territory. The authorities successfully prosecuted one individual for the export of prohibited dual-use goods. The enforcement function is shared between the RCMP and the CBSA, with the former taking the lead in instances that include a potential nexus with national security or OCGs, and the CBSA taking the lead in other instances. So far, the investigations revealed no need for freezing measures: the individuals had little assets, most of which had been used to purchase unauthorized dual use goods.

199. Through the analysis of STRs and other information, FINTRAC has detected potential violations of the SEMA and import-export legislation which it disclosed to the CBSA and CSIS.[75] The analysis of STRs notably pointed to some instances of potential wire stripping and sanctions evasion. No figures were provided as the system does not keep track of STRs that also mention suspicion of PF. According to the authorities, in most instances, the REs may not specifically refer to suspicions of PF, but simply highlight that the transactions does not make economic sense. FINTRAC has discussed some of these cases with its partner agencies in the operation meetings of the Counter-Proliferation Operations Committee.

FIs and DNFPBs' understanding of and compliance with obligations

200. Large FIs, and in particular the D-SIBs, have a good understanding of their freezing obligations, including with respect to PF. They generally have staff dedicated to the implementation of TFS that regularly check the UN lists. They are also aware of the risk of wire stripping and have reported instances of potential wire stripping to FINTRAC. Smaller FRFIs have a relatively good understanding of their obligations, although several do not distinguish the PF-related from the TF-related sanctions. DNFBPs, however, are far less aware of their PF-related obligations, so far, none of them have frozen assets belonging to designated persons.

201. Some outreach has been conducted, notably by the RCMP, with a view to increase the general public's awareness of the proliferation risk. Although some of the outreach activities include information on red flags for potentially suspicious PF activities, these efforts have, so far, mainly focused on proliferation activities rather than the implementation of related TFS.

Competent authorities ensuring and monitoring compliance

202. There is no formal mechanism for monitoring and ensuring compliance by FIs and DNFBPs with PF-related obligations. Nevertheless, some monitoring does take place in practice with respect to FRFIs: OSFI, in the exercise of its general functions, has examined the systems put in place by FRFIs to implement the sanctions regimes for both TF and PF. It has also identified shortcomings (in particular the lack of screening of persons other than the customer) and requested improvements in the screening processes. As a result of a sanction recently imposed by the US regulator on a foreign bank with subsidiary operations in Canada and the US for violations of the PF-related sanctions, OSFI

[75] While FINTRAC does not have an explicit mandate to receive reports of suspicions of PF, it is required by law to disclose financial intelligence to assist in investigations and prosecutions for ML, TF and other threats to the security of Canada, which could include PF.

increased its dialogue with and monitoring of that specific bank. Ultimately, it was satisfied that the activities conducted in Canada were different than those conducted in the US and that the risk was limited in Canada. OSFI is not, however, habilitated to sanction any potential breach of PF-related obligations.

203. While this ad hoc monitoring by the OSFI is proving helpful with respect to FRFIs and useful in identifying shortcoming in their implementation of TFS, it does not entirely compensate the lack of a more comprehensive monitoring system.

Overall Conclusions on Immediate Outcome 11

204. **Canada has achieved a moderate level of effectiveness with IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

Several, but not all REs listed in the standard are subject to Canada's AML/CFT framework:

- AML/CFT requirements were found to breach the constitutional right to attorney-client privilege by the Supreme Court of Canada, and, as a result, are inoperative with respect to legal counsels, legal firms, and Quebec notaries. The exclusion of these professions is not line with the standard and raises serious concerns (e.g. in light of these professionals' key gatekeeper role in high-risk activities such as real-estate transactions and formation of corporations and trusts).
- TCSPs (other than trust companies), non FI providers of open loop pre-paid card, factoring companies, leasing and financing companies, check cashing business and unregulated mortgage lenders, online gambling, and virtual currencies do not fall under the AML/CFT regime, but legislative steps have been taken with respect to online gambling, open-loop pre-paid cards and virtual currencies.

FIs including the D-SIBs have a good understanding of the ML/TF risks and of their AML/CFT obligations. While a number of FIs have gone beyond existing requirements (e.g. in correspondent banking), technical deficiencies in some of the CDD requirements (e.g. related to PEPs) undermine the effective detection of some very high-risk threats, such as corruption.

Requirements—on FIs only—pertaining to beneficial ownership were strengthened in 2014 but there is an undue reliance on customers' self-declaration for the purpose of confirming beneficial ownership.

Although REs have gradually increased the number of STRs and threshold-based reports filed, the number of STRs filed by DNFBPs other than casinos remains very low.

With the exception of casinos and BC notaries, DNFBPs—and real estate agents in particular—are not adequately aware of their AML/CFT obligations.

Recommended Actions

Canada should:

- Ensure that legal counsels, legal firms, and Quebec notaries are subject to AML/CFT obligations when engaged in the financial transactions listed in the standard.
- Ensure that TCSPs (other than trust companies) open loop pre-paid cards, including non FI providers, virtual currency and on line gambling to AML/CFT requirements.
- Require DNFBPs to identify and verify the identity of beneficial owners and PEP in line with the standard.

- Require FIs to implement preventive measures with respect to PEPs, and wire transfers in line with the FATF standards, and monitor (e.g. through targeted inspections) and ensure compliance by all FIs of their obligation to confirm the accuracy of beneficial ownership in relation to all customers.
- Enhance the dialogue with DNFBPs other than casinos to increase their understanding of their respective ML/TF vulnerabilities and AML/CFT obligations, in particular with real estate agents, dealers in precious metals and stones (DPMS) (with greater involvement of the provincial regulators and the relevant trade and professional associations). Update ML/TF typologies and specific red flags addressed to the different categories of DNFBPs to assist in the detection of suspicious transactions.
- Consider introducing a licensing or registration regime, or other controls for DPMS.
- Monitor and ensure DNFBPs' and small retail MSBs' compliance with TFS obligations.
- Issue further guidance, especially to non-FRFIs, on the new requirements related to domestic PEPs.
- Strengthen feedback to small banks and the insurance sector on the use of STRs.
- Issue guidance for all REs to facilitate the detection of the possible misuse of open loop prepaid cards in ML and TF schemes.

The relevant Immediate Outcome considered and assessed in this chapter is I04. The recommendations relevant for the assessment of effectiveness under this section are R9-23.

Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF Risks and the Application of Mitigating Measures

205. The level of understanding of ML/TF risks and AML/CFT obligations, as well as the application of mitigating measures vary greatly amongst the various REs.

206. FIs are aware of the main threats and high-risk sectors identified in the NRA, as well as of the level of ML/TF vulnerabilities associated to their activities. Recent trends in the FIs' understanding of risks and AML/CFT obligations is not immediately apparent in the supervisory data (because the latter aggregates as "partial deficiencies" both minor and more severe failures), but, according to the authorities, have been positive. The major banks have developed comprehensive group-wide risk assessments and implement mitigating measures derived from detailed consideration of all relevant risk factors (including lines of business, products, services, delivery channels, customer profiles). Several other FIs stated that their risk assessment and mitigating measures are already in line with the findings of the NRA. Specific attention is paid to cash (including potentially associated to tax evasion) and to the geographic risk (which, especially in the case of large banks, takes into account the index of corruption developed by relevant international organization and includes offshore financial centres). Some FIs also consider trust accounts held by lawyers and other legal professions as presenting a higher risk and, as a result, conduct enhanced

monitoring of these accounts. Specific products associated to real estate transactions, such as mortgage loans, are also considered as high-risk products. Over the last three fiscal years, a total of 9 556 STRs were filed with FINTRAC regarding suspected ML/TF activities in relation to real estate, which represents 3,8% of the overall amount of STRs received, with most STRs coming from banks, credit unions, *caisses populaires*, and trust and loan companies. The main typologies identified in this respect range from the use of nominees by criminals to purchase real estate or structuring of cash deposits to more sophisticated schemes where, for example, loan and mortgage schemes are used in conjunction with the use of lawyer's trust account.

207. In some instances, however, the regulator's on-site inspections revealed issues with the quality and scope of the risk assessments, especially in relation to the elements taken into account as inherent risk of individuals, and to the consistency among business-lines. Smaller FRFIs display a weaker understanding of ML/TF risks, and tend to regard AML/CFT obligations as a burden.

208. The life insurance sector appears to underestimate the level of risk that it faces. According to FINTRAC supervisory findings, life insurance companies and trust and loan companies that are non-FRFIs show the highest level of deficiency in their risk assessment, as well as the weakest understanding of their AML/CFT obligations. Non-federally regulated life insurance companies have a weak understanding of their ML/TF risks than federally regulated companies, and appear particularly refractory to improving AML/CFT compliance.

209. The representatives of the securities sector recognized the high risk rating of their activities, but also noted that the higher level of risk lie mainly in smaller security firms and individuals. Firms not involved in cross-border activities seem to underestimate their vulnerability to ML risk, having a limited notion of geographic risk, as mainly referred to offshore countries. Overall, securities dealers have a good understanding of their AML/CFT obligations, although supervisory findings highlight that the level of understanding is weaker in more simplified structures and that internal controls are a recurring area of weakness.

210. MSBs' level of awareness of AML/CFT obligations is consistent with their size and level of sophistication of their business model. MSBs that operate globally as part of larger networks are aware of the specific ML/TF risks that they face (i.e. risks emanating mainly from the fact their activity is essentially cash-based). They have developed specific criteria to evaluate certain risk (e.g. the risks posed by their agents) to enable them to determine the appropriate level of controls. While the assessment team did not have an opportunity to meet with representative from the smaller independent MSBs,[76] representatives from other private sector entities as well as FINTRAC confirm that smaller MSBs are far less aware of their AML/CFT obligations and their vulnerabilities to ML/TF. According to FINTRAC, community-specific MSBs are reluctant to apply enhanced due diligence to higher risk customers. To assist mainly small MSBs in the development of a RBA, on 1 September 2015 FINTRAC developed an RBA workbook for MSBs.

[76] Under the glossary of the NRA the said category has been defined as these MSBs are focused on retail transactions, and have stand-alone computer systems and street-level retail outlets across Canada. Of these, one sub-group offers currency exchanges only, typically in small values, and is often found in border towns (e.g. duty-free shops), while the other sub-group offers currency exchanges, but may also offer money orders and EFTs, typically as an agent of a national full-service MSB.

211. Casinos vary greatly in size, complexity, and business models. All the relevant gaming activities are subject to AML/CFT requirements where (on the basis of the model in place) the province or the Crown corporation is responsible for their compliance. Representatives from casinos demonstrated a good understanding of their AML/CFT obligations and of the most frequent ML typologies in their sector. Nevertheless, their implementation of CDD measures seems to follow a tick-box approach rather than be based on an articulated risk-assessment. Moreover, casinos seem to be essentially focused on cash, and appear to underestimate to some extent the risk posed by funds received from accounts with FIs.

212. DPMS are highlighted as a high-risk in the NRA. Compliance examinations conducted between 2012 and 2014 revealed industry-wide non-compliance. FINTRAC has worked with two DPMS associations (namely the Canadian Jewelers Association, CJA, and the Jewelers Vigilance Canada, JVC, which, together, represent about one quarter of the Canadian DPMS) to strengthen compliance of this sector. This has led to an increase in these DPMS' understanding of their AML/CFT obligations, as shown in subsequent examinations. Nevertheless, the absence of licensing or registration system or other forms of controls applicable to the sector in its entirety creates major practical obstacles for FINTRAC to properly establish the precise range of subjects that it should reach out to.

213. The real estate agents met, despite being aware of the results of NRA, consider that they face a low risk because physical cash is not generally used in real estate transactions. As the normal practice is to accept bank drafts—agents consider banks have mitigated the ML/TF risk. In the province of Quebec, notaries trust accounts are used to deposit the funds involved in real estate transactions—real estate agents therefore consider that notaries are in a better position to detect possible ML activities, but Quebec notaries are not currently covered by the AML/CFT regime. Real estate agents are overly confident on the low risk posed by "local customer," as well as non-resident customer originating from countries with high levels of corruption.

214. The accountants' level of awareness of AML/CFT obligations is quite low. The competent professional association underlined that, in the absence of guidance and outreach efforts, accountants are often unclear as to when they are subject to the AML/CFT regime.

215. BC notaries provide a wide range of services related to residential and commercial real estate transfers. They are, however, not fully aware of the risk and their gatekeeper role in relation to real estate transactions. Like real estate agents, they consider that all risks have been mitigated by the bank whose account the funds originated from.

216. In May 2015, FINTRAC issued guidance to assist REs in the implementation of their RBA. Most representatives of DNFBPs considered this helpful, but also expressed the need for further initiatives focused on their respective activities.

217. AML/CFT obligations are inoperative towards legal counsels, legal firms and Quebec notaries involved in the activities listed in the standard. In February 2015, the Supreme Court of Canada declared that a portion of Canada's AML/CFT legislation is unconstitutional as to attorneys, because it violates the solicitor-client privilege. Representatives from the private sector and the Canadian authorities confirmed that lawyers in Canada are frequently involved in financial transactions, often related to high-risk sectors, such as real estate, as well as in the formation of trust

and companies. In the context of real estate transactions, in particular, lawyers and Quebec notaries provide not only legal advice, but also trading services,[77] and receive sums from clients for the purchase of a property or a business, deposited and held temporarily in their trust accounts. Representatives of the Federation of Law Societies, although aware of the findings of the NRA, did not demonstrate a proper understanding of ML/TF risks of the legal profession. In particular, they appeared overly confident that the mitigation measures adopted by provincial and territorial law societies (i.e. the prohibition of conducting large cash transactions[78] and the identification and record-keeping requirements for certain financial transactions performed on behalf of the clients)[79] mitigate the risks. While monitoring measures are applied by the provincial and territorial law societies, they are limited in scope and vary from one province to the other. The on-site visit interviews suggested that the fact that AML/CFT requirements do not extend to legal counsels, legal firms and Quebec notaries also undermines, to some extent, the commitment of REs performing related functions (i.e. real estate agents and accountants).

CDD and Record-Keeping

218. CDD obligations, and especially those dealing with beneficial ownership, politically exposed foreign persons (PEFPs) and, for FIs, wire transfers, are not fully in line with FATF standards. In addition, some DNFBPs are not subject to AML/CFT requirements and monitoring (see TCA for more details).

219. Since February 2014, FIs are required to obtain, take reasonable measures to confirm, and keep records of the information about an entity's beneficial ownership. In practice, FIs seem to interpret this new provision as requiring mostly a declaration of confirmation by the customer that the information provided is accurate, to be followed, in some cases, by an open source search. Only a few of the FIs interviewed stated that they would spend time to check the information received and verify the information through further documents and information, which raises concerns. The undue reliance on a customer's self-declaration (as a way to replace the duty to confirm the accuracy of the information provided) appears to be a significant deficiency in the implementation of preventive measures and OSFI has issued findings to FRFIs requiring that more robust beneficial ownerships confirmation measures be undertaken. Moreover, REs have limited methods to confirm the accuracy of beneficial ownership information (see IO.5). Several FIs are in the process of implementing the new requirement by reviewing the information gathered for their existing customers, but most of the FIs interviewed were unable to establish the current stage of this review.

220. Due to the recent entry in force of the new beneficial ownership requirements, there is limited information on how well FRFIs are complying with the new obligations. Recent supervisory findings—albeit limited in numbers- suggest that serious deficiencies remain.

---

[77] This is notably confirmed by the exemption from the requirement to be licensed as real estate agent granted under the relevant provincial legislation (for example in British Columbia, Real Estate Service Act, Section 3, (3) lett. f, and, for Quebec Notaries, Quebec Notary Act, Art.18).
[78] Model Rule on Cash Transactions adopted by the Council of the Federation of Law Societies of Canada on July 2004.
[79] Model Rule on Client Identification and Verification Requirements, adopted by the Council of the Federation of Law Societies of Canada on 20 March 2008 and modified on 12 December 2008.

221. Discussions with DNFBPs, in particular those with real estate representatives, highlighted that even basic CDD requirements are not properly understood and that the implementation of the "third-party determination rule" seems to be mainly limited to asking the customer whether he/she is acting under the instructions of other subjects, without further enquiry.

222. Measures to prevent and mitigate the risks emanating from corruption and bribery (classified as very high threats in the NRA) are insufficient, because of shortcomings in the legal framework (see TCA) and weak implementation of existing requirements. REs' capacity to properly detect these criminal activities is significantly undermined. This is in particular the case with DNFBPs considering that they are not required to take specific measures when dealing with PEPs. In order to determine whether they are in a business relationship with foreign PEPs (i.e. PEFPs) or their family members, FIs combine the information gathered through the client identification forms and the screening process (realized mainly through commercial databases). Most FIs interviewed limited their search to the customer and did not seem to establish whether they were dealing with "close associates" of PEFPs. Furthermore, the range of information required by FIs is limited to the source of funds, and does not always include the source of wealth. Most FIs appear to be over-reliant on the self-declaration of the customer to determine the source of funds, and do not perform further verification of the accuracy of the information provided. The approval of senior management can be obtained "within 14 days" from the day on which the account is activated, which will be extended to 30 days when the new provisions on domestic PEPs enter into force. Some FIs confirmed that, during that timeframe, the PEPs can operate the account—the business relationship can therefore be conducted without adequate controls having taken place. According to OSFI's supervisory findings, in some cases, the involvement of senior management occurs even beyond the prescribed timeframe.

223. There are nevertheless some encouraging signs: over the last four fiscal years, FINTRAC assessed non-FRFIs' determination of PEFPs[80] in the context of 2 508 examinations in four different sectors (credit unions and *caisses populaires*, trust and loan companies, MSB and securities dealers), and identified shortcomings were identified in only 4% of the cases.

224. Several FRFIs, including the D-SIBs,[81] interviewed, apply an onboarding procedure for all customers who include the same determination in relation to "domestic PEPs" and the same enhanced due diligence measures; in order to determine whether a customer is a "domestic PEP," the large banks rely mainly on the information contained in commercial databases. The notion of "domestic PEP" that they apply varies greatly from one institution to the other, and focuses on customers only, i.e. without taking the beneficial owners into account. Some non-FRFIs expressed the need for timely guidance to clarify and facilitate the implementation of the new requirement regarding domestic PEPs and their close associates.

[80] The said determination is considered in relation to the following cases: the opening of new accounts (financial entities and securities), when an EFT over CAD 10 000 is sent or received (financial entities and MSBs) or a lump sum payment of CAD 100 000 or more in respect to an annuity or life insurance policy.

[81] In this respect, OSFI Guidelines B-8, Deterring and detecting ML/TF, explain that FRFIs are not (currently) under any legal obligation to identify domestic PEPs *per se*, nevertheless, where a FRFI is aware that a client is a domestic PEP, the FRFI should assess what effect this may have on the overall assessed risk of the client. If the assessed risk is elevated, the FRFI should apply such enhanced due diligence measures as it considers appropriate.

225. DNFBPs, however, are not required to determine whether they are dealing with foreign PEPs. The interviews conducted confirmed that the political role of customers is not an element that DNFBPs take into account in practice to determine whether further mitigation measures are necessary.

226. While FRFIs have adequate record-keeping measures in place, the smaller credit unions, retail money services business and DNFBPs active mainly in the real estate sector implement weaker measures, which are mainly paper based or based on a combination of paper and manual procedures. FINTRAC identified several deficiencies in record-keeping procedures of BC notaries as well, especially with respect to the conveyancing of real estate.

227. Correspondent banking services are mostly offered by D-SIBs. The D-SIBs have a centralized global management and monitoring of correspondent banking relationships. In some cases, they go above and beyond the current requirements: for example, when reviewing correspondent bank relationships, they also take the quality of AML/CFT supervision into account. Controls on correspondent banking seem to be also reviewed through visits on site and testing procedures by the internal audit. According to OSFI supervisory findings, FRFIs properly assess these services as a higher risk activity, taking necessary mitigation measures.

228. Before introducing new technologies and products, banks typically conduct an assessment of the potential ML/TF risks (and, in doing so, go beyond the requirements of Canadian law). Some banks indicated the lack of information from the authorities regarding typologies on possible exploitation of emerging products that would be helpful in their risk assessment. Among the new products it is worth noting that pre-paid cards are used in Canada but are not currently subject to AML/CFT requirements.[82] Nevertheless, OSFI has alerted FRFIs in the context of its inspections to the need to consider that reloadable prepaid cards operate similarly to deposit accounts, and therefore require equivalent mitigation measures. OSFI supervisory findings reveals that in two cases, FIs had failed to integrate their risk assessment regarding prepaid cards into their overall risk assessment methodology as well as to establish effective controls over their agents. Following OSFI's supervisory interventions, the two institutions are now implementing prepaid access controls in reloadable card programs similar to controls over deposit accounts. Regulatory amendments to include prepaid cards in the regulations are being developed. Other new products currently used—albeit to a very limited extent—include virtual currencies,[83] which fall outside the current framework but which the government has proposed to regulate for AML/CFT purposes.[84]

[82] Global open loop prepaid card transaction volumes have grown by more than 20% over the past four years and were expected to reach 16.9 billion annually in 2014. Despite pre-paid open loop access (thus meaning any financial product that allows customers to load funds to a product that can then be used for purchases and, in some cases, access to cash or person-to-person transfers) has been considered under the NRA of high vulnerability rating, pre-paid cards are not currently subject to AML/CFT requirements.

[83] According to the Canadian Payments Association, as of 10 April 2014, there were between 1 000 and 2 000 daily transactions in Canada involving bitcoin, which represent 1/100 of 1% of the total volume of Canada's daily payments transactions. See Senate Canada, Digital Currency: you can't flip this coin!, June 2015, p. 23.

[84] The legislation to include dealing in virtual currencies among MSBs has been passed, and the associated enabling regulations are being developed.

229. Some of the larger FIs and money transfer companies go beyond current requirements for wire transfers and the filing of EFTRs by applying stricter measures: they notably monitor such transfers on a continuous basis through sample checks of wires received on behalf of customers in order to verify whether they contain adequate originator information, and, if not, take up the matter with the originating banks.

230. FIs have a good understanding of their obligations with respect to TFS (see IO.10). MSBs belonging to large networks, although they are not required to screen on a continuous basis their customer base against the sanctions lists, in practice do so. On-site supervisory inspections revealed, however, deficiencies in the timeliness of the name-screening processes, as well as in their scope (because they do not always extend the screening to the beneficial owners and authorized signers of corporate entities). According to industry representatives and FINTRAC, this is not the case in smaller independent MSBs, where less sophisticated procedures of record-keeping and monitoring are in place.

231. DNFBPs, in particular in the real estate sector, acknowledged that they do not fully understand the requirements related to TFS. They also recognized that their implementation of these requirements is weak, largely because their procedures are mainly paper-based.

Reporting Obligations and Tipping Off

232. With the exception of casinos, reporting by the DNFBPs sectors is very low, including in high-risk sectors identified in the NRA.

Table 18. **Number of STRs Filed by FIs and DNFBPs**

	2011–2012	2012–2013	2013–2014	2014–2015
FIs				
Banks	16 739	17 449	16 084	21 325
Credit Unions/*Caisses populaires*	11 473	12 217	12 522	16 576
Trust and Loan Company	617	757	702	729
Life Insurance	379	379	453	427
MSB	35 785	42 246	46 158	47 377
Securities dealers	811	1 284	2 087	1 825
DNFBPs				
Accountants	-	1	-	-
BC Notaries	1	-	-	1
Casinos	4 506	4 810	3 472	3 994
DPMS	66	129	235	243
Real Estate	15	22	22	34
Total	**70 392**	**79 294**	**81 735**	**92 531**

233. Nevertheless, FINTRAC is of the view that the quality of STRs is generally good and improving. The 1 256 examinations conducted in this respect from 2011/12 to 2014/15, revealed

that 82% of REs examined complied with their obligation. In particular, the REs' write-up for Part G of the reporting form (which relates to the reason for the suspicions) has evolved over the years from a basic summary to a very thorough and complex analysis of the facts. FINTRAC also noted that the percentage of STRs submitted with errors has significantly decreased, namely from 84% (in July 2011) to 17% (in July 2015). Most FIs interviewed rely on both front line staff and automated monitoring systems to detect suspicions. At the end of their internal evaluation process, if the STR is not filed, a record is kept with the rationale for the lack of reporting. STRs are generally filed within 30 days.

234. Awareness and implementation of reporting obligations vary greatly amongst the various sections. In particular: casinos are adequately aware of their reporting obligations. The larger casinos detect suspicious transactions not only through front-line staff, but also through analytical monitoring tools developed at the corporate level on the transaction performed and on the basis of video-investigation in order to identify possible unusual behaviours (such as passing chips). They also report to FINTRAC suspicious transactions that were merely attempted. The real estate sector, however, appears generally unaware of the need to report suspicious transactions that have not been executed. In brokerage firms, the detection of suspicious transactions is mainly left to the "feeling" of the individual agents, rather than the result of a structured process assisted by specific red flags. MSBs, securities dealers and DPMS have significantly increased the number of STRs filed, mainly in response to the outreach, awareness raising and monitoring activities performed by FINTRAC. The *caisses populaires* have also increased their reporting as a result of the centralized system of detection of suspicious transactions developed by the *Fédération des Caisses Desjardins du Quebec*.

235. The larger REs interviewed had good communication channels with FINTRAC and receive adequate feedback on an annual basis on the quality of their STRs and on the number of convictions related to FINTRAC's disclosure. In particular, a Major Reporter Group was established in FINTRAC to foster dialogue. In this context, FINTRAC hosted, in May 2014, a first forum for D-SIBs to enhance compliance with STRs obligations and targeted feedback sessions, and another, in 2015, for casinos. D-SIBs and casinos met considered these forums particularly helpful. Small banks and most categories of DNFBPs do not to receive the same kind of feedback.

236. Tipping off does not appear to be a significant problem in Canada. REs have included in their internal policies, controls and training initiatives some provisions that address the prohibition of tipping off. The measures are considered effective by FINTRAC. So far, no charges have been laid as regards tipping off.

Internal Controls and Legal/Regulatory Requirements Impending Implementation

237. OSFI supervisory findings conducted in the last three years confirm that FRFIs apply sufficient internal controls to ensure compliance with AML/CFT requirements with the five core

elements of the compliance regime.[85] A key OSFI finding is the scope of the two-year review, which is frequently more limited to the existence of controls rather than to their effectiveness.

238. REs with cross-border operations include their overseas branches in their AML/CFT program and extend their internal controls to their foreign subsidiaries. They also adopt the more stringent of Canadian or host jurisdiction rules in their group-wide AML/CFT framework on areas where host country requirements are stricter or more in line with FATF standards. The larger banks reported that they had sharing information mechanisms at group level and, in cases where the local jurisdiction had created obstacles to the information sharing, the local branches were closed.

239. Three of the D-SIBs have branches in Caribbean countries: the two REs interviewed took specific risk mitigating measures by adopting an enterprise-wide management to the highest level. As a result, every high-risk client in the Caribbean must be pre-approved both by senior management in the business and the compliance officer.

240. The data provided by FINTRAC indicates an uneven level of compliance among non-FRFIs. Credit unions and *caisses populaires* have good internal controls in place, which is not the case for trust and loan companies, securities dealers, insurance sector and MSBs: several deficiencies have been identified, including incomplete or not updated policies and procedures, the limited scope of controls, a lack of comprehensive assessment of effectiveness, and no communication to senior management.

241. DNFBPs other than casino and BC notaries have either no or weak internal controls. The discussions with real estate sector representatives also revealed some concerns about the effective control of the proper implementation of AML/CFT requirements by their agents. Some DNFBPs professional associations are working with their members to assist them in increasing their level of compliance and in increasing their awareness with their obligations. In this context, the associations felt that further engagement with FINTRAC would be useful.

Overall Conclusions on Immediate Outcome 4

242. **Canada has achieved a moderate level of effectiveness for IO.4**.

[85] Under PCMLTFR s. 71 (1), the five elements of the compliance regime are the following: appointment of a compliance officer, development and application of written compliance policies and procedures, assessment and documentation of ML/TF risks and of mitigating measures, written ongoing training program, a review of the compliance policies and procedures to test their effectiveness. The review has to be done every two years. Failure to implement any of these five elements is considered serious violation under AMPR and shall lead to an administrative monetary penalty of up to CAD 100 000 for each one (ss 4 and 5).

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

FINTRAC and OSFI have a good understanding of ML and TF risks; and FIs and DNFBPs are generally subject to appropriate risk-sensitive AML/CFT supervision, but supervision of the real estate and DPMS sectors is not entirely commensurate to the risks in those sectors.

The PCMLTFA is not operative in respect of legal counsels, legal firms, and Quebec notaries—as a result, these professions are not supervised for AML/CFT purposes which represents a major loophole in Canada's regime.

A few providers of financial activities and other services fall outside the scope of Canada's supervisory framework (namely TCSPs other than trust companies, and those dealing with open loop pre-paid card, including non FI providers on line gambling and virtual currency, factoring companies, leasing and financing companies, check cashing business, and unregulated mortgage lenders), but legislative steps have been taken with respect to online gambling, open-loop pre-paid cards and virtual currencies.

Supervisory coverage of FRFIs is good, but the current supervisory model generates some unnecessary duplication of effort between OSFI and FINTRAC.

FINTRAC has increased its supervisory capacity to an adequate level but its sector-specific expertise is still somewhat limited. OSFI conducts effective AML/CFT supervision with limited resources.

Market entry controls are good and fitness and probity checks on directors and senior managers of FRFIs robust. There are, however, no controls for DPMS, and insufficient fit-and-proper monitoring of some REs at the provincial level.

Remedial actions are effectively used but administrative sanctions for breaches of the PCMLTFA are not applied in a proportionate and/or sufficiently dissuasive manner.

Supervisory actions have had a largely positive effect on compliance by REs. Increased guidance and feedback has enhanced awareness and understanding of risks and compliance obligations in the financial sector and to a lesser extent in the DNFBP sector.

Recommended Actions

Canada should:

- Ensure that all legal professions active in the areas listed in the standard are subject to AML/CFT supervision.
- Coordinate more effectively supervision of FRFIs by OSFI and FINTRAC to maximize the use of resources and expertise and review implementation of Canada's supervisory approach to FRFIs.
- Ensure that FINTRAC develops sector-specific expertise, continues to have a RBA in its

examinations, and applies more intensive supervisory measures to the real estate and DPMS sectors.

- Ensure that there is a shared understanding between FINTRAC and provincial supervisors of ML/TF risks faced by individual REs and ensure adequate controls are in place after market entry at the provincial level to prevent criminals or their associates from owning or controlling FIs and DNFBPs.
- Ensure that the administrative sanctions regime is applied to FRFIs and that AMPs are applied in a proportionate and dissuasive manner including to single or small numbers of serious violations and repeat offenders. Ensure that OSFI's guidelines relating to AML/CFT compliance and fitness and probity measures are subject to the administrative sanctions regime for non-compliance.
- Provide more focused and sector-specific guidance and typologies for the financial sector and further tailored guidance for DNFBPs, particularly with respect to the reporting of suspicious transactions.

The relevant Immediate Outcome considered and assessed in this chapter is IO3. The recommendations relevant for the assessment of effectiveness under this section are R26-28 & R.34 & 35.

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

243. Market entry controls are applied at federal and provincial level. After market entry, there are effective measures in place at the federal level to ensure that when changes in ownership and senior management occur, FRFIs conduct appropriate fitness and probity (F&P) checks. The federal prudential regulator, OSFI, applies robust controls when licensing a federally regulated financial institution (FRFI). Due diligence measures, including criminal background checks on individuals, are carried out at the market entry stage and OSFI has refused or delayed applications when issues arise. OSFI provided an example where it became aware of misconduct by a small domestic bank's former CEO and ultimately undertook a suitability review of the person. OSFI concluded that he was not suitable to be an officer of the bank and recommended that he not be a member of the board. The bank removed the officer and as a result, OSFI's supervisory oversight strategy of the bank was downgraded. After market entry, FRFIs are responsible for implementing controls around the appointment of senior managers and directors of FRFIs under OSFI Guidelines. OSFI supervises FRFIs for compliance around conducting background checks but this control is not as robust as it is the responsibility of FRFIs to apply fit and proper controls after market entry stage rather than OSFI's in the approval of the appointment of senior managers in FRFIs. Provincial regulators apply market entry controls for non-FRFIs (e.g. securities dealers, credit unions, and *caisses populaires*). These controls include criminal checks to verify the integrity of applicants and to ensure that RE's

implement fit and proper controls. The controls are usually conducted by the RE but are subject to oversight by the provincial regulators. These market entry controls differ between provinces and sectors but, overall, the market entry controls being applied by provincial regulators are robust.

244. Since its last MER, Canada has implemented a money service business (MSB) registration system under the supervision of FINTRAC. One exception to the federal system of registration is in Quebec, where MSBs register with the *Autorité des marchés financiers* (AMF) and FINTRAC. Applicants for registration undergo criminal record checks and fitness and probity checks by FINTRAC and AMF. Individuals convicted of certain criminal offenses are ineligible to own or control an MSB. FINTRAC monitors the control of MSBs as they are required to submit updated information on owning or controlling individuals or entities when changes occur and again when the MSB applies for renewal of its registration every two years. FINTRAC has refused to register applicants and has revoked registration when the applicant was convicted for a criminal offense. An example was given where FINTRAC revoked the registration of two MSBs after the conviction of two individuals that owned both MSBs. Another example was provided where an MSB terminated its relationship with an agent due to fitness and probity concerns about the agent as part of follow-up activity conducted after an examination by FINTRAC. When an MSB registration is denied, revoked, expired, or pending, FINTRAC follows-up appropriately, for example by conducting an offsite review or on-site visit to the MSBs' last known address to ensure that the entity is not operating illegally.

245. There are market entry controls for most DNFBPs in Canada that require them to be licensed or registered by provincial regulators or by self-regulatory bodies (SRBs). Criminal checks are applied by supervisors and SRBs to casinos, BC notaries, accountants, and real estate brokers and agents during the licensing or registration process. The only exception to this is in the DPMS sector where there is no requirement to be registered or licensed or to be subjected to other forms of controls to operate in Canada. All casinos are provincially owned and apply thorough fit and proper procedures for employees.

246. After market entry, provincial regulators conduct some ongoing monitoring of non-FRFIs and DNFBPs and withdraw licenses or registration for criminal violations. The assessment team was provided with examples of restrictions or cancellations of investment dealers' registration by the Investment industry Regulatory Organization of Canada (IIROC) due to misconduct or a violation of the law. However, FINTRAC does not have responsibility for the licensing or registration of FIs or DNFBPs (apart from MSBs) and non-federal supervisors do not appear to implement the same level of controls to monitor of non-FRFIs and DNFBPs to ensure that they are not controlled or owned by criminals or their associates after the licensing or registration stage.

Supervisors' understanding and identification of ML/TF risks

247. Supervisors in Canada participated in the NRA process and understand the inherent ML/TF risks in the country. FINTRAC and OSFI have a good understanding of ML/TF risks in the financial and DNFBP sectors.

248. FINTRAC is the primary AML/CFT supervisor for all REs in Canada and is relied upon by provincial regulators to understand ML/TF risks within their population and to carry out AML/CFT

specific supervision. Provincial supervisors integrate ML/TF risk into their wider risk assessment models and leverage off FINTRAC for their assessment of ML/TF risks as FINTRAC has responsibility for AML/CFT compliance supervision in Canada.

249. OSFI is the prudential regulator for FRFIs and conducts an ML/TF specific risk assessment that applies an inherent risk rating to entities on a group-wide basis rather than an individual basis. It is also able to leverage off its prudential supervisors to better understand the vulnerabilities of individual FRFIs complementing the results of the NRA. OSFI demonstrated that it understands the FRFIs' ML/TF risks through its risk assessment model that appropriately identifies the vulnerabilities in the different sectors and REs under its supervision. It also collaborates well with FINTRAC and other supervisors on their understanding of ML/TF risk. This is very important strength of Canada's system because FRFIs account for over 80% of the financial sector's assets in the country. The sector is dominated by a relatively small number of FRFIs: the six D-SIBs control the banking market and hold a significant portion of the trust and loan company and securities markets in Canada. The largest life insurance companies in Canada are also federally regulated. OSFI has identified 34 FRFIs as high-risk, 32 as medium-risk, and 66 as low-risk. The D-SIBS are all rated as high-risk, given their size, transaction volumes and presence in a range of markets. OSFI updates its risk category for an FRFI or FRFI group on an ongoing basis following on-site assessments, ongoing monitoring and follow-up work. The outcomes from OSFI's risk assessment are effective.

250. FINTRAC has recently developed a sophisticated risk assessment model that assigns risk ratings to sectors and individual REs: the model was reviewed in detail by the assessment team and was compared against the data being collected and analysed in FINTRAC's case management tool. The model is a comprehensive ML/TF analytical tool that considers various factors to predict the likelihood and consequence of non-compliance by a RE. On the basis of its analysis, it rates reporting sectors and entities and the rating is then used to inform its supervisory strategy. FINTRAC's risk assessment has rated all 31 000 REs under the PCMLTFA and identified banks, credit unions, *caisses populaires*, securities dealers, MSBs and casinos as high-risk. FINTRAC has incorporated the findings of the NRA into the model to take account of the inherent risk ratings identified in the real estate and DPMS sectors.

251. Other supervisors, notably AMF and IIROC, integrate ML/TF risk into wider operational risk assessment models of entities that they supervise. They rely on FINTRAC to understand the ML/TF risks among all REs and to disseminate this information to prudential or conduct supervisors, given FINTRAC's role as primary supervisor for AML/CFT compliance in Canada. This appears to be happening in cases where AML/CFT issues arise in the course of prudential or conduct supervision. However, FINTRAC does not share with other supervisors its understanding of ML/TF risks in particular sectors on a regular basis. Provincial supervisors are therefore not aware of the ML/TF risks faced in their respective sectors, particularly around vulnerabilities relevant to ownership and management controls in the non-FRFI and DNFBP sectors. Similarly, FINTRAC and OSFI do not sufficiently share their understanding of detailed risks in FRFIs, e.g. through sharing of existing tools to carry out an integrated risk assessment of all FRFIs. As a result, they do not adequately leverage off their respective knowledge of the different business models and compliance measures in place.

Risk-based supervision of compliance with AML/CTF requirements

252. The regulatory regime involves both federal and provincial supervisors. FINTRAC is responsible for supervising all FIs and DNFBPs for compliance with their AML/CFT obligations under the PCMLTFA. Other supervisors may incorporate AML/CFT aspects within their wider supervisory responsibilities although the assessment team found that in instances where an AML/CFT issue arose, the primary regulator would refer the issue to FINTRAC. Given the primary responsibility held by FINTRAC for all REs and the federal and provincial division of powers for financial supervision other than in the areas of AML/CFT, combined with the geographical spread of the Canadian regulatory regime, the assessment team focused primarily on FINTRAC and OSFI's supervisory regime, but also met with provincial supervisors (e.g. AMF in Quebec) and other supervisors (e.g. IIROC for investment dealers).

253. FINTRAC has increased its resources and the level of sophistication of its compliance and enforcement program ("supervisory program") in recent years. In 2014/2015, there was 79 full-time staff employed in FINTRAC's supervisory program. Of this, 57 staff members were involved in direct enforcement activities including outreach and engagement (10), reports monitoring (5), examinations (37), and AMPs/NCDs (5). It has also developed, and continues to develop, its supervisory capabilities on a RBA. Its understanding of the different sectors and business models and of how AML/CFT obligations apply taking into account materiality and context is somewhat limited. This was communicated to the assessors by REs in the banking and real estate sectors during the on-site visit. FINTRAC has nevertheless increased its understanding of its different reporting sectors which is a challenge given the large number and diverse range of entities it supervises.

254. A range of supervisory tools is used by FINTRAC to discharge its supervisory responsibilities and, for the most part, those tools are applied consistently with the risks identified. A case management tool determines the level and extent of supervision to be applied to sectors and individual REs scoping specific areas for examinations, recording supervisory findings and managing follow-up activities. High-risk sectors are subject to on-site and desk examinations (details of which are contained in this report). Less intensive supervisory tools are used for lower-risk sectors. These tools include self-assessment questionnaires (Compliance Assessment Reports or CARs); observation letters (setting out deficiencies that require action); Voluntary Self Declarations of Non-Compliance (VSDONC); and policy interpretations on specific issues that require clarification. The use of observation letters was piloted with the *caisses populaires* sector in 2013/2014. FINTRAC had identified that *caisses populaires* were reporting large cash transactions of more than CAD 10 000 through automated teller machines which was not possible given the low limit on transactions through such machines. Observation letters were used to correct a misinterpretation of reporting obligations and clarify the correct way to report these types of transactions. FINTRAC also uses outreach tools for lower-risk sectors assistance and awareness building tools among smaller REs with limited resources, compliance experience and works with industry representatives. While supervisory measures are generally in line with the main ML/TF risks, more intensive supervisory measures should be applied in higher risk areas such as the real estate and DPMS sectors. FINTRAC

has updated its risk assessment to identify those sectors as high-risk, in line with the findings of the NRA.

255. OSFI applies a close touch approach to AML/CFT supervision of FRFIs. It engages with FRFIs through its prudential supervisors on an ongoing basis and is well placed to supervise higher-risk entities from an AML/CFT perspective given its knowledge of RE's business models OSFI has a particular focus on the large banking groups (D-SIBs) and insurance companies that dominate the financial market in Canada. These are identified as not only high-risk for prudential purposes but also for ML/TF as identified by OSFI and in the NRA. There is a specialist AML compliance (AMLC) division solely responsible for AML/CFT and sanctions supervision in OSFI and allocates its resources on a risk sensitive basis to supervise FRFIs. OSFI's "AML and ATF (i.e. CFT) Methodology and Assessment Processes" assesses the adequacy of FRFIs' risk management measures through its program of controls and assesses FRFIs' compliance with legislative requirements and OSFI guidelines. The AMLC division has expertise in the sectors it supervises and is covering the principal FRFIs leveraging off prudential supervision. OSFI has a good understanding of its sector, its staff has a high degree of expertise and it is adequately supervising FRFIs for AML/CFT compliance (in conjunction with FINTRAC). The number of OSFI AML/CFT supervisors (i.e. currently 10 supervisors including senior management) is, however, too low given the size of supervisory population and the market share and importance of FRFIs in the Canadian context.

256. FINTRAC and OSFI provided comprehensive statistics, case studies, and sample files relating to examinations of FIs and DNFBPs. There were a greater number of examinations of FIs than DNFBPs; in line with Canada's understanding of ML/TF risk and there were more desk-based than on-site examinations. Between April 2010 and March 2015, 3 431 examinations (1 949 desk-based and 1 482 on-site) of FIs were conducted. During the same period, there were 1 300 examinations (895 desk-based and 405 on-site) of DNFBPs.

Table 19. **AML/CFT Examinations Conducted by FINTRAC/OSFI in Canada 2009–2015**

Sector	Activity Sector	Number of ERs (primary population)	FINTRAC/OSFI Examinations						
Financial Institutions (FIs)			**2009/10**	**2010/11**	**2011/12**	**2012/13**	**2013/14**	**2014/15**	**Total**
Financial Entities	Banks	81	11	10	15	10	19	16	81
	Trusts and Loans	75	6	6	13	7	6	7	45
	Credit Unions */Caisse Populaire*	699	173	205	432	301	170	165	1 446
Life Insurance	Life Insurance	89	70	54	8	13	123	61	329
Money Service Businesses	Money Service Businesses	850	210	201	426	222	161	143	1 363
Securities Dealers	Securities Dealers	3 829	83	120	136	129	167	85	720
Total FI – Desk Exam			270	260	668	389	409	223	2 219
Total FI – On-site Exam			283	336	362	293	237	254	1 765
Total FIs			553	596	1 030	682	646	477	3 984

Sector	Activity Sector	Number of ERs (primary population)	FINTRAC/OSFI Examinations						
DNFBPs			**2009/10**	**2010/11**	**2011/12**	**2012/13**	**2013/14**	**2014/15**	**Total**
Accountants	Accountants	3 829	48	20	0	25	11	10	114
BC Notaries	BC Notaries	336	0	0	0	16	1	6	23
Casinos	Casinos	39	12	12	5	10	1	6	46
Dealers of Precious Metals and Stones	Dealers of Precious Metals and Stones	642	0	0	10	166	276	2	454
Real Estate	Real Estate	20 784	90	70	40	270	203	140	813
Total DNFBP – Desk Exams			83	41	27	322	391	114	978
Total DNFBP – On-site Exams			67	61	28	165	101	50	472
Total DNFBPs			150	102	55	487	492	164	1 450
Total FIs and DNFBPs – Desk Exams			353	301	695	711	800	337	3 197
Total FIs and DNFBPs – On-site Exams			350	397	390	458	338	304	2 237
Total FIs and DNFBPs			**703**	**698**	**1 085**	**1 169**	**1 138**	**641**	**5 434**

257. Both FINTRAC and OSFI demonstrated that they apply scoping mechanisms within their examination strategies. Factors used by FINTRAC to prioritize examinations include: its follow-up strategy; concurrent assessments (with OSFI); market share; cycles; risk score; theme-based; regional selections and compliance coverage (used for lower risk where the preceding factors may not apply). OSFI primarily relies on its risk rating of FRFIs to inform its examination strategy and supervises on a cyclical basis with high-risk entities supervised on a three-year cycle, medium risk on a four-year cycle and low risk on a five-year cycle. It does, however, also supervise on a reactive basis arising out of information received from FRFIs, prudential supervisors or FINTRAC. An average on-site examination conducted by FINTRAC lasts between 2-3 days typically involving 2-3 supervisors, whereas on-site examinations of FRFIs typically last between 1 and 3 weeks and involves 10 or more supervisors from both OSFI and FINTRAC.

Supervision of FRFIs

258. Since 2013, FRFIs have been supervised by OSFI and FINTRAC concurrently. This involved examinations of high and medium risk FRFIs by each agency concurrently but with OSFI taking a top down (i.e. group wide) approach and FINTRAC taking a bottom up (i.e. individual entities/sector) approach with the two agencies coordinating their approaches during examinations but issuing separate supervisory letters setting out their respective findings. At the time of the on-site, it was planned to move to a more coordinated approach through joint examinations. Between 2009 and 2015, OSFI and FINTRAC conducted 126 assessments of FRFIs (OSFI carried out 78, FINTRAC carried out 48, and 22 were concurrent). During that period, OSFI and FINTRAC assessed all 6 D-SIBs (18 assessments in total) that hold a significant share of the Canadian financial market. OSFI issued 373 findings, including 97 requirements relating to lack of processes to comply with AML/CFT obligations and 276 recommendations relating to broader prudential AML/CFT risk management findings. The largest number of findings reflected changes that were required to correct or enhance

policies or procedures and the failure to ensure that risk assessment processed included prescribed criteria, and weaknesses in applying these criteria.

259. There is good supervisory coverage of FRFIs in Canada, which is being applied on a risk-sensitive basis. The level and intensity of the supervision of FRFIs was detailed to the assessment team by FINTRAC and OSFI, sample files were reviewed and feedback was also received from individual FRFIs during the on-site. OSFI provided examples of examinations and its follow-up activity including an AML/CFT examination of a major bank (D-SIB). A 2010 assessment of the bank found its AML/CFT program to be basic or rudimentary and there were 27 major findings ranging from instances of non-compliance with the PCMLTFA and weak risk management processes and policies. OSFI conducted an extensive follow-up program in tandem with the host regulators. When OSFI determined that the action plan to remedy deficiencies was not progressing satisfactorily it met with senior management in the bank. Enhanced monitoring by OSFI was implemented up until 2013 when the bank had adequately addressed the deficiencies to OSFI's satisfaction. Another example was provided involving a bank, which was a small subsidiary of a foreign bank and identified significant issues in its AML/CFT program, OSFI conducted quarterly monitoring of the bank which resulted in all recommendations being addressed by the bank. OSFI and FINTRAC provided examples where they have leveraged off each-others' supervisory findings including where a conglomerate life insurance company had issues with the process for submitting electronic fund transfer reports to FINTRAC that was subsequently reported to OSFI by FINTRAC that led to a prudential finding by OSFI. FINTRAC has also used OSFI's observations of compliance regime gaps to expand its standard scope of that RE to include a review of the compliance regime.

260. OSFI is taking measures to ensure that FRFIs heighten monitoring around overseas investment in Canada to mitigate any risk of illicit flows of funds entering the financial system. OSFI is also monitoring overseas branches of FRFIs as part of its group wide supervisory approach. There are three D-SIBs with branches in the Caribbean and South America. OSFI supervises FRFI on a group wide basis and FRFIs apply group wide policies and procedures and oversee controls (including ongoing monitoring of transactions) applied in overseas branches in Canada. From the discussions held and the material submitted it was found that OSFI exercises rigorous oversight of parent banks' group-wide controls in this key area.

261. Despite there being good supervisory coverage of FRFIs, the split of AML/CFT supervision generates some duplicative efforts. There are currently two agencies supervising FRFIs for AML/CFT compliance, which may be desirable given the size and importance of FRFIs, but suffers to some extent from insufficient coordination between the two agencies and duplication of supervisory resources. OSFI has a good understanding of its sectors and is implementing an effective supervisory regime with limited resources. FINTRAC has more resources but has a very wide population to supervise for AML/CFT compliance that may hinder a full appreciation of FRFIs' business models.

Supervision of non-FRFIs and DNFBPs

262. FINTRAC is applying its supervisory program to non-FRFIs and DNFBPs on an RBA. It is conducting more examinations in higher-risk sectors and using assistance, outreach, and compliance questionnaires to a large extent in sectors that it sees as lower-risk.

263. FINTRAC has shown that it is focusing mostly on high-risk non-FRFIs, securities, MSBs, and credit unions/*caisses populaires* for on-site examinations. It is, however, also conducting on-site examinations in lower-risk sectors, although it is conducting more desk exams in those sectors. FINTRAC also uses other supervisory tools for lower risk REs in the financial sector. On-site examinations have been undertaken by FINTRAC of non-FRFIs including securities dealers, credit unions and *caisses populaires*. The market share of credit unions is concentrated in a relatively small number of credit unions that are being supervised by FINTRAC and credit unions in Canada do not have cross-border operations. Another priority area for FINTRAC is the supervision of MSBs given the high-risk assigned to the sector. It has conducted a high number of examinations of MSBs relative to the size of the primary population figures provided to the assessment team. There appears to be ongoing cooperation between primary regulators and FINTRAC concerning the supervision of non-FRFIs based on details of referrals from other supervisors under MOU arrangements that were provided to the team. FINTRAC is adopting an adequate RBA to supervision of the non-FRFI sector.

264. FINTRAC applies intensive supervisory measures to casinos in line with the risks identified in the sector. This involves in-depth on-site examinations that are conducted on a cyclical basis that ranges from a two to five year cycle based on key factors such as size, risk level and market share. The three largest casinos (that represent 80% of the sector's market share) are examined on a two-year cycle. For other sectors, it has been relying on less intensive activities such as assistance and outreach to DNFBPs to build awareness of compliance obligations. FINTRAC identified the real estate sector and DPMS as medium-risk and accordingly is applying less intensive supervisory tools to those sectors. In the NRA, however, both sectors have been identified as high-risk. FINTRAC is therefore updating its risk assessment of these two sectors in line with the findings of the NRA with a view to applying more intensive measures in the future (including on-site examinations). FINTRAC is relying on the risk model (amongst other factors) of real estate agents to decide on examination selections to cover the sector. It also does not appear to identify adequately DPMS businesses in Canada that fall within the definition of the PCMLTFA.

265. FINTRAC utilizes lower intensity activities to good effect for lower-risk REs. Between 2011 and 2013, close to 10 000 compliance questionnaires (CARs) were issued to mainly sectors identified as lower or medium ML/TF risk. The questionnaire results were used to initiate close to 250 "themed-CAR" risk-informed examinations based principally on the significant non-compliance identified in the CAR. Observation letters are also used to highlight repeated non-compliance or reporting anomalies and remedial action is taken if the entity fails to respond or does not resolve the issues.

266. The legal profession is not currently subject to AML/CFT supervision due to a successful constitutional challenge that makes the PCMLTFA inoperative in respect of legal counsels, legal firms, and Quebec notaries. There is therefore no incentive for the profession to apply AML/CFT measures and participate in the detection of potential ML/TF activities. The exclusion of the legal profession from AML/CFT supervision is a significant concern considering the high-risk rating of the sector and its involvement in other high-risk areas such as the real estate transactions as well as company and trust formation. This exclusion also has a negative impact on the effectiveness of the supervisory regime as a whole because it creates an imbalance amongst the various sectors, especially for REs that perform similar functions to lawyers.

Remedial actions and effective, proportionate, and dissuasive sanctions

267. Supervisors in Canada take a range of remedial actions. There is also an administrative monetary penalties (AMPs) regime in place that is the responsibility of FINTRAC to apply under the PCMLTFA. OSFI and FINTRAC require REs to remediate any deficiencies identified during the assessment process. OSFI has implemented a graduated approach to applying corrective measures or sanctions for FRFIs. Both OSFI and FINTRAC issue supervisory letters to entities subject to AML/CFT assessment that contain supervisory findings and REs are required to take appropriate remedial action. OSFI has provided examples of follow-up action it has taken when FRFI fails to take remedial action.

268. OSFI and FINTRAC have thorough ongoing monitoring and follow-up processes to ensure remediation and have provided examples of steps taken to ensure that deficiencies have been addressed in the FRFI sector, MSBs and a large FI. Measures taken by supervisors include follow-up meetings, further examinations, action plans, and sanctions. OSFI may "stage" FRFIs, which is an enhanced monitoring tool involving four stages where severe AML/CFT deficiencies remain unaddressed. Staging is an effective tool to improve compliance as demonstrated by the Canadian authorities in case studies. There were examples provided where a small bank had not applied AML/CFT obligations correctly and where a staged RE underwent follow-up examinations demonstrated the process increased compliance. FINTRAC also provided examples of monitoring activities of non-FRFIs and DNFBPs where follow-up meetings and re-examinations of MSBs and large FIs resulted in significant improvements in compliance. Remedial actions have also been applied when REs failed to respond to mandatory CARs in the real estate sector. Follow-up activities on all non-responders found that of 55 non-responders, 37 were inactive REs, 1 was a late responder, 10 had inaccurate addresses, and 7 were true non-responders (i.e. increasing RE's risk profile). Where low levels of reporting have been identified, FINTRAC has conducted examinations and put in place remedial actions to increase reporting. This appears to have had an effect on reporting in the institutions concerned, but does not address the wider issue of general low levels of reporting. Supervisors have demonstrated that effective steps have been taken to a large extent to ensure that remediation measures are in place to address AML/CFT deficiencies.

269. FINTRAC can apply sanctions on all REs (including FRFIs) under the AMP regime. AMPs have been imposed and non-compliance disclosures (NCD) have been made to LEAs by supervisors for serious AML/CFT breaches and failure to address significant deficiencies. A notice of violation (NOV) is issued to the RE outlining the violation and penalty prior to an AMP being imposed. The most common violations cited in a NOV were for compliance regime deficiencies and reporting violations. AMPs are not always made public but can be published in egregious cases. AMPs have been imposed in the credit unions and *caisses populaires*, securities, MSBs, casinos, and real estate sectors but at the time of the on-site an AMP had not been applied to a FRFI. The imposition of AMPs in the MSB and casino sector was reported to have had a significant dissuasive effect in those sectors and FINTRAC confirmed that compliance had improved in those sectors as a result. However, the level of AMPs being applied is low relative to the reporting population and the size of the Canadian market. AMPs had not been applied to FRFIs at the time of the on-site is an issue that needs to be addressed. The non-sanctioning of FRFIs, the low number of AMPs applied to other FIs and the low

level of fines imposed to date is unlikely to have a dissuasive effect on FRFIs/larger FIs given their market share and the resources available to them. FINTRAC provided the assessors with current statistics at the time of the on-site (see table below) and with figures for NOVs, which included, among others, the FRFI sector, but for which proceedings were not concluded. OSFI has published guidelines for FRFIs on AML/CFT compliance, and while these guidelines cannot result in a financial penalty under OSFI's regulatory enforcement regime they are subject to measures such as staging.

Table 20. **Administrative Monetary Penalties for AML/CFT Breaches Between 1 April 2010 and 31 March 2015**

Sector	NOV Issued	Reporting Entity Size				Total Value of NOVs Issued (in CAD)	Publicly Named
		Micro	Small	Medium	Larger		
Casino	4	0	0	0	4	2 435 500	0
Financial Entities	15	0	6	9	0	897 705	3
MSB	28	22	5	1	0	768 375	16
Real Estate	7	6	1	0	0	197 310	2
Securities	5	0	3	2	0	587 510	4
Total	**59**	**28**	**15**	**12**	**4**	**4 886 400**	**25**

270. FINTRAC can submit an NCD to LEAs for failure to comply with the PCMLTFA, but this is only done in the most serious cases. Between 2010/2011 and 2014/2015, FINTRAC submitted seven NCDs (all from the MSB sector). These resulted in five investigations being commenced with two cases leading to criminal charges and one conviction (two individuals and one RE).

271. There are proportionate remedial actions being taken by supervisors, in particular extensive follow-up activities by supervisors (e.g. staging by OSFI) that demonstrated their dissuasive effect on the RE involved in the process as it exposes the RE being "staged" to costly remedial activities over a long period of time and ancillary costs such as higher deposit insurance premiums. While remedial actions, as opposed to AMPs, appear effective with respect to the individual RE they apply to, their wider dissuasive impact on other entities is limited, notably because they are not made public. More importantly, the lack of AMPs being applied to FRFIs and the relatively low level of fines imposed negatively impact the effectiveness of the enforcement regime as it affects its dissuasiveness. The non-application of the AMP regime to OSFI guidelines also affects the effectiveness of the Canadian supervisory regime.

Impact of supervisory actions on compliance

272. FINTRAC and OSFI provided examples where their actions have had an effect on compliance through the use of action plans, follow-up activities and findings from subsequent examinations. Feedback from the private sector indicates that supervisors' actions have led to increased compliance in the financial sector. There were examples given of increased compliance in

the FRFI, MSB and insurance sectors arising out of examinations and follow-up activities conducted by supervisors. It was reported by the private sector that the "close touch" nature of OSFI's supervision has enhanced compliance by FRFIs with their AML/CFT obligations. There has been an increase in compliance by REs as FINTRAC's compliance activities increased in recent years, e.g. MSB and casinos, and with the publication of additional information about PCMLTFA obligations.

273. FINTRAC and OSFI have provided written examples of examination findings and follow-up outcomes that demonstrate their effect on compliance by specific FIs and DNFBPs. There has been an increase in compliance among FRFIs and non-FRFIs (casinos) that are subject to cyclical examinations. The more intensive focus on higher risk areas in examination selection strategies has increased compliance in sectors such as FRFIs, MSBs, securities dealers and credit unions.

274. OSFI and FINTRAC supervisory measures to ensure compliance and their remedial actions are having a clear effect on the level of compliance of the individual RE that they apply to. OSFI has a robust follow-up system to monitor the remediation of deficiencies identified. OSFI requires FRFIs provide documentary evidence supporting progress on a continuous basis and requires validation prior to closure of every finding. Quarterly monitoring meetings are conducted with every D-SIB, and meetings with other FRFIs are frequently conducted at the request of OSFI or the FI when there are significant concerns or outstanding issues. Significant remedial steps have been taken by FRFIs based on findings by supervisors and OSFI has demonstrated that it has comprehensive supervisory measures to ensure compliance including the use of more intensive supervision (staging). FINTRAC's follow-up activities have been shown to have a positive effect on compliance by non-FRFIs and DNFBPs. It conducted 515 subsequent examinations across non-FRFIs and DNFBPs over a three-year period and by comparing previous performance indicators with the follow-up indicators revealed that the average deficiency rate had reduced by 13% due to increased compliance. AMPs, when applied, have also had a positive effect on the compliance of REs as demonstrated in follow-up examinations.

275. FINTRAC uses a supervisory tool that assigns "deficiency rates" to REs that are examined. It rates the levels of non-compliance on each specific area of the examination that leads to an overall deficiency rating being assigned to the RE. The overall rating is high, medium, or low and the RE's rating is used to tailor appropriate remedial measures to be put in place. Once remediation has occurred, a follow-up rating is applied and this is compared with the previous rating to identify whether compliance improvements have been made by the RE. The use of deficiency rates at RE and sector level is a useful tool to measure the effect the examination and follow-up process has on compliance by REs. Overall, supervisory measures taken in Canada are having an effect on compliance with improvements demonstrated –albeit to varying degrees- both in the financial and DNFBP sectors. Information provided indicates that compliance has improved in the financial sector, but less so in DNFBPs particularly in the real estate and DPMS sectors.

Promoting a clear understanding of AML/CTF obligations and ML/TF risks

276. There is a good relationship and open dialogue between OSFI and FRFIs. The private sector reports that OSFI has a good understanding of the compliance challenges faced by FRFIs and provides constructive feedback. OSFI has published compliance guidelines and raises awareness

through participation in outreach activities. FINTRAC has published a substantial amount of guidance on its website and increased its level of feedback and guidance to both the financial and, albeit to a lesser extent, the DNFBP sectors. FINTRAC deals with general enquiries through a dedicated call line and has published query specific policy interpretations, both of which are reported by the private sector to be good guidance tools. FINTRAC has dealt with a substantial amount of queries and it has a "Major Reporters" team that provides guidance directly to the largest reporters (mostly financial sector and casinos). It has also taken good steps to raise awareness amongst the MSB sector around the requirement to register and to explain AML/CFT obligations. However, more focused and sector-specific guidance and typologies is required for the financial sector as well as further tailored guidance for DNFBPs to enhance their understanding of the ML/TF risks that they face and of their AML/CFT obligations, particularly with respect to the reporting of suspicious transactions.

277. Supervisors have increased AML/CFT awareness through the use of presentations, seminars, public-private sector forums, establishment of OSFI supervisory colleges, and meetings with the industry. FINTRAC has engaged with non-FRFIs and DNFBPs conducting 300 presentations between 2009 and 2015. It has also hosted events to raise awareness on compliance obligations including a Major Reporters Forum in the financial sector in 2014 and a Casino Forum in 2015.

278. Overall, in light of supervisors' efforts and ML/TF risks in Canada, FINTRAC provides good quality general guidance to REs, but not enough sector-specific compliance guidance and typologies especially in the real estate and DPMS sectors.

Overall Conclusions on Immediate Outcome 3

279. **Canada has achieved a substantial level of effectiveness with IO.3.**

6

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

Canadian legal entities and arrangements are at a high risk of misuse for ML/TF and mitigating measures are insufficient both in terms of scope and effectiveness.

Some basic information on legal persons is publicly available. However, nominee shareholder arrangements and, in limited circumstances bearer shares, pose challenges in ensuring accurate, basic shareholder information.

Most TCSPs, including those operated by lawyers, are outside the scope of the AML/CFT obligations and DNFBPs are not required to collect beneficial ownership information. These pose significant loopholes in the regime (both in terms of prevention and access by the authorities to information).

FIs do not verify beneficial ownership information in a consistent manner.

The authorities rely mostly on LEAs' extensive powers to access information collected by REs. However, there are still many legal entities in Canada for which beneficial ownership information is not collected and is therefore not accessible to the authorities.

Access to beneficial ownership is not timely in all cases and beneficial ownership information is not sufficiently used.

For the majority of trusts in Canada, beneficial ownership information is not collected.

LEAs do not pay adequate attention to the potential misuse of legal entities or trusts, in particular in cases of complex structures.

Recommended Actions

Canada should:

- As a matter of priority, increase timeliness of access by for competent authorities to accurate and up-to-date beneficial ownership information - consider additional measures to supplement the current framework.
- Take the necessary steps to make the AML/CFT requirements operative with regards to all legal professions providing company or trust-related services.
- Ensure that FIs and DNFBPs identify and take reasonable measures to verify the identity of beneficial owners based on official and reliable documents.
- Take appropriate measures to prevent the misuse of nominee shareholding and director arrangements and bearer shares.
- Ensure that basic information indicated in provincial and federal company registers is accurate and up-to-date.
- Apply proportionate and dissuasive sanctions for failure by companies to keep records; to file

information with the relevant registry; or to update registered information within the required 15-day period.

- Determine and enhance the awareness of the ML and TF risks from an operational perspective and the means through which legal persons and trusts are abused in Canada, taking into account ML schemes investigated in Canada as well as international typologies involving legal entities and legal arrangements.

The relevant Immediate Outcome considered and assessed in this chapter is IO5. The recommendations relevant for the assessment of effectiveness under this section are R24 & 25.

7

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

280. Innovation, Science and Economic Development Canada (ISED, formerly Industry Canada) provides a comprehensive overview and comparison on its internet homepage of the various types, forms, and basic features of federal corporations under CBCA, and gives detailed guidance on the incorporation process.[86] Similar information and services are provided through the homepages of all provincial governments except that of New Brunswick. The relevant web links are easy to find through ISEDC's homepage and provide public access to the relevant provincial laws that describe the various legal entities available; the name and contact information for the relevant authority competent for registration; and the procedures to be followed to establish a legal entity. In addition, the Canada Business Network, a collaborative arrangement among federal departments and agencies, provincial and territorial governments, and not-for-profit entities aimed at encouraging entrepreneurship and innovation also provides comprehensive information on the various types of legal entities as well as various forms of partnerships available at the federal and provincial/territorial levels.[87] For legal arrangements, the CRA provides on its homepage comprehensive information on the various trusts structures available under Canadian law.[88]

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

281. Both legal entities and legal arrangements in Canada are at a high risk of being abused for ML/TF purposes. The NRA indicates that organized crime and third-party ML schemes pose a very high ML threat in Canada. Some of FINTRAC's statistics reflected in the NRA suggest that well over 70% of all ML cases and slightly more than 50% of TF cases involved legal entities. Canadian legal entities play a role in the context of channelling foreign POC into or through Canada, as well as in the

[86] See www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs04843.html#articles.
[87] See Canada Business Network (nd), Sole proprietorship, partnership, corporation or co-operative?, www.canadabusiness.ca/eng/page/2853/#toc- corporations.
[88] See Canada Revenue Agency (nd), Types of trusts, www.cra-arc.gc.ca/tx/trsts/typs-eng.html.

laundering of domestically generated proceeds.[89] Typologies identified include: foreign PEPs creating legal entities in Canada to facilitate the purchase, of real estate and other assets with the proceeds of corruption; laundering criminal proceeds through shell companies in Canada and wiring the funds to offshore jurisdictions; and utilization of Canadian front companies to layer and legitimize unexplained sources of income and to commingle them with or mask them as profits from legitimate businesses.[90]

282. LEAs generally concurred with the NRA's findings, and have observed a high number of companies being established without carrying out any business activities, and the use of corporate entities and trusts in Canada to facilitate foreign investment. LEAs also stated that they encounter difficulties in identifying beneficial owners of Canadian companies owned by entities established abroad, particularly in the Caribbean, Middle East, and Asia. While the legal powers available to LEAs are comprehensive and sufficient, the instances in which LEAs were able to identify the beneficial owners of Canadian legal entities and legal arrangements appear to have been very limited and investigations do not sufficiently focus on international and complex ML cases involving corporate elements. Some LEAs are therefore less familiar with ML typologies involving corporate structures. Also, in a number of cases that have been investigated and where Canadian companies were owned by foreign entities or foreign trusts, it was not possible for LEAs to identify the beneficial owners.

Mitigating measures to prevent the misuse of legal persons and arrangements

283. Canada has a range of measures available to collect information on the control and ownership structures of legal entities as outlined below, and comprehensive investigation powers to locate and obtain such information if and as needed (see also R. 24). (i) In cases where a legal entity enters into a business relationship with a Canada FI, that FI must collect and keep beneficial ownership information. (ii) The federal register or the provincial register where the legal entity is incorporated must collect information; and the CRA collects information on legal entities as part of the tax return. (iii) The legal entities themselves are required to keep records of their activities, shareholders and directors. For public companies listed on the stock exchange disclosure requirements exist for shareholders with direct or indirect control over more than 10% of the company's voting rights. Only measure (iii) —maintenance of records by the companies— apply to all legal entities created in Canada.

284. Legal entities in a business relationship with a Canadian FI must provide basic and beneficial ownership information to the FI which has an obligation under the PCMLTFA to maintain this information and confirm its accuracy as needed (see R.10). Many of the FIs that the assessors met confirmed that beneficial ownership would generally be obtained through self-disclosure by the customer, and, in some instances, be followed by an open data search to confirm the accuracy of the information provided. Most FIs stated that they would not require the customer to provide official

[89] FINTRAC Research Brief: Review of Money Laundering Court Case between 2000 and 2014 determines that one of the most frequently used vehicles for ML (in a sample of 40 Canadian Court Cases reviewed) were companies acting as shells for or allowing for a commingling of illicit proceeds with regular business transactions.
[90] Ibid. as well as Project Loupe and Project Chun.

documents to establish the identity of the beneficial owners, nor carry out any independent verification measures other than the open data search. Of the 2.5 million registered legal entities in Canada and customers of a Canada FI, only a fraction had accuracy checks performed with respect to beneficial ownership. In addition, the mitigation of risks is limited by the fact that TCSPs, including those operated by lawyers, are outside the scope of the AML/CFT obligations and DNFBPs are not required to collect beneficial ownership information.

285. Federal and provincial registers record basic information on Canada companies and their directors, as well as on partnerships with businesses in Canada, but do not require the collection of beneficial ownership information. Alberta and Quebec have slightly more comprehensive registration mechanisms, which also cover shareholder information. All information maintained in the federal and provincial registers is publicly available. Updating requirements exist and violations thereof can be sanctioned criminally, but no sanction has been imposed in practice. The reliability of the information recorded raises concerns because there is no obligation on registrars to confirm the accuracy of the basic company information provided at the time of incorporation. Once the incorporation has been completed, companies are obliged to update their records held by the government registrar when there is a material change (e.g. a change in directors) and on an annual basis, and may do so electronically. The same situation applies to partnerships that register for a business permit. The updating process of registered information involves the company reviewing the information indicated in the register and confirming that the information is still correct. There is no need to submit any supporting documents. Despite the absence of verification process at the company registration stage, LEAs stated that basic company information would generally be reliable and comprehensive both on the provincial and federal levels, but they also raised concerns with respect to the accuracy and completeness of shareholder information in the registers of Quebec and Alberta. The CRA, as part of its tax revenue collection obligation, also obtains information on legal entities. However, such information does not include beneficial ownership information.

286. All legal entities, whether incorporated or registered at the federal or provincial level, are subject to record-keeping obligations. All statutes require the keeping of share registers, basic company information, accounting records, director meeting minutes, shareholder meeting minutes and the company bylaws and related amendments. While the relevant obligations are relatively comprehensive, their implementation raises serious concerns. ISEDC and provincial company registries indicated that they would consider company laws to be "self-enforcing" by shareholders, interested parties and the courts, and that they would have no mandate to enforce the implementation of the relevant provisions. While the Director of Corporations Canada has statutory powers to inspect company records, this power has been used only in the context of a shareholder's complaint and not to verify whether a company complies with its record-keeping obligations or to assist the RCMP in obtaining relevant information. So far, no company has been sanctioned criminally for failure to keep accurate and comprehensive company records. The LEAs expressed concern over the accuracy and completeness of companies' records, and stated that it would often be difficult to establish the true shareholder of a company as shareholder registers would often be either outdated or imprecise as they would not indicate whether the registered shareholder is the actual beneficial owner of the share or a proxy for another person.

287. Disclosure obligations for publicly listed companies are comprehensive and include beneficial ownership information.

288. Both bearer shares and nominee shareholders and directors are permitted in Canada. According to the authorities, bearer shares are rarely issued, but nominee shareholder arrangements are a frequent occurrence, and typically involve the issuance of shares in the name of a lawyer, who holds the shares on behalf of the beneficial owner. While companies are generally obliged to keep share registers, there is no obligation on nominees to disclose their status and information on the identity of their nominator, nor to indicate when changes occur in the beneficial ownership of the share.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

289. For information that is not publicly available, Canada has a wide range of law enforcement powers available to obtain beneficial ownership information as discussed in R.24. While the legal powers available to LEAs are comprehensive and sufficient, the instances in which LEAs were able to identify the beneficial owners of Canadian legal entities or legal arrangements appear to have been very limited and investigations do not sufficiently focus on international and complex ML cases involving corporate elements. In a number of cases that have been investigated and where Canadian companies were owned by foreign entities or foreign trusts, it was not possible for LEAs to identify the beneficial owners. This was due mainly to foreign jurisdictions not responding to requests by the Canadian authorities for beneficial ownership information.

290. As indicated in IO 6, other important practical limitations hamper the effectiveness of investigations relating to legal entities and legal arrangements. Despite the adequacy of their powers, it is often difficult for LEAs to obtain beneficial ownership information. As a result, their access to that information is not timely. The relevant Director under each corporate statute has the power to request company records but in practice this power has never been used to assist the RCMP in obtaining beneficial ownership information on a specific legal entity. Equally, at the time of the on-site visit the CRA had not made use of its newly acquired power to refer information to the RCMP in case of a suspicion of a listed serious offense.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

291. The level of transparency of legal arrangements is even lower than in the case of legal entities. There are two mechanisms in place to collect information on trusts: (i) the CRA, as part of the tax collection process, requires the provision of information on the trust assets and the trustee; and (ii) FIs are required to obtain information in relation to customers that are or represent a trust. These two measures suffer from significant shortcomings, both in terms of their scope and effective implementation, for the same reasons as in the context of legal persons, and only a small fraction of Canadian trusts file annual tax returns. There is also a fiduciary duty under common law principles of trustees vis-a-vis those who have an interest in the trust. While this makes it necessary for the

trustee to know who the beneficiaries are, it does not necessarily mean that trustees keep records or obtain information on the beneficial ownership of the trust in practice.

292. The information collected by FIs about legal arrangements raise the same concerns of reliability as outlined for legal entities because FIs rely mostly on the customer to declare the relevant information, they do not require official documentation to establish the identity of the beneficial owners, and do not conduct an independent verification of the information provided. Furthermore, there is no obligation on trustees to declare their status to the FI. As a result, in many cases, the FI may not know that the customer is acting as a trustee. It is unclear how many of the millions of trusts estimated to exist under Canadian law are linked with a Canadian FI.

Effectiveness, proportionality and dissuasiveness of sanctions

293. Proportionate and dissuasive criminal sanctions are available under the PCMLTFA, the CBCA and provincial laws for failure by any person to comply with the record-keeping obligations or registration or updating requirements under the law (see write up for R.24 for more details), but none have been imposed between 2009 and 2014.

294. So far, there seems to have been few instances in which administrative measures were applied for a failure by FIs to identify the beneficial owner or confirm the accuracy of the information received. Similarly, no legal entity in Canada has been struck off the company registry based on in its involvement in illicit conduct. In sum, sanctions have not been applied in an effective and proportionate manner.

Overall Conclusions on Immediate Outcome 5

295. **Canada has achieved a low level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

International cooperation is important given Canada's context, and Canada has the main tools necessary to cooperate effectively, including a central authority supported by provincial prosecution services and federal counsel in regional offices.

The authorities undertake a range of activities on behalf of other countries and feedback from delegations on the timeliness and quality of the assistance provided is largely positive. Assistance with timely access to accurate beneficial ownership information is, however, challenging, and some concerns were raised by some Canadian LEAs about delays in the processing of some requests.

The extradition framework is adequately implemented.

Canada also solicits other countries' assistance to fight TF and, to a somewhat lesser extent, ML.

Informal cooperation appears effective amongst all relevant authorities, more fluid and more frequently used than formal cooperation, but the impossibility for FINTRAC to obtain additional information from REs, and the low quantity of STRs filed by DNFBPs limit the range of assistance it can provide.

Recommended Actions

Canada should:

- Ensure that, where informal cooperation is not sufficient, LEAs make greater use of MLA to trace and seize/restraint POC and other assets laundered abroad.
- Ensure that good practices, such as consultation with prosecution services are applied across police services with a view to improve the use of MLA to identify and pursue ML, associated predicate offenses and TF cases with transnational elements.
- Assess and mitigate the causes for the delays in the processing of incoming and outgoing MLA requests.
- Consider amending the MLACMA to include the interception of private communications (either by telephone, email, messaging, or other new technologies) as a measure that can be taken by the authorities in response of a foreign country's MLA request without the need to open a Canadian investigation.

The relevant Immediate Outcome considered and assessed in this chapter is IO2. The recommendations relevant for the assessment of effectiveness under this section are R.36-40.

Immediate Outcome 2 (International Cooperation)

Providing constructive and timely MLA and extradition

296. Since its previous assessment, Canada has greatly improved its statistics on MLA, and is now able to show several different aspects of MLA related to ML and TF. Canada receives a large number of MLA requests each year. From 2008 to 2015, it received a total of 4,087 MLA requests across all offenses, including 383 for ML investigations and 34 related to TF investigations.

297. The IAG[91] prioritizes the requests (in terms of urgency, court date or other deadline, seriousness of the offense, whether the offense is ongoing, danger of loss of evidence, etc.); it contacts the foreign authorities to obtain further information if the request is incomplete or unclear; and forwards it to the Canadian police for execution (if no court order is needed), or to the IAG's provincial counterparts, or to a counsel within federal DOJ Litigation Branch, if a court order is required.

298. Canada generally provides the requested assistance, both in the context of ML and TF cases:

Table 21. **Outcome of Incoming MLA Requests for ML**

FISCAL YEAR	EXECUTED	WITHDRAWN	ABANDONED	REFUSED
2008–2009	24	0	4	2
2009–2010	23	1	1	0
2010–2011	21	1	5	1
2011–2012	42	5	4	0
2012–2013	39	1	8	3
2013–2014	56	5	8	0
2014–2015	48	4	6	1
TOTAL	253	17	36	7

Table 22. **Outcome of Incoming MLA Requests for TF**

FISCAL YEAR	EXECUTED	WITHDRAWN	ABANDONED	REFUSED
2008–2009	10	0	0	0
2009–2010	2	1	2	0
2010–2011	6	0	0	0
2011–2012	3	1	1	0
2012–2013	5	0	0	0
2013–2014	0	1	0	0
2014–2015	8	0	0	0
TOTAL	34	3	3	0

[91] The IAG is part of the Litigation Branch of the federal DOJ, and which assists the Minister of Justice as central authority for Canada.

299. The assistance provided is of good quality, as was confirmed by the feedback received from 46 countries. There have been numerous good cases of assistance, especially with the US, including covert operations, joint investigations and extraditions. This is an important positive output of the Canadian framework in light of the risk context (e.g. the extensive border with the US, the size of the US economy, and the opportunities it offers to criminal activity).

300. Canada undertakes a range of activities on behalf of other countries. It is, however, limited in its ability to provide in a timely manner accurate beneficial ownership information of legal persons and arrangements established in Canada, for the reasons detailed in IO.5 and IO.7. The fact that Canada cannot intercept, upon request, private communications (either telephone or messaging) in the absence of a Canadian investigation can also hamper foreign investigations, especially those pertaining to OCGs from or with links to Canada or international ML. While this measure is not specifically required by the standard, it is particularly relevant in the Canadian context given the high risk emanating from OCGs, including those with ties to other countries. The scope of this practical shortcoming is, however, limited by the fact that, in most instances, a domestic investigation is likely to be initiated, thus enabling the Canadian authorities to share evidence collected from wiretaps.

301. To facilitate MLA, Canada entered into 17 administrative arrangements with non-treaty partners over the past two years. It also executed over 300 non-treaty requests, mostly to interview witnesses and to provide publicly available documents.

302. Measures were also taken to expedite MLA. The IAG may now send the information requested by a foreign country directly, without the need for a second judicial order. The evidence shared includes, for example, transmission data for an electronic or telephonic message, which help identify the party communicating, tracking data that identify the location of a person or an object, information about a bank account and the account holder. In addition, LEAs that have obtained evidence lawfully for the purposes of their own investigation, may share this information with foreign counterparts without the need for a judicial order authorizing this sharing. For example, evidence obtained through wiretapping by Canadian police may be shared with foreign counterparts in this manner, as confirmed by case law.[92]

303. According to the feedback from delegations, the average time for Canada to respond to their requests varies between 4 and 10 months. The majority of delegations stated that assistance was timely, or did not comment on timeliness, with only one country commenting that the process was slow. Some Canadian LEAs also expressed concerns with the length of time taken to process some of the incoming and outgoing requests. The IAG explains that some of the factors that contribute to lengthening the process include: (i) missing information in the request and the requesting state's slow response to requests for clarification or additional information; (ii) litigation (i.e. when a party affected by the request contests the validity of the court order required, particularly in instances the litigation continues into appellate courts; (iii) because the fact that Canada is awaiting the fulfilment of a condition by the foreign authorities (e.g. in cases where Canada has restrained assets, a final judgment of forfeiture issued by the relevant foreign court may be pending); and (iv) the complexity of the file (e.g. cases involving multiple bank accounts, many witnesses, several Canadian provinces and successive supplemental requests). According to the Auditor General Report 2014, the DOJ processes formal requests for extradition and obtains evidence from abroad appropriately, but does not monitor the reasons

[92] See Supreme Court's decision in *Wakeling v. United States of America* 2014 SCC 72.

for delays in the process.[93] The report found that only 15% of the overall time needed to process MLA requests are within Justice Canada's control, and 30% of the overall time to process extradition requests are within its control. Justice Canada can only take actions to mitigate the delays when it develops insight about the reasons for the delays. In response to the comments by the Auditor General of Canada and after consultations with its international partners and closer research of its files in more recent years, there has been a significant reduction in the delays associated with executing MLA requests made to Canada.

304. Canada extradites its nationals. Pursuant to the Supreme Court of Canada's decision in *U.S. v. Cotroni*, where the extradition of a Canadian citizen is sought based on facts that might form the basis for a prosecution in Canada, certain consultations and an assessment of evidence and circumstances must take place before a decision can be made as to whether to prosecute or extradite. In 99% of such cases, the circumstances favour extradition. Between 2008 and 2015, Canada received 92 extradition requests based on a charge for ML. From the 92 requests, 77 came from the US. As a result of these requests, a total of 48 persons were extradited, while 13 were subject to other measures such as deportation, discharge, voluntary return, or were not located or the means of the return not listed. In the seven cases where the request was refused, the grounds were related either to insufficient evidence to show knowledge of ML, concerns with human rights record or prison conditions in the requesting state, or the defendant was not located. Between 2008 and 2015, five persons were extradited for TF.

305. More than half (52%) of the extradition requests take from 18 months to five years to be completed; from which 28% take from three to five years to be completed. An approximate of 4% take more than five years to be completed. Most of the delegations mentioned having successful extradition requests with Canada, although some mentioned having experienced delayed responses from the Canadian authorities regarding those requests.

Seeking timely legal assistance to pursue domestic ML, associated predicate and TF cases with transnational elements

306. From 2008 to 2015, Canada sent more than 700 MLA requests, including 124 (i.e. around 17%) on the grounds of ML charges. Some requests were made, e.g. in the context of real estate or to obtain bank records, as well as to freeze and confiscate funds or assets abroad.[94] Most of these requests were made on the basis of investigations conducted in the province of Quebec (which is in line with the findings in IO.7 and IO.8). Between 2008 and 2015, Canada also made 24 requests in the context of TF investigations, 11 of which during fiscal year 2014/2015 in light of increased concern about "foreign fighters."

307. The number of request for assistance on ML cases has increased over the years, but still appears relatively low in light of Canada's risk profile. The authorities explained that they frequently have recourse to informal means of cooperation (see core issue 2.3 below) in lieu of MLA because it is quicker. However, while informal means do simplify and expedite the process

[93] Office of the Auditor General of Canada (2014), Report of the Auditor General of Canada—Fall 2014, p. 11, www.oag-bvg.gc.ca/internet/docs/parl_oag_201411_02_e.pdf. The assessors reviewed 50 extradition and MLA files from between 2011 and 2013, which included incoming and outgoing requests, and both ongoing and closed files.

[94] From 2008 to 2005, Canada sent 113 requests with respect to tracing (bank or real estate records) and 33 requests with respect to freezing/restraint (funds or assets).

of assistance, they cannot substitute formal MLA in all cases (e.g. when there is a need for the tracing or the freezing of assets abroad). The relatively small number of outgoing requests may also be explained by the fact that Canada is not pursuing complex and transnational ML schemes to the extent that it should (see IO.7). Although the outflows of POC generated in Canada appear to be moderate in comparison to the inflows of POC generated abroad, data suggests that Canadian citizens and corporations use tax havens and offshore financial centres to evade taxes, in particular those located in the Caribbean, Europe and Asia- cooperation with the relevant countries in these regions would therefore prove helpful to Canada. Some domestic provincial LEAs mentioned concerns about the delay in the sending of requests to foreign countries. In response to that point, the IAG assures that the same case management prioritization measures are in place for outgoing requests as for incoming requests.

Seeking other forms of international cooperation for AML/CTF purposes

308. Canadian agencies regularly seek and provide other forms of international cooperation to exchange financial intelligence and other information with foreign counterparts for AML/CFT purposes. In particular, the cases studies provided as well as the discussions held on-site indicate a regular use by LEAs of foreign experts, missions abroad to secure evidence and assets, and joint investigations. Canada does not separate the information according to the function (i.e. seeker or provider of assistance), and the information provided therefore combines the objects of core issues 2.3 and 2.4.

309. FINTRAC is both a FIU and a regulator/supervisor:

- As Canada's FIU: FINTRAC is a member of the Egmont Group and shares information only on the basis of MOUs with counterparts. FINTRAC is open to sign a MOU with any FIU, and the process can be concluded very quickly, but sometimes this does not happen due to the absence of interest of the foreign FIU. At the time of the on-site there were 92 MOUs with foreign FIUs. In the absence of an MOU, they cannot share information. According to the feedback provided by other delegations, the information provided by FINTRAC is of good quality. Nevertheless, some limitations have a negative impact on the type of information that FINTRAC can share: more specifically, the fact that (i) FINTRAC is not habilitated to request and obtain further information from any REs; (ii) there are no STRs from lawyers. Canada receives far more requests for assistance than it sends to support Canadian investigations and prosecutions. Although there were fewer queries sent to its foreign counterparts a few years ago, FINTRAC has recently increased the number of requests sent. The queries received and sent to the US (which, as mentioned above, is a major Canadian partner in international cooperation) are generally comparable. In addition to requests sent, the significant increase of FINTRAC's numbers of proactive disclosures sent to its counterparts (2012-2013:52; 2013-2014:93; 2014-2015:190) highlights the Canadian FIU's willingness to share the relevant information it holds with its foreign partners.

- As a supervisor, FINTRAC regularly shares information with foreign supervisors and consults with international partners. In addition to general information, it also exchanges, on an on-going basis, since 2009, compliance information on operational processes with AUSTRAC. After several bilateral meetings, FINTRAC and AUSTRAC are working together in compliance actions on an MSB that operates both in Canada and in Australia. FINTRAC's public MSB registry was also provided to Australia and other jurisdictions, because the comparison of MSB lists is useful during the criminal record check of MSBs, who may operate in more than one country. FINTRAC has also an MOU with FINCEN.

310. The RCMP regularly exchanges information with its foreign counterparts. Cooperation is developed through police channels (Interpol, Europol, Five Eyes Law Enforcement Group), through the Camden Asset Recovery Informal Network (CARIN) and through several MOUs, including one with The People's Republic of China. The existence of this MOU with China is important in light of the risks of inward flow of illicit money generated in China; however, no assistance with this country was reported in the province of British Columbia, despite the fact that it appears to be at greater risk of seeing its real estate sector misused to launder POC generated in China. The RCMP uses a well-established and effective network of liaisons officers (42 officers and 10 intelligence analysts in 26 countries) to seek and provide assistance and other types of information, in ML and TF investigations. It shares intelligence information, carries out investigations on behalf of foreign counterparts, and participates in joint investigations, as demonstrated in several cases studies provided by the authorities. From 2008 to 2013, it sent 98 requests for assistance on PPOC and ML/TF-related occurrences to the US, 94 to Europe and 60 to Asia. The RCMP and other police forces are also the ones who execute incoming requests of assistance, when there is no need for a judicial order, and the information or documentation is publicly available or can be obtained on a voluntary basis.

311. OSFI concluded 30 MOUs with various international prudential supervisors. No statistical information was provided in this respect but the authorities mentioned that OSFI regularly exchanges information regarding FRFIs with its foreign counterparts. In 2012, OSFI hosted an AML/CFT Supervisory College on five conglomerate banks with 19 foreign regulators in attendance. The College provided an opportunity for the foreign regulators to provide information on AML/CFT supervision in the host jurisdictions, and also for the banks themselves to provide an overview of their AML/CFT programs. The OSFI Relationship Management Team also hosts Supervisory Colleges of a general prudential nature, where foreign regulators attend. When OSFI conducts assessments at foreign operations of FRFIs, it seeks cooperation of the host regulator, who usually participates on the on-site with OSFI. The Colleges are an important and effective way for the sharing of information with OSFI's foreign counterparts.

312. The CBSA cooperates on a regular basis with US Immigration and Custom Enforcement (ICE) and US Custom Border Protection for the Sharing of Currency Seizure Information, including in AML/CFT matters. This cooperation is very important due to the extensive border shared by Canada and the US Cases provided by the authorities demonstrated the CBSA's participation in joint operations. CBSA also receives information from the US Department of Homeland Security, which helps the detection of suspected POC and leads to the seizure of the currency. Its participation in the Homeland's Security BEST Program resulted in the CBSA

initiating 103 criminal investigations related to the smuggling of narcotics, smuggling of currency and firearms and illegal immigration. The CBSA also receives international cooperation from foreign governments or law enforcement and maintains strong collaboration with the 5-Eyes Community. It shares FINTRAC results with partner agencies in the US on files that indicate ML activities that cross the Canada/US border (Mexican Mennonites, outlaw motorcycle gangs, Persian organized crime). Nevertheless, the authorities also mentioned that financial information and information on import and export files declared in Canada are difficult to obtain by their counterparts, due to Canada's strong privacy framework.

313. The CRA has 92 Tax treaties and 22 Tax Information Exchange Agreements (TIEA) with international partners. However, CRA and CBSA do not cooperate under the Customs Mutual Assistance Agreement with the US. As is common for Canadian authorities, they would always require and MLAT to share the information regarding trading operations (where there is an important risk of trade-based ML, especially considering that more than 60% of Canada's GDP consists of international trade). Between 2009 and 2015, the CRA sent 72 requests and received 11 requests for exchange of information to foreign counterparts, in the context of criminal investigations.

314. The CSIS regularly receives from and shares financial information with FINTRAC in support of both organizations' mandates. In relation to high-risk travellers, it uses financial intelligence to determine how ready an individual may be to travel by determining whether they have purchased equipment, or if they have saved up money that could be used to support themselves while they are abroad. Due to confidentiality issues and matters of national security, CSIS did not provide the assessors any statistical data.

315. Feedback from the countries on Canada's assistance through other forms of cooperation is generally good. Most of the delegations indicated that the information received from FINTRAC in response to their requests was useful, of good content and of high quality. The limitation to request further information from any REs and bank information was, however, also reported. FINTRAC's average time to respond to request from its counterparts is 35 days (which is in line with the Egmont Group standards).The feedback from the US FIU is very positive. FINTRAC and FINCEN have had a strong working relationship for years, both as FIUs and as AML/CFT supervisory/regulatory agencies, which is very important in light notably of the extensive border between the two countries, the illicit flows of criminal money, as well as the linkages between OCGs active in both countries. The US, which is Canada's main partner in cooperation, also reported and outstanding cooperation exchange with CRA. They indicated that the CRA responds to American requests for records in a very timely manner and has provided assistance in the location and coordination of witness interviews.

International exchange of basic and beneficial ownership information of legal persons and arrangements

316. While the authorities recognize the risk of misuse of Canadian legal persons and arrangements, they do not appear to have identified, assessed and understood with sufficient granularity the extent to which Canadian legal persons and legal arrangements are misused for ML or TF in the international context. In addition, there are serious concerns about the timeliness access to relevant information by competent authorities as well as with respect to the

quality of the information collected by REs. As a result, cooperation in relation to foreign requests regarding BO of legal persons and arrangements cannot be fully effective.

317. Canada, and FINTRAC in particular, regularly receives requests for corporate records and information on beneficial ownership of both corporations and trusts (which points to the relevance of Canadian legal entities and trusts in international ML operations). FINTRAC provides the requested information as long as it already has it (i.e. it has received a STR or other report including VIRs regarding the relevant corporation or trust), it can access it (e.g. information from the corporate registries of Alberta and Quebec, or from the MSB registry, when the ownership is 25% or more, or from any other public source). The IAG also receives requests for basic and beneficial ownership information which it forwards to LEAs for execution. Between 2008 and 2015, it received 222 for corporate or business records, including 78 related to ML and 1 to TF investigations. Most of these requests have been executed.

Overall Conclusions on Immediate Outcome 2

318. **Canada has achieved a substantial level of effectiveness for IO.2**.

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations of Canada in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation (R.). It should be read in conjunction with the Detailed Assessment Report (DAR).

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2008. The report for that assessment or evaluation is available from the FATF website.[95]

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

The requirements of R.1 were added to the FATF standard in 2012 and were, therefore, not assessed during the previous mutual evaluation of Canada.

Obligations and Decisions for Countries

Risk Assessment

Criterion 1.1— The Government of Canada has developed a risk assessment framework to support the identification, assessment and mitigation of ML/TF risks and includes a process to update and enhance this assessment over time. ML and TF threats were documented separately. Canada completed its first National Risk Assessment (NRA), the "Assessment of Inherent Money Laundering and Terrorist Financing Risks in Canada," in December 2014. In April 2015, the senior officials of participating federal departments and agencies endorsed the internal and draft public versions of the report. In July 2015, the Minister of Finance, on behalf of the government, released the public version of the NRA.[96] Canada's ML/TF Inherent RA is supported by a documented NRA Methodology with defined concepts on ML/TF risks and rating criteria. The report, which reflects the situation in Canada up to 31 December 2014, provides an overview of the ML/TF threats, vulnerabilities and risks in Canada before the application of mitigation measures.

The NRA consists of an assessment of the inherent (i.e. before the application of any mitigation measures) ML/TF threats and inherent ML/TF vulnerabilities of key economic sectors and financial products, while considering the contextual vulnerabilities of Canada, such as geography, economy, financial system and demographics.

Pursuant to the Interpretative Note to R.1, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from ML and TF, and which do not fall under the definition of financial institution or DNFBP, they should

[95] See FATF (2008), Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism, www.fatf-gafi.org/countries/a-c/canada/documents/mutualevaluationofcanada.html
[96] See Department of Finance Canada (2015), Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp

consider applying AML/CFT requirements to such sectors. In that regard, the 2008 MER discussed whether Canada had considered extending AML requirements to white-label ATMs (see paragraphs 1357 to 1364). In a 2007 FINTRAC report highlighted the vulnerability of white-label ATMs to ML, and various press articles highlight the risk of misuse of white-label ATMs. The authorities are considering mechanisms to address this risk.

Criterion 1.2— The Department of Finance Canada (Finance Canada) is the designated authority for coordinating the work associated with the ongoing assessment of ML/TF risks. In Canada government responsibilities in regard to AML/CFT are divided between the federal government and the ten provinces (the three territorial governments exercise powers delegated by the federal parliament). In that regard, the execution of AML/CFT actions involves collaboration and coordination across all levels of government.

The terms of reference for (i) the Interdepartmental Working Group on Assessing ML and TF Risks in Canada and (ii) the permanent National Risk Assessment Committee (NRAC; the senior-level AML/CFT Committee) establish Finance Canada as the designated authority for the initiative. The Minister of Finance is the Minister responsible for the PCMLTFA. Therefore, as decided by the Cabinet, the responsibility for coordinating the AML/CFT regime and the NRA falls also to Finance Canada.

Criterion 1.3— Canada's risk assessment framework contemplates a process to update and enhance this assessment over time. In accordance with the document "Proposed Governance Framework for Canada's ML/TF Risk Assessment Framework" (endorsed on 13 November 2014), the NRA update is now coordinated through the NRAC, the successor body to the Working Group that developed the NRA. The Terms of Reference of NRAC were approved at the senior-level AML/CFT Committee in April 2015. NRAC is composed of representatives of the federal departments and agencies that comprise Canada's AML/CFT (and may invite other public and private sector partners to participate), which facilitates sharing findings across the organizations represented to help them understand the evolving risks and ML/TF environment, as well as discuss and propose mitigations. Finance Canada is the permanent co-chair of the NRAC; the other co-chair position rotates every two years among other federal departments or agencies. NRAC is required to prepare a formal update every two years on the results of the risk assessment and an informal update on an annual basis. The reports are addressed to the senior level AML/CFT Committee. As Canada completed its NRA in December 2014, it is relatively up to date. Furthermore, the Committee will meet every six months or more frequently if needed, to review emerging threats and new developments and will report to the senior-level Committee on an annual basis with updates.

Criterion 1.4—Information on the results of the NRA is provided to competent authorities, self-regulatory bodies, FIs and DNFBPs through different working groups, committees and outreach activities. The NRA was released publicly on 31 July 2015 (and is available on the websites of Finance, FINTRAC, and OSFI). The NRA methodology and results were also shared and discussed beforehand by Finance

Risk Mitigation

Criterion 1.5— The risk mitigation is implemented through various thematic national strategies, to wit: National Identity Crime Strategy (2011), Canada's Counter-terrorism Strategy (2013); National Border Risk Assessment 2013–2015; 2014–2016 Border Risk Management Plan; Enhanced Risk Assessment Model and Sector profiles; OSFI's AMLC Division AML and CFT Methodologies and Assessment Processes; OSFI-Risk Ranking Criteria; and the CRA's techniques to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals.

Criterion 1.6— Financial activities are subject to AML/CFT preventive measures as required in the FATF Recommendations, except when these activities are conducted by the sectors that are not subject to AML/CFT obligations under the PCMLTFA. These sectors include check-cashing businesses, factoring companies, and leasing companies, finance companies, and unregulated mortgage lenders, among others. The NRA assessed the ML/TF vulnerabilities of factoring, finance and financial leasing companies as medium risk, while pointing out that these entities were very small players as a proportion of Canada's financial sector. However, the ML/TF risks for these sectors has not been proven to be low and the non-application of AML/CFT measures is not based on a risk assessment. .

Except for the legal profession, all DNFBP sectors are required to apply AML/CFT preventive measures. Lawyers are covered as obliged AML/CFT entities, pursuant to PCMLTR, Section (s.) 33.3; however, the AML/CFT provisions are inoperative in relation to lawyers and Quebec notaries (who provide legal advice and are, therefore, considered legal counsel, PCMLTFA s. 2) as a result of a 2015 Supreme Court of Canada ruling.

Supervision and Monitoring of Risk

Criterion 1.7— REs are required to implement enhanced or additional measures in high-risk situations pursuant to PCMLTFA, ss.9.6(2) and 9.6(3) and PCMLTFR, §71(c) and 71.1(a) and (b) (see discussion on R.10 for additional information on enhanced CDD measures). The REs are expected to integrate the NRA results in their own risks assessments.

PCMLTFA, s.9.6(2) provides that REs develop and apply policies and procedures to address ML and TF risks. PCMLTFA, s.9.6(3) and PCMLTFR, s.71.1(a) and (b) require REs to apply "prescribed special measures" to update client identification and beneficial ownership information, and to monitor business relationships when higher risks are identified through the entity's risk assessment.

Nevertheless, the provisions discussed in the paragraphs above do not apply to the sectors that are not subject to reporting obligations under the PCMLTFA. These include sectors such as the legal counsels, legal firms and Quebec notaries, factoring companies, financing and leasing companies, among others. Of these sectors, the legal counsels, legal firms and Quebec notaries are exposed to ample ML opportunities and are exposed to higher risks. Therefore, as the legal profession is not required to take enhanced measures regarding higher ML risks (or any ML risks, for that matter) the risks associated with this sector are not being effectively mitigated.

Exemptions

Criterion 1.8— PCMLTFR ss.9, 62 and 63 provide for exemptions from the customer identification and record-keeping requirements in certain specific circumstances assessed as low risk by the authorities (for details about the exemption regime, see discussion on R.10 below). OSFI and FINTRAC continuously assess the risks associated with their supervised sectors and the current assessment of low risks appear to be consistent with the findings of the NRA.

Criterion 1.9— PCMLTFA, s.40(e) requires FINTRAC to ensure compliance with PCMLTFA provisions. PCMLTFA, s.9.6(1)-(3) requires REs Act to implement measures to assess ML and TF risks, and monitor transactions in respect of the activities that pose high ML/TF risks. OSFI and FINTRAC apply a risk-based approach to the supervision of their supervised sectors. As discussed previously, the legal profession is not subject to AML/CFT obligations and is, therefore, not monitored by FINTRAC. However, some high-risk DNFBPs are not subject to AML/CFT obligations and are thus not supervised in relation to their obligations under R.1.

Obligations and Decisions for Financial Institutions and DNFBPs

Risk Assessment

Criterion 1.10— PCMLTFA, s.9.6(2) and PCMLTFR, §71(c) requires REs to conduct risk assessments and consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied. PCMLTFR, s.71(e) provides that the REs shall keep their risk assessments up to date. All supervised entities and those subject to examination by FINTRAC are obligated under their sector legislation or PCMLTFA, s.62 to provide any material that FINTRAC or sector regulators may require. FINTRAC Guideline 4 (Implementation of a Compliance Regime, February 2014) provides a checklist of products or services that should be considered high-risk. OSFI Guideline B-8 (Deterring and Detecting Money Laundering and Terrorist Financing) provides instruction on the FRFIs risk assessment policies and procedures. As mentioned above, none of the AML/CFT requirements are applicable to lawyers, legal firms, and Quebec notaries.

Risk Mitigation

Criterion 1.11— *a)* Under PCMLTFA s 9.6(1) and PCMLTFR, s.71, REs are required to develop written AML/CFT compliance policies and procedures, which are approved by a senior officer of the RE in accordance with PCMLFTR s.71(1)(b).

b) These policies and procedures, the risk assessment and training program are required to be reviewed at least every two years (PCMLFTR, ss.71(1)(e) and 71(2)). The REs must also assess and document ML and TF risks (PCMLTFA, s.9.6(2) and PCMLFTR, s.71(1)(c)).

c) There are several different provisions that require REs to implement enhanced or additional measures in high-risk situations: Under PCMLTFA, ss.9.6(2) and 9.6(3), REs are required to assess ML and TF risks and enhanced due diligence, record keeping and monitoring of financial transactions that pose a high risk of ML or TF. The PCMLTFR requires REs to apply enhanced measures when high risks are identified in their activities as a result of ongoing monitoring. The

sectors covered by the PCMLTFR are banks and other deposit-taking institutions (s.54.4); life insurance (s.56.4); securities (s.57.3); MSBs (s.59.02); accountants (s.59.12); real estate (s.59.22); British Columbia Notaries (s.59.32); real estate developers (s.59.52), casinos (s.60.2); and Departments and agents of the Queen in rights of Canada or a Province for the sale or redemption of money orders for the general public (s.61.2). The provisions addressing the legal profession are not applicable to legal counsels, legal firms and Quebec notaries for the reasons stated earlier. FINTRAC, Guideline 4 and OSFI Guideline B-8 provide additional guidance.

Criterion 1.12— The Canadian AML/CFT legislation does not provide for simplified measures.

Weighting and Conclusion:

The main inherent ML and TF risks were identified and assessed for the implementation of appropriate mitigation.

Canada is largely compliant with R.1.

Recommendation 2 - National Cooperation and Coordination

Canada was rated LC in the 2008 MER with former FATF R.31; the cooperation between the FIU and LEAs was not considered to be fully effective.

Criterion 2.1— Several national strategies and policies are in place to inform AML/CFT policies and operations. The main AML policies and strategies are the *National Identity Crime Strategy* (RCMP 2011); *National Border Risk Assessment 2013–2015* (CBSA); *2014–16 Border Risk Management Plan* (CBSA); *Enhanced Risk Assessment Model and Sector profiles* (FINTRAC); *AMLC Division AML and CFT Methodology and Assessment Processes* (OSFI); *Risk Ranking Criteria* (OSFI); *Risk-Based Approach to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals* (CRA) and CRA-RAD Audit Selection process. The RCMP is currently developing their National Strategy to Combat Money Laundering. These AML strategies and policies are linked to the 2011 *Canadian Law Enforcement Strategy on Organized Crime*. In addition, the Government's other main AML/CFT concerns are reflected in Finance Canada's Report on Plans and Priorities,[97] which outlines the AML/CFT regime's spending plans, priorities and expected results. Canada's CFT strategy forms part of the broader Counter-terrorism Strategy.[98] Similarly, the country's PF strategy forms part of the broader strategy to counter the proliferation of chemical, biological, radiological and nuclear weapons.[99]

The TRWG is an interdepartmental body that serves as a forum to enhance dialogue, coordination, analysis and collaboration, among PS Portfolio members and government departments with an intelligence mandate, on issues related to threat resourcing, including ML, TF and proliferation

[97] Department of Finance Canada (2015), Report on Plans and Priorities 2015–16, p. 29, www.fin.gc.ca/pub/rpp/2015-2016/index-eng.asp
[98] Public Safety Canada (2013), Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx
[99] Public Safety and Emergency Preparedness Canada (2005), The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg-rchvd/index-en.aspx

activities, organized crime and other means through which threat actors resource their activities. It also highlights the security and intelligence components of files associated with Canada's AML/ATF Regime.

Criterion 2.2— Finance Canada is the domestic and International policy lead for the whole AML/CFT regime, and is responsible for its overall coordination, including AML/CFT policy development and guiding and informing strategic operationalization of the NRA framework.

Criterion 2.3— The Canadian regime is also supported by various interdepartmental formal and informal working-level bilateral and multilateral working groups and committees, depending on the nature of the issues to be addressed including: NRAC; NCC; IPOC ; IFAC; TRWG, and the ICC.

To combat ML, Canada also coordinates domestic policy on the federal criminal forfeiture regime under the IPOC. IPOC's interdepartmental Director General-level Senior Governance Committee led by Public Safety Canada includes: CBSA, CRA, PPSC, PS, PWGSC and the RCMP. The Committee is mandated to provide policy direction, promote interdepartmental policy coordination, promote accountability, and to support the Initiative.

The NCC is the primary forum that reviews progress of the National Agenda to Combat Organized Crime. NCC's 5 Regional Coordinating Committees communicate operational and enforcement needs and concerns to the NCC, acting as a bridge between enforcement agencies and officials and public policy makers. Canada coordinates domestic AML policy on the federal criminal forfeiture regime under the IPOC Advisory Committee and the IPOC Senior Governance Committee.

The IFAC is an interdepartmental consultative body that has the responsibility for the sharing, analysis and monitoring of information related to ML/TF threats posed to Canada by foreign jurisdictions or entities. The ICC assists the Minister of Public Safety and Emergency Preparedness by providing the requisite analysis and considerations to inform the recommendations to the Governor in Council regarding listing of entities.

OSFI and FINTRAC coordinate their activities through a common approach for supervision of FRFIs, starting in 2013, by conducting simultaneous AML/CFT examinations. FINTRAC informs its compliance enforcement strategies with findings provided by other federal and provincial regulators in order to monitor and enforce AML/CFT compliance by REs. FINTRAC has established 17 Memoranda of Understanding (MOU) with federal and provincial regulators for the purpose of sharing information related to compliance with Part 1 of the PCMLTFA. The RCMP leads the Integrated National Security Enforcement Teams (INSETs) in major centers throughout the country). INSETs are made up of representatives of the RCMP, federal partners and agencies such as CBSA, CSIS, and provincial and municipal police services.

Criterion 2.4— Counter-proliferation (CP) efforts, including proliferation financing, are coordinated via a formalized CP Framework created in 2013. PS chairs the Counter-Proliferation Policy Committee, at which CP partners identify, assess and address policy and programming gaps that may undermine Canada's CP capacity. Global Affairs Canada chairs the Counter-Proliferation Operations Committee, through which CP partners work together to address specific proliferation threats with a

Canadian nexus. FINTRAC is a member of the Operations Committee, and as per PCMLTFA s.55.1(1)(a), is able to disclose designated financial information to the Canadian Security Intelligence Service (CSIS) when it has reasons to suspect that it would be relevant to investigations of threats to the security of Canada, which includes proliferation activities. FINTRAC can also disclose information on threats related to proliferation to the appropriate police force and the CBSA if separate statutory thresholds are met.

Weighting and Conclusion:

Canada has a number of standing committees, task forces and other mechanisms in place to coordinate domestically on AML/CTF policies and operational activities.

Canada is compliant with R.2.

Recommendation 3 - Money laundering offense

Canada was rated LC with former R.1 and 2 based on a number of shortcomings. The range of predicate offenses was slightly too narrow and for one part of the ML offense the *mens rea* requirement was not in line with the FATF standard. Since 2008, the range of predicate offenses for ML was expanded to include tax evasion, tax fraud, and copyright offenses.

***Criterion* 3.1**— ML activities are criminalized through Criminal Code (CC), ss.354 (possession of proceeds), 355.2 (trafficking in proceeds), and 462.31 (laundering proceeds). *Conversion or Transfer:* CC, s.462.31 criminalizes the use, transfer, sending or delivery, transportation, transmission, altering, disposal of or otherwise dealing with property with the intent to conceal or convert the proceeds and knowing or believing that all or part of that property or proceeds was obtained or derived directly or indirectly as a result of a predicate offense. S.462.31 falls somewhat short of the FATF standard due mainly because the perpetrator must intend to conceal or convert the property itself rather than the illicit origin thereof. Additionally, no alternative purpose element of "helping any person who is involved in the commission of a predicate offense to evade the legal consequences of his or her action" is provided for. S.355.2 criminalizes many of the same acts as s.462.31 but without setting out any specific intent requirement. However, the Supreme Court in *Canada in R. v. Daoust, 2004, 1 SCR 217, 2004 SCC 6 (CanLII)* held that "the intention of parliament was to forbid the conversion pure and simple, of property the perpetrator knows or believes is proceeds of crime, whether or not he tries to conceal it or profit from it." *Acquisition, possession or use:* Ss.354 and 355.2. criminalize the sole or joint possession of or control over (s.354) and the selling, giving, transferring, transporting, exporting or importing, sending, delivering or dealing with in any way (s.355.2) of property or things that the person knows were obtained or derived directly or indirectly from an indictable offense. Neither provision explicitly refers to the "acquisition or use," but such acts would be covered by "control over proceeds" in s.354 and the various material elements under s.355.2. *Concealment or disguise:* Under CC, s.354 it is an offense to conceal or disguise property that the perpetrator has possession of or control over, in which case liability is invoked for "possession and trafficking of proceeds." Additionally, the concealment or disguise is covered under s.355.2 and liability is for "trafficking in proceeds."

Criterion 3.2— Ss.354 and 355.2 cover acts relating to proceeds of an "indictable offense;" and s 462.31 to proceeds of a "designated offense." "Designated offense" is defined as "any offense that may be prosecuted as an indictable offense other than those prescribed by regulation". Canada's ML provisions apply to all serious offenses under Canadian law and cover a range of offenses in each FATF designated categories of predicate offenses, including tax evasion.

Criterion 3.3— All serious offenses under Canadian law, defined as offenses with a statutory sanction of imprisonment for more than six months, constitute a predicate offense for ML. As indicated in the 2008 MER, federal laws criminalize a range of serious offenses under each FATF designated categories of predicate offenses.

Criterion 3.4— Ss.354, 355.2, and 462.31 apply to any property or proceeds of property obtained or derived, directly or indirectly, from the commission of an indictable offense. No value threshold applies. "Property" is defined under s.2 of the CC to include real and personal property of every kind and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, including converted or exchanged property. The definition covers material and immaterial, tangible and intangible, and corporeal and incorporeal property as well as interest in such property.

Criterion 3.5— The legal provisions do not require a conviction for a predicate offense to establish the illicit source of property. Case law further confirmed this principle. [100]

Criterion 3.6— The text of ss.354, 355.2 and 462.31 apply the relevant offenses to indictable offenses committed in Canada and to any act or omission committed abroad that would have constituted an indictable offense had it occurred in Canada.

Criterion 3.7— Nothing in the relevant provisions prevent their application to the person who committed the predicate offense. Canadian case law supports the notion that the ML provisions can also be applied to the person who committed the predicate offense.[101]

Criterion 3.8— As a general rule, Canada allows for the intentional element of criminal offenses to be inferred from objective factual circumstances and based on credible, admissible and relevant circumstantial evidence. This principle has been confirmed through case law in multiple instances, as indicated in the 2008 MER.[102]

Criterion 3.9— Offenses pursuant to s.354 are punishable with imprisonment for up to ten years (if the value of the property exceeds CAD 5 000) or for up to two years (if the value of the property is less than CAD 5 000). S.355.5 applies the same value thresholds but set out slightly stricter sanctions of imprisonment for up to 14 years or up to five years, respectively. S.462.31 provides for a statutory

[100] United States of America and the honorable Allan Honourable Allan Rock, Minister of Justice for Canada v. Dynar, 1997, 2 SCR 462, 1997, CanLII 359 (SCC); R.c.Chun, 2015 QCCQ 2029 (CanLII); and R.c. Lavoie, 1999 CanLII 6126 (QCCQ).
[101] R. v. Tortine, 1998, 2 SCR 972, 1993 CanLII 57 (SCC); and R. v. Trac at R. v. Trac, 2013 ONCA 246 (CanLII).
[102] Manitoba Court of Appeal in R. v. Jenner (2005), 195 CCC (3d) 364 at para 20; and Ontario Court of Appeal in R. v. Aiello (1978), 38 CCC (2d) 485 affirmed 46 CCC (2d) 128n SCC at page 488.

sanction of imprisonment for up to ten years, regardless of the amounts involved. The statutory sanctions may be increased or reduced pursuant to CC, s.718.2 based on aggravating or mitigating circumstances. CC, s.718.1 requires that the sanction in all cases be proportionate to the gravity of the offense and the degree of responsibility of the offender. The statutory sanctions are considered to be both dissuasive and proportionate.

Criterion 3.10— Legal entities may be subject to criminal liability and be held criminally responsible for ML. Pursuant to CC, s.735 (1) a legal entity, partnership, trade union, municipality or association convicted of an indictable offense is liable to a fine with the relevant amount being determined by the court. In determining the relevant sanction, s.718.21 stipulates that factors such as the advantage realized, the degree of planning involved in carrying out the offense, whether the organization has attempted to conceal its assets or convert them to avoid restitution; and any regulatory penalty imposed shall be taken into account. CC, s.718.1 requires that a sentence must in all cases be proportionate to the gravity of the offense and the degree of responsibility of the offender. Given the wide discretion the court has in determining the sanction, the statutory sanctions are considered to be dissuasive and proportionate. Parallel civil or administrative sanctions may be applied in addition to the criminal process.

Criterion 3.11— Ancillary offenses are criminalized in the general provisions of the CC (s.24— Attempt; s.21 (1)—aiding and abetting; s.21 (2)—conspiracy to commit; s.22— counselling, procuring, soliciting or inciting to commit; s.23—accessory after the fact).

Weighting and Conclusion:

Canada is compliant with R.3.

Recommendation 4 - Confiscation and provisional measures

Canada was rated LC with former R.3.

Criterion 4.1— CC, s.462.37 (1) provides for the permanent forfeiture of proceeds of crime based on a conviction for a designated offense. CC, s.490.1 (for all crimes) and Controlled Drugs and Substances Act (CDSA), ss.16 and 17 set out similar forfeiture provisions in relation to property used or intended to be used for the commission of an indictable offense. In all cases, the court will consider forfeiture based on the application by the Attorney General. In the context of convictions for participation in a criminal organization or offenses under the CDSA, extended forfeiture orders may be granted for material benefits received within 10 years before commencement of the proceedings and income from sources that cannot be reasonably accounted for. In a standalone ML case, CC, s.462.37(1) allows for the confiscation of the proceeds of the laundering activity as well as the property laundered, although for the latter a stricter standard of proof would apply. CC, ss.462.37 (1) and 490.1 allow for forfeiture of property from a third party. In cases where the accused has died or absconded, forfeiture *in rem* is available under ss.462.38 and 490.2.

Equivalent value confiscation is not permitted. CC, s.462.37(3) provides for the issuance of a fine in lieu of forfeiture in cases where the court determined that a forfeiture order under CC, s.462.37 cannot be made in respect of any property. While the issuance of a fine may result in the same outcome as an equivalent value confiscation, from a legal point of view the concept of a fine cannot substitute equivalent value confiscation.

Criterion 4.2— The CC and CDSA set out a wide range of measures including search and seize warrants pursuant to CC, ss.487, 462.32 and 462.35 and CDSA, s.11; production orders pursuant to CC, s.487.018 regarding the existence of bank accounts; production orders pursuant to CC, ss.487.014 and 487.015; warrants for transmission of data including computer and telecommunication program recordings under CC, s.492.2; general information warrants under CC, s.487.01 and tax information orders under CC, s.462.48. The power under CC, s.487.01 to "use any device, investigation technique or procedure or do anything described in the warrant" is sufficiently broad to also cover account monitoring, In addition, PCMLTFA, s.23 allows for the seizure and forfeiture of cash or bearer-negotiable instruments for violations of the cross border declaration obligation. Seizing and restraint warrants to secure property or instrumentalities for forfeiture are available under CC, ss.462.33 and 490.8 and CDSA, s.14. Seizing and restraint orders may be issued based on reasonable grounds to believe that a forfeiture order will be made in regards to the relevant property. In both cases, the judge may opt to apply provisional measures ex parte and without prior notice. CC, ss.490.3 and 462.4 permit the judge to void any conveyances of transfers unless the transfer was for valuable consideration to a bona fide third party. Prior to the issuance of a seizing or restraint order, the holder of such property may become subject to criminal liability under CC, s.354(1) provided he acted knowingly. A specific forfeiture provision for property owned or controlled by a terrorist group or property that has been or will be used to carry out a terrorist activity is set out in CC, s.83.14.

Criterion 4.3— Rights of bona fide third parties are protected through CC, ss.462.42, 462.34 (b), 490.4 (3) and 490.5 (4), which allow for exclusion of certain property from a restraining, seizing, or forfeiture order.

Criterion 4.4— The Seized Property Management Act regulates the management of seized or restrained property and the disposal and sharing of forfeited property. Under the Act, the Minister of Public Works and Government Service is competent to take into custody all such property and may take any measures he deems appropriate for the effective management thereof. Forfeited property is to be disposed of and the proceeds to be paid into the Seized Property Proceeds Account. Fines paid in lieu of forfeited property and amounts received from foreign governments under asset-sharing agreements are to be credited to the Proceeds Account as well. Excessive amounts in the Account are to be credited to accounts of Canada as prescribed by the Governor in Council.

Weighting and Conclusion:

The confiscation framework has some shortcomings.

Canada is largely compliant with R.4.

Recommendation 5 - Terrorist financing offence

Canada was rated LC with former SR. II.

Criterion 5.1— TF is criminalized through CC, ss.83.02 to 83.04: S. 83.02 criminalizes the direct or indirect, wilful and unlawful collection or provision of property with the intent that the property is to be used or knowing that the property will be used to carry out a terrorist activity. CC, s.83.04 criminalizes the use of property for the purpose of facilitating or carrying out a terrorist activity, and the possession of property intending that it be used or knowing that it will be used to facilitate or carry out a terrorist activity. CC, s.83.01 defines "terrorist activity" to cover all acts which (1) constitute an offense as defined in one of the conventions and protocols listed in the Annex to the TF Convention, all of which are criminalized in Canada; and (2) any other act or omission carried out with terrorist intent.

Criterion 5.2— CC, s.83.03(a) criminalizes the direct or indirect collection or provision of property with the intent that such property is to be used or knowing that such property will be used to benefit any person who is facilitating or carrying out a terrorist activity. The offense applies also where the property is used by the financed person for a legitimate purpose. CC s.83.03(b) covers the direct or indirect collection or provision of property, knowing that such property, in whole or in part, will benefit a terrorist group. "Terrorist group" includes a person, group, trust, partnership, or fund or unincorporated associations or organizations that has as one of its purposes or activities the facilitating or carrying out of any terrorist activity. The mental element required under subsection (b) is slightly stricter than under subsection (a) as the offense only applies where the perpetrator knows that property will be used for the benefit of a terrorist group, but not where he merely intends for this to be the case. For both CC, ss. 83.03 (a) and (b) the courts have interpreted the term "facilitates" broadly to cover "any behaviour/activity taken to make it easier for another to commit a crime."[103] The term thus includes the "organizing or directing of others" to commit a terrorist activity, or the "contributing to the commission of a terrorist activity by a group of persons acting with a common purpose."

Criterion 5.3— "Property" is defined under CC, s.2 to include real and personal property of every kind and deeds and instruments relating to or evidencing the title or right to property or giving a right to recover or receive money or goods, including converted or exchanged property. CC, ss.83.01 to 83.03 are not limited in scope to financing activities involving illicit property. The source of the property used for the financing activity is irrelevant.

Criterion 5.4— CC, s.83.02 implies that the financing offense can also be applied in cases where a person collects or provides property merely with the intention to finance a specific terrorist activity. Thus, it is neither required that the financed activity has been attempted or committed, nor that the money collected or provided is linked to a specific terrorist activity. CC, s.83.03(b) extends to the collection or provision of funds for the benefit of a terrorist group, regardless of the purpose for which the funds are eventually used, but does not cover financing merely with the intent to benefit

[103] R. v. Nuttall, 2015 BCSC 943 CanLII.

an individual terrorist or terrorist organization. For financing of individual terrorists, CC, s.83.03(a) applies where the financed person is facilitating or carrying out a terrorist activity at the time the financing activity takes place and CC, s.83.03(b) covers situations where the property collected or provided is known to be used by or benefit a terrorist.

Criterion 5.5— Canada allows for the intentional element of criminal offenses to be inferred from objective factual circumstances and based on credible, admissible and relevant circumstantial evidence. This principle has been confirmed through case law in multiple instances, as indicated in the 2008 MER.[104]

Criterion 5.6— The statutory sanctions for a natural person is imprisonment for up to ten years with the possibility of an increased or reduced sentence pursuant to CC, ss.718.2 and 718.21 based on aggravating or mitigating circumstances. The statutory sanctions are considered to be both dissuasive and proportionate.

Criterion 5.7— Legal entities may be held criminally responsible for terrorism financing. Pursuant to CC, s.735 (1) of the CC, a legal entity, partnership, trade union, municipality, or association may fine in an amount that is in the direction of the court. CC, s.718.21 stipulates that factors such as the advantage realized, the degree of planning involved in carrying out the offense, whether the organization has attempted to conceal its assets or convert them to avoid restitution; and any regulatory penalty imposed shall be taken into account by the court. CC, s.718.1. CC further requires that the sentence be proportionate to the gravity of the offense and the degree of responsibility of the offender. Given the wide discretion by court in determining the sanction, the statutory sanctions are dissuasive and proportionate. Parallel civil or administrative sanctions may be applied.

Criterion 5.8— Ancillary offenses are criminalized in the general provisions of the CC (s.24—Attempt; s.21 (1)—aiding and abetting; s.21 (2)—conspiracy to commit; s.22—counselling, procuring, soliciting or inciting to commit; s.23—accessory after the fact). s.83.03 criminalizes inviting another person to provide or make available property for TF and ss.83.21 and 83.22 to knowingly instruct, directly or indirectly, any person to carry out an activity for the benefit of, at the direction of or in association with a terrorist group for the purpose of enhancing the ability of that group to facilitate or carry out a terrorist activity.

Criterion 5.9— Canada takes an all crimes approach to defining predicate offenses for ML. TF is, thus, a predicate offense for ML.

[104] Manitoba Court of Appeal in R. v. Jenner (2005), 195 CCC (3d) 364 at para. 20; and Ontario Court of Appeal in R. v. Aiello (1978), 38 CCC (2d) 485 affirmed 46 CCC (2d) 128n SCC at page 488.

Criterion 5.10— CC, ss.83.02 and 83.03 apply regardless of whether the underlying terrorist activity is committed inside or outside Canada, or whether the terrorist group or financed person is located inside or outside Canada.

Weighting and Conclusion

TF is set out as a separate criminal offense that covers all aspects of the offense set out in the Terrorism Financing Convention, with minor shortcomings.

Canada is largely compliant with R.5.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

Canada was rated LC with former SR. III. For certain FIs and other persons or entities that may hold targeted funds the assessors found that the names of designated persons and entities were not effectively communicated, the guidance issued was not sufficient and the implementation of the relevant legal provisions was not effectively monitored. The framework for the implementation of the TF-related targeted financial sanctions remains substantially unchanged. A new Security of Canada Information Sharing Act was adopted in 2015 to facilitate the sharing of information between Canadian government agencies with regards to any activity that undermines the security of Canada, including terrorism.

Identifying and Designating

Under United Nations Act, s.2, the Governor in Council may issue regulations to give effect to decisions and implement measures decided by the UNSC pursuant to Article 41, Chapter VII of the UN Charter. Two Regulations were issued on this basis—the *United Nations Al-Qaida and Taliban Regulations* (UNAQTR) and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST). In 2001, Canada enacted an additional domestic terrorist listing procedure under CC, ss.83.05 to 83.12 in addition to the RIUNRST. Over time, the listing mechanism under the CC has become the primary domestic listing regime and consequently no listings have been added to the RIUNRST since 2006. The Security of Canada Information Sharing Act facilitates implementation of the mechanisms by allowing for the exchange of information between government agencies with regards to terrorism, either spontaneously or upon request.

Criterion 6.1— *Sub-criterion 6.1a*—Department of Foreign Affairs, Trade and Development Act, s.10(2)(b) assigns responsibility to the Minister of Foreign Affairs for all communications between Canada and international organizations, including for proposing designations under UNSCR 1267/1989 or 1988 to the relevant UN Sanctions Committees.

Sub-criterion 6.1b—Based on the above mentioned s.10(2)(b), the Minister of Foreign Affairs identifies, reviews and proposes individuals or entities for designation, in consultation with an interdepartmental committee of security and intelligence officials. The interdepartmental committee on average meets once a month to discuss all listing regimes.

Sub-criterion 6.1c—The authorities stated that the identification process outlined above is based on a standard of "reasonable grounds to believe" and that a criminal conviction was not necessary for proposing the designation of an entity or individual to the UN. In the absence of any written procedures on this point, the assessors were not in a position to verify the authorities' view.

Sub-criterion 6.1d—Canada supports co-designation and co-sponsorship and its experience in proposing designations was so far limited to cosponsoring proposals for designations. To propose designations, Canada would use the UN standard forms and follow the procedures outlined under UNSCR's 2160 and 2161 (2014) and the relevant Sanctions Committee Guidelines.

Sub-criterion 6.1e—The authorities stated that Canada would provide as much relevant information to support a proposal for designation as possible, including identifying information and a statement of case.

Criterion 6.2— *Sub-criterion 6.2a*—Canada implements UNSCR 1373 through two distinct mechanisms: (i) for terrorist groups, CC, s.83.05 grants the Governor in Council the authority to list, on the basis of a recommendation by the Ministry of Public Safety Canada, a person, group, trust, partnership or fund or unincorporated association or organization. Requests for designation from another country can also be considered under the CC process; (ii) the RIUNRST designates the Governor in Council as responsible for making designations on the basis of a recommendation by the Minister of Foreign Affairs (Article 2 RIUNRST). The Minister may recommend a designation under the RIUNRST also based on a request from another country. In practice the mechanisms under the CC is the main one and no listings have been added to the RIUNRST since 2006.

Sub-criterion 6.2b—The CC and RIUNRST include mechanisms for identifying targets for designation and to decide upon designations based on clearly stipulated criteria in line with the designation criteria under UNSCR 1373.

Sub-criterion 6.2c—Foreign requests for designations are processed the same way as domestic designations. As a first step, authorities ensure that a request for listing is supported by verified facts that meet the legal threshold. Verification includes both factual and legal scrutiny. After verification is completed, the proposed listing is presented to the Cabinet and the relevant Minister recommends to the Governor in Council that the foreign request be granted. Authorities stated that the process takes on average six months but can be expedited, if necessary.

Sub-criterion 6.2d—The Governor in Council takes the decision to designate based on "reasonable grounds to believe" that a person meets the designation criteria in CC or the RIUNRST, independently from any criminal proceedings.

Sub-criterion 6.2e—The authorities stated that when making 1373 request to other countries, as much identifying information as possible would be provided to the requesting country to allow for a determination that the reasonable basis test is met Canada stated that it is in regular contact with its allies to discuss potential listings and notifies G7 partners prior to any domestic listing.

Criterion 6.3— The Canadian Security Intelligence Service Act s. 12 grants the CSIS the power to collect and analyse information on activities that may threaten Canada's security and to report and advise the government of any such activities. The Security of Canada Information Sharing Act, s.5 further allows government agencies to share such information. In the context of a criminal suspicion or the designation procedure under CC, s.83.05 the authorities may also collect information under criminal procedures. The outlined measures may in all cases be applied *ex parte* to avoid tipping off.

Freezing

Criterion 6.4— The UNAQTR, CC and RIUNRST set out a wide range of prohibitions to deal with property of or provide financial services to designated persons. The prohibitions apply as soon as any person is designated by the competent UN Sanctions Committee (for UNSCR 1267/1989 or 1988) or is added to the Regulations Establishing a List of Entities pursuant to the CC or is included in Schedule 2 to the RIUNRST (for UNSCR 1373). The prohibitions apply without delays, as soon as a person has been designated by the UN (for UNSCR 1267 and 1988) or was added to the domestic list. The term "person" covers both natural and legal persons.

Criterion 6.5— No authority has been designated for monitoring compliance by FIs and DNFBPs with the provisions of the UNAQTR, CC, and RIUNRST. Sanctions for violations of the Regulations are available but have never been applied in practice.

Sub-criterion 6.5a—The UNAQTR, CC and RIUNRST prohibit that any person or entity in Canada or any Canadian outside Canada knowingly deals with; provides financial or other services to; or enters into or facilitates any financial transaction involving funds or property of a designated person. The prohibition applies as soon as a person is listed and covers all aspects of the freezing obligation, thus also without prior notice.

Sub-criterion 6.5b—The UNAQTR, RIUNRST, and CC target funds or property owned or controlled, directly or indirectly, by any designated person or by any person acting on behalf or at the direction of a designated person. In the case of the UNAQTR but not the CC, does the prohibition extend also to funds derived or generated from such property. The concepts of "ownership and control" also cover property owned and controlled jointly. The obligations under all three procedures apply to property of every kind, including any funds, financial assets or economic resources.

Sub-criterion 6.5c—The UNAQTR, the CC, and RIUNRST prohibit Canadians and any persons in Canada from making property or financial or other services available, directly or indirectly, for the benefit of a designated person (Articles 4 RIUNRST; CC, ss.83.08 and UNAQTR s.4 and 4.1. CC, s.83.03 further criminalizes the provision of property or services to a listed entity, but the prohibition does not extend the provision of services to entities owned or controlled by a designated person or persons acting on behalf or at the discretion of a designated person.

Sub-criterion 6.5.d—Canada makes public all designations under all three listing regimes on government websites and through notification services. FRFIs have the option of signing up to receive information notices regarding list changes from OSFI and/or directly from the 1267 Al-Qaida

Sanctions Committee and the 1988 Taliban Sanctions Committee. OSFI receives a note verbale from the 1267 Al-Qaida Sanctions Committee and the 1988 Taliban Sanctions Committee in advance of a formal press release (i.e. before the Committees lists the entities publically). OSFI sends out email alerts to those entities that subscribe to its email notifications of any changes to the lists the same day or subsequent day from receiving the note verbale. However, if there are extensive changes to the lists, this process can be delayed by two weeks. The UN 1267 Al-Qaida Committee and 1988 Taliban Sanctions Committee also notify all email subscribers, which can include FIs or any persons, of new listings and de-listings the same day or the next UN business day. REs are informed without delay of any entities listed under the CC and RIUNRST. When an entity becomes listed pursuant to the CC, a notice is published in the *Canada Gazette*, which constitutes official public notice of the listing. These changes are also included in OSFI's email notifications. Public Safety also issues a news release for all new listings and de-listings, and both Public Safety and OSFI include information on its websites.

Sub-criterion 6.5.e—Banks, cooperative credit societies, savings and credit unions, and insurance companies are required to determine, on a continuous basis, whether they are in possession of targeted funds or property and must regularly report this and any associated information to the competent supervisory authority (OSFI or FINTRAC depending on whether it is a FRFI or not). A more general obligation applies to any person in Canada and any Canadian outside Canada to report to the RCMP or the CSIS transactions or property believed to involve targeted funds.

Sub-criterion 6.5.f—The CC and the RIUNRST both prohibit persons from "knowingly" dealing with listed entities. Third parties acting in good faith are thus protected in that they would not be covered under these obligations. The CC further clarifies that any person who "acts reasonably in taking, or omitting to take, measures to comply" with the relevant obligations shall not be liable in any civil action if they took all reasonable steps to satisfy themselves that the relevant property was owned or controlled by or on behalf of a terrorist group. The procedures under the UNAQTR, the RIUNRST and the CC for delisting and access to frozen funds also apply to protect bona fide third parties.

De-Listing, Unfreezing and Providing Access to Frozen Funds or other Assets

Criterion 6.6— The UNAQTR, CC and RIUNRST set out mechanisms for the delisting of persons or entities that do not meet the designation criteria (respectively in UNAQTR, ss.5.3. and 5.4.; CC, ss.83.05(5) and 2.1., and RIUNRST, s.2.2). Both Regulations and the CC are published in the official Gazette and the relevant procedures are thus "publicly known." CC, s.85.05(9) requires the Minister of Public Safety and Emergency Preparedness to review the list of entities every two years to determine whether there are still reasonable grounds for the entities to remain listed. The Minister can recommend to the Governor in Council at any time that an entity be delisted, either as part of the review process or upon application by the listed entity. Information on delisting processes is also set out at www.international.gc.ca/sanctions/countries-pays/terrorists-terroristes.aspx?lang=eng.

Sub-criterion 6.6.a—Under the UNAQTR, the Minister based on written receipt of a motion to delist under s 5.3 decides whether to forward a petition for delisting to the UN. The Minister's submission must be in accordance with guidance issued by the relevant UN Sanctions Committee. The possibility

of a judicial review of the Minister's decision is provided for under s.5.4. Procedures to unfreeze funds of de-listed entities are not available but the obligations under the UNAQTR automatically cease to apply once a person is removed from the UN's list.

Sub-criterion 6.6.b—The delisting procedures under the CC and RIUNRST are similar to those under the UNAQTR insofar as a listed entity may apply in writing to the relevant Minister to request to be removed from the list. Upon receipt of a written application for delisting from the relevant Minister, it has 60 days to determine whether there are reasonable grounds to recommend a delisting to the Governor in Council. The applicant can seek a judicial review of this decision.

Sub-criterion 6.6.c—Judicial review of the listing decision is available upon receipt of a motion to delist.

Sub-criterion 6.6d and 6.6e—UNAQTR, s.5.3 provides Canadians and any residents of Canada the option to apply to the Minister to be delisted from the 1988 or 1267 sanctions lists in accordance with the Guidelines of the 1988 and 1267 Sanctions Committees.

Sub-criterion *6.6f*—Pursuant to UNAQTR, s.10 and RIUNRST, s.10 a person claiming not to be a listed entity may apply to the Minister of Foreign Affairs for a certificate stating that the person is not a listed entity. The Minister then has a specific period of time to issue the certificate if it is established that the individual is not a listed entity. CC, s.83.07 allows an entity claiming not to be a listed entity to apply to the Minister of Public Safety and Emergency Preparedness for a certificate stating that it is not a listed entity.

Sub-criterion 6.6.g—Any changes to designations under the UNAQTR, CC or RIUNRST result in the publication of an updated Schedule to the relevant Regulation. For changes to the 1267/1988 lists, FIs and DNFBPs can subscribe to an automatic notification system. OSFI also notifies those entities that have subscribed to its email list of any changes to any of the three listing regimes.

Criterion 6.7— The Minister of Foreign Affairs or the Minister of Public Safety and Emergency Preparedness (for the CC) may grant a person access to frozen funds to cover basic or extraordinary expenses pursuant to UNAQTR, s.10.1, CC, s.83.09 or RIUNRST, s.5.7. Under the UNAQTR, the Minister must notify (for basic expenses) or obtain authorization from (for extraordinary expenses) the relevant UN Sanctions Committee before he/she may grant a motion for access to frozen funds. Once granted, the Minister issues a certification exempting the relevant property or funds from the scope of the Regulations. Under UNAQTR the procedures applied by the Minister have to be in line with the requirements under UNSCR 1452 (2002).

Weighting and Conclusion

There are some shortcomings in regard to the requirements of UN Resolutions 1267, 1988, and 1373.

Canada is largely compliant with R.6.

Recommendation 7 – Targeted financial sanctions related to proliferation

R.7 includes new requirements that were not part of the previous assessment.

Criterion 7.1— Two regulations implementing targeted financial sanctions (TFS) relating to Iran and North Korea were issued under Canada's *United Nations Act*—the *Regulations Implementing the United Nations Resolutions on Iran (RIUNRI)* and the *Regulations Implementing United Nations Resolutions on the Democratic People's Republic of Korea (RIUNRDPRK)*. Both require any person in Canada and any Canadian outside Canada to implement TFS in relation to individuals or companies that have been designated by the UN under paragraph 8(d) of UNSCR 1718 (ss.7, 8, and 9 RIUNRDPRK for North Korea) or paragraphs 10 or 12 of UNSCR 1737 (ss.5, 6, 9 and 9.1 RIUNRI for Iran). Under both regulations, it is clear that the relevant prohibition applies only from the date the relevant UNSCR came into force and not retroactively. Neither regulation specifies that sanctions must be applied "without delay" but the relevant obligations and prohibitions apply as soon as a person or entity is included in the UN's list of designated persons, and the communication procedures described under criterion 7.2(d) are sufficient that new listings are brought to the attention of the public. The Security of Canada Information Sharing Act facilitates the implementation of the two regulations by allowing for the exchange of information between government agencies with regards to proliferation of nuclear, chemical, radiological, or biological weapons, either spontaneously or upon request.

Criterion 7.2— Under UN Act, s.2 the Governor in Council issues regulations to give effect to decisions and implement measures decided by the UN Security Council (UNSC) pursuant to Article 41, Chapter VII of the UN Charter. Section 9 of the RIUNRDPRK and RIUNRI impose freezing obligations by prohibiting any person in Canada and any Canadian outside Canada from dealing with; or entering into or facilitating any financial transaction relating to; or providing financial or other related services in relation to property owned or controlled directly or indirectly by a designated person or by a person acting on behalf or at the direction of a designated person.

Sub-criterion 7.2.a—The legal prohibitions are triggered without delay as soon as a person is designated by the UN.

Sub-criterion 7.2b—The above-mentioned prohibitions apply to property owned or controlled by a designated person, including those owned or controlled jointly, or by a person acting on behalf or at the direction of a designated person.

Sub-criterion 7.2c—Under both regulations it is an offense to make property or any financial or other related services available, directly or indirectly, for the benefit of a designated person. Article 3 of the UN Act prescribes sanctions of a fine of up to CAD 100 000 or imprisonment for not more than two years or both (upon summary conviction); or to imprisonment for a term of not more than 10 years (upon conviction on indictment).

Sub-criterion 7.2d—The communication procedures described in criterion 6.5d are also applicable in the context of the RIUNRI and RIUNRDPRK. Canada publishes new designations in the public Canada

Gazette as well as on government websites and through notification services. The Ministry of Foreign Affairs has issued guidance for both sanction regimes.[105]

Sub-criterion 7.2e—All FRFIs and casualty insurance companies, savings and credit unions, and other provincially regulated FIs are required to determine, on a continuous basis, whether they are in possession of targeted funds or property and must freeze such property and regularly report this and any associated information to the competent supervisory authority (ss.11 RIUNRI and RIUNRDPRK). More general obligations apply to any person in Canada and any Canadian outside Canada to report to the RCMP or the CSIS transactions or property believed to involve targeted funds.

Sub-criterion 7.2f—The RIUNRI and RIUNRDPRK prohibitions apply only in cases where a person acts "knowingly." Bona fide third parties acting in good faith are, therefore, protected.

Criterion 7.3— Apart from the notification system outlined, under criterion 7.2.e, Canada does not have a mechanism in place for monitoring compliance by FIs and DNFBPs with the provisions of the RIUNRI and RIUNRDPRK. Sanctions for violations of the Regulations are available, but have never been applied in practice.

Criterion 7.4— Global Affairs Canada provides guidance on its homepage on the procedures and content of the RIUNRI and RIUNRDPRK.[106] While the homepage provides information that needs to be submitted as part of an application to the Minister for delisting, it does not give information on the procedures applied by the Minister to submit delisting requests to the UN on behalf of a designated person or entity.

Sub-criterion 7.4.a—Neither the Regulations nor the Global Affairs' homepage provide information on the availability of the UN Focal Point as a direct or indirect way to effect a delisting.

Sub-criterion 7.4.b—Claims of false positives can be filed with and granted by the Minister under RIUNRDPRK, s.14 and RIUNRI, s.16. *Sub-criterion 7.4.c*—RIUNRDPRK, s.15 and RIUNRI, s.17 further provide for the possibility for the Minister to grant access to frozen funds subject to the conditions and procedures set out in UNSCR 1718 and 1737.

Sub-criterion 7.4.d—FIs and DNFBPs can subscribe to the UNs automatic notification system found on its website. OSFI also notifies those entities that have subscribed to its email list of any changes to any of the three listing regimes. Detailed guidance on the provisions of the RIUNRI and RIUNRDPRK is provided on the Global Affairs' homepage.

Criterion 7.5— Neither Regulation allows for additions to frozen accounts but the Minister may permit such additions on the basis of a one-off exemption. Payments from frozen accounts are

[105] Global Affairs Canada (nd), Canadian Sanctions Related to Iran, www.international.gc.ca/sanctions/countries-pays/iran.aspx?lang=eng; Canadian Sanctions Related to North Korea, www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.
[106] See footnote 16.

permitted under the circumstances set out in relevant UNSCRs based on RIUNRI, s.19 and RIUNDPRK, s.15.

Weighting and Conclusion

There are minor shortcomings in regard to the implementation of the RIUNRI and RIUNRDPRK.

Canada is largely compliant with R.7.

Recommendation 8 – Non-profit organisations

Canada was rated LC with former SR. VIII, with only one deficiency having been identified regarding coordination amongst competent domestic authorities.

Criterion 8.1— *Sub-criterion 8.1.a*—The adequacy of laws and regulations relating to NPOs is reviewed on an ongoing basis and has recently resulted in amendments of various laws and regulations.

Sub-criterion 8.1.b—Canada has carried out a risk assessment of its NPO sector and determined that registered charities pose the greatest risk of TF in Canada and, thus, shall fall within the functional definition of "non-profit organization" as defined under the FATF standard. Canada's risk mitigation efforts are primarily focused on registered charities.

The NRA, which focuses on inherent risk, indicates that both for domestically and internationally operating charities, it may be difficult in practice to determine the origin or ultimate use of funds. In addition to the NRA, the CRA in 2015 conducted a comprehensive review of the entire NPO sector. Other relevant studies and reviews include the Canadian Non-Profit and Voluntary Sector in Comparative Perspective in March 2005; the Canada Survey on Giving, Volunteering and Participating in 2010; and the CRA's Non-Profit Organization Risk Identification Project, all of which provide insight into the way NPOs are organized and operate in Canada. All registered charities, regardless of the value of their assets, as well as non-charitable NPOs with assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000, must file an annual Information Return with the CRA, which includes information about their activities, assets and liabilities, and the amount of money received during the fiscal period in question. Incorporated NPOs are subject to additional filing obligations pursuant to the relevant statutes. NPOs must indicate whether they carry out activities outside of Canada (and specify where) and disclose the physical location of their books and records. Through information provided in these returns, the CRA has the capacity to obtain timely information on the activities, size and relevant features of the NPO sector and to identify those NPOs that are particularly at risk of abuse by virtue of their activities or characteristics.

Sub-criterion 8.1.c—The efforts described under the previous sub-criteria are ongoing and continuously integrate new information on the sector's potential vulnerabilities.

Criterion 8.2— Awareness raising events are focused on registered charities as those are the organizations that fall within the FATF definition of NPOs. The CRA is undertaking efforts to increase awareness amongst registered charities of terrorism financing risks and vulnerabilities, including on international best practices for mitigating terrorism financing risks in the charities sector, sound governance, accountability procedures, transparency reporting, as well as consultative processes and presentations by senior management. The CRA also maintains a grants program to motivate and reward the development and application of innovative compliance programs amongst charities. Many of these activities include a TF component.

Criterion 8.3— Canada imposes comprehensive registration and regulatory requirements on charities under the Income Tax Act (ITA). Other NPOs may operate without being subject to any registration requirements, but are subject to record-keeping obligations on their stated purpose, administration, and management pursuant to the federal or provincial legislation under which they were established. In addition, all registered charities, regardless of the value of their assets, and all NPOs with assets in excess of CAD 200 000 or annual investment income exceeding CAD 10 000 must file an annual information return with the CRA. Based on the information provided by the authorities, it is estimated that as of December 2014, a total of 180 000 NPOs existed in Canada of which 86 000 or about 50%, were registered under the ITA. Under the ITA, a failure by a registered charity to comply with the registration requirements, including links to terrorism, may result in denial or revocation of registration. Under the Charities Registration (Security Information) Act the CRA may utilize all information available to determine the existence of terrorism links for new applications or existing registrations, including security or criminal intelligence and otherwise confidential information. Once registered, charities are required to file annual information returns and financial statements, including information on the directors and trustees, the location of activities, the charity's affiliation and the organization's name. Much of the information is made publicly accessible on the CRA's homepage. Donations, spending and record keeping are regulated under the ITA. The CRA is granted wide powers under Part XV of the ITA to administer and enforce the provisions of the law. The CRA is responsible for ensuring compliance by registered charities with the requirements under the ITA and to sanction non-compliance. In addition, law enforcement and intelligence authorities monitor NPOs and investigate those suspected of having links to terrorism.

Criterion 8.4— Based on the information provided by the authorities, it is estimated that as of December 2014 a total of 180 000 NPOs existed in Canada of which 86 000 or about 50%, were registered under the ITA. According to the CRA's NPO Sector Review of 2015, the 86 000 registered charities represent 68% of all revenues of the NPO sector and nearly 96% of all donations. CRA registered charities also account for a substantial share of the sector's foreign activities as about 75% of internationally operating NPOs are registered as charities.

Sub-criteria 8.4.a and b—Charities registered under the ITA have comprehensive annual filing obligations, including on their directors and trustees, and financial statements including balance sheets and income statements. All this information is publicly available at the CRA's webpage.

Sub-criterion 8.4.c—All registered charities, regardless of their assets, and all other types of NPOs with revenue in excess of CAD 200 000, and/or annual investment income exceeding CAD 10 000, must file an annual information return with the CRA, including financial information. In addition, registered charities with revenue in excess of CAD 100 000 and/or property used for charitable activities over CAD 25 000 and/or that have sought permission to accumulate funds, must provide financial information. CRA-Charities must ensure that charities' funds are fully accounted for by reviewing and conducting analysis of information submitted in the annual information return. Where there are irregularities or concerns CRA-Charities may conduct an audit to review charity's finances and activities in detail.

Sub-criterion 8.4.d—Registration with the CRA is optional, not mandatory.

Sub-criterion 8.4.e—ITA registered charities are required to know intermediaries that provide services on its behalf, and to ensure that charity funds are used only for charitable activities. As such, there is an obligation to know enough about beneficiaries to meet this obligation. NPOs can be held liable for acts by associated NPOs if the court finds that there is an agency relationship between the two, which provides an additional incentive for NPOs to know associate NPOs. Records of registered charities must be sufficient for the CRA to verify that the charity's resources have been used in accordance with its activities.

Sub-criterion 8.4.f—Comprehensive record-keeping obligations apply both for ITA registered charities and other types of NPOs based on the provisions of provincial or federal legislation.

Criterion 8.5— As part of their annual information return charities must provide a breakdown of financial information related to revenue and expenditures. This includes information on the total expenditures for charitable activities, management and administration, and gift to qualified donees. Charities must also report ongoing and new charitable programs. Where audits reveal financial irregularities, the CRA may apply a range of sanctions set out in the ITA. The CRA is granted a wide range of powers to monitor registered charities for compliance with the filing obligations under the ITA and to apply sanctions, including financial penalties and suspensions, or revocation of registration.

Criterion 8.6— *Sub-criterion 8.6.a*—For registered charities, the registration system under the ITA is supported by the Charities Registration (Security Information) Act which allows the Minister of Public Safety and Emergency Preparedness to take into account criminal and security intelligence reports on registered charities or those applying for registration. The CSIS and also the RCMP and CBSA contribute information to these criminal and security intelligence report. The CRA has entered into MOUs with the CSIS and RCMP to facilitate the process. Any suspicion that a specific charity is linked to terrorism may result in registration being denied or revoked.

Sub-criterion 8.6.b—For ITA registered charities, the CRA may share certain information about registered charities with the public, including foreign counterparts, online through the CRA's website, or upon request. Information that is publicly accessible, includes governing documents, the name of directors or trustees, annual information returns and financial statements.

Sub-criterion 8.6.c—For non-publicly available information, the ITA allows but does not oblige the CRA to disclose to FINTRAC as well as the RCMP and CSIS information about charities suspected of being involved in FT. Equally, the Security of Canada Information Sharing Act (SCISA) permits the CRA to share any taxpayer information relevant to a terrorism offense (under part II of the CC) or threats to the security of Canada (under the CSIS Act) with competent authorities, including any information that the CRA may have on the broader sector of NPOs. FINTRAC is required under the PCMLTFA to disclose information to the CRA with regards to registered charities. Additional information sharing powers are available under the Security of Canada Information Sharing Act whenever there is a threat to Canada's national security. For NPOs other than registered charities regular investigative and information-gathering powers under the criminal procedure code are available to obtain records and information, they are required to maintain under provincial or federal NPO legislation.

Criterion 8.7— The CRA may share certain information about registered charities with foreign counterparts, including governing documents, the names of directors or trustees, annual information returns, and financial statements. Additional information may be shared by the CRA with foreign tax authorities. If required, information on registered charities or NPOs may also be shared by FINTRAC and the RCMP as described under R.40 or based on formal MLA. In sum, Canada is found to have appropriate points of contact and procedures in place to respond to international request for information sharing regarding particular NPOs.

Weighting and Conclusion:

Canada is compliant with R.8.

Recommendation 9 – Financial institution secrecy laws

In its 2008 MER, Canada was rated C with R.4, and neither the relevant laws nor the applicable FATF R. have subsequently changed. The MER assessors' only concern was that data protection law implementation was subject to excessively strict interpretations that might prevent LEAs accessing information in the course of investigations.

Criterion 9.1— Various constitutional and legal provisions impose confidentiality obligations over personal information and individuals' privacy. In particular, s.8 of the Canadian Charter of Rights and Freedoms (which forms part of Canada's Constitution) provides that everyone has the right to be secure against unreasonable search and seizure. According to the Supreme Court of Canada, the purpose of s.8 is to protect a reasonable expectation of privacy. Accordingly, those who act on behalf of a government, including LEAs and supervisors, must carry out their duties in a fair and reasonable way. Canada also has two privacy laws: the Privacy Act covers the personal information-handling practices of federal government departments and agencies; and the PIPEDA is the main federal private-sector privacy law.

PIPEDA, s.5 notably contains specific obligations concerning organizations' collection, dissemination and use of customers' personal information. Every province and territory has its own public-sector

legislation and the relevant provincial act applies to provincial government agencies (in lieu of the Privacy Act). Some provinces also have private-sector privacy legislation. Alberta, British Columbia and Québec notably have legislation that have been declared "substantially similar" to the PIPEDA and apply to private-sector businesses that collect, use and disclose personal information while carrying out business within these provinces. Finally, several federal and provincial sector-specific laws also include provisions dealing with the protection of personal information: The federal Bank Act, in particular, contains provisions regulating the use and disclosure of personal financial information by FRFIs (ss.606 and 636 (1)); and most provinces also have laws governing credit unions that require the confidentiality of information related to members' transactions.

Various provisions also govern the authorities' access to information: of the PIPEDA, s.7(3)(d), in particular, provides that an organization may, without the individual's knowledge or consent or judicial authorization, disclose personal information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed and the information is used for the purpose of investigating that contravention. The "substantially similar" laws in Alberta, British Columbia and Quebec contain broadly equivalent provisions. The PCMLTFA also contains a number of provisions that enable FINTRAC to access information (ss.62-63) and the Bank Act (ss.643-644) and equivalent provisions governing other FRFIs gives OSFI powers to access all records of FRFIs.

As regards sharing of information between competent authorities, implementation of the Privacy Act, which obliges federal government departments and agencies to respect privacy rights, does not seem to have caused AML/CFT problems. The PCMLTFA (ss.55, 55.1, 56 and 65(1) and (2)) empowers FINTRAC to disclose information to a range of law enforcement and other competent authorities within Canada in specified circumstances. Similarly, the PCMLTFA, s.65.1(1)(a) allows FINTRAC to make agreements with foreign counterparts to exchange compliance information. The Bank Act, s 636(2) also enables OSFI to disclose information to other governmental agencies.

Weighting and Conclusion:

Canada is compliant with R.9.

Recommendation 10 – Customer due diligence

In the 2008 MER, Canada was rated NC with R.5. There were numerous deficiencies, and also the CDD requirement did not cover all FIs as defined by the FATF. Subsequently, both the PCMLTFA and PCMLTFR were amended to include measures covering the circumstances in which CDD must take place. Further PCMLTFR amendments, effective from February 2014, addressed most of the remaining deficiencies.

The 2008 MER noted that the requirement to conduct CDD excluded financial leasing, factoring and finance companies. The Sixth FUR (2014) concluded that the set of sectors not covered by the AML/CFT regime and not yet properly risk assessed was not a major deficiency. Since then, Canada's NIRA assessed the ML/TF vulnerabilities of factoring, finance and financial leasing companies as medium risk, while pointing out that these entities were very small players. Sectors not covered by

the AML/CFT regime are continually evaluated to identify trends indicating a higher ML/TF risk rating. Their current exclusion from the scope of the AML/CTF regime is an ongoing minor deficiency.

Criterion 10.1— In its 2008 MER, Canada explained that, while there was no explicit prohibition on opening anonymous accounts, the basic CDD requirements on all new account holders effectively prohibited anonymous accounts. This also applied to accounts in obviously fictitious names. The legal position remains unchanged: The PCMLTFA, s.6.1, requires REs to verify identity in prescribed circumstances and s.64 of the PCMLTFR sets out the measures to be taken for ascertaining identity. However, the 2008 assessors were concerned about the absence of detailed rules or guidance for FIs' use of numbered accounts, including compliance officers having access to related CDD information. Subsequently, OSFI Guideline B-8 addressed this latter point, covering the provision of account numbering or coding services that effectively shield the identity of the client for legitimate business reasons. Thus, FRFIs should ensure that they had appropriately ascertained the identity of the client and that the firm's Chief AML Officer could access this information. Consequently, this deficiency has been partially addressed through an adequate control mechanism, for FRFIs only, albeit not by enforceable means. This is a relatively minor matter.

When CDD is Required

Criterion 10.2— PCMLTFR ss.54, 54.1, 55, 56, 57, 59(1), 59(2) and 59(3) of the require FIs to ascertain the identity of their clients when establishing business relations. Similarly, all REs must ascertain the identity of every client with whom they conduct an occasional large cash transaction of CAD 10 000 or more. Two or more such transactions that total over CAD 10 000, conducted within a period of 24 hours, are deemed a single transaction. CDD is required for both cross-border and domestic wire transfers exceeding CAD 1 000.

Pursuant to PCMLTFR s.53.1(1) FIs must) take reasonable measures to verify the identity of every natural person or entity who conducts, or attempts to conduct, a transaction that should be reported to FINTRAC (i.e. where there is suspicion of ML or TF). This obligation applies (s.62(5)) even when it would not otherwise have been necessary to verify identity. Also, FIs must reconfirm (s.63 (1.1) of the PCMLTFR) the client's identity where doubts have arisen about the information collected. However, this measure applies only to natural persons, not to legal persons or arrangements.

The limited application of this last measure remains a deficiency under 10.2(e).

Required CDD Measures for all Customers

Criterion 10.3— PCMLTFA, s.6.1 of the requires REs to verify the identity of a person or entity in prescribed circumstances and in accordance with the Regulations. PCMLTFR ss.64 to 66 detail the measures that REs must take to ascertain the identity of a prescribed individual, corporation and "entity other than a corporation.[107]" For individuals, acceptable identification documents include a

[107] This is not defined in the Regulations, but would include any kind of unincorporated business or legal arrangement.

birth certificate, driver's license, passport, or other similar document. For corporations, the corporation's existence is confirmed, and the names and addresses of its directors ascertained, by reference to its certificate of corporate status. However, other methods are acceptable, e.g. a record that it is required to file annually under applicable provincial securities legislation, or any other record that validates its existence as a corporation. The existence of an entity other than a corporation must be confirmed by reference to a partnership agreement, articles of association, or other similar record that ascertains its existence. These legal provisions meet the FATF standard.

Criterion 10.4— The "Third Party Determination" provisions of the PCMLTFR require FIs to determine whether their customers are acting on behalf of another person or entity. Where an account is to be used by or on behalf of a third party, the FI must collect CDD information on that third party and establish the nature of the relationship between third party and account holder.

Criterion 10.5— PCMLTFR s.11.1(1) requires FIs, at the time the entity's existence is confirmed, to obtain the following information:

For corporations, the name of all directors of the corporation and the name and address of all persons who own or control, directly or indirectly, 25% or more of the shares of the corporation;

For trusts, the names and addresses of all trustees and all known beneficiaries and settlors of the trust;

For entities other than corporations or trusts (typically, a partnership fund or unincorporated association or organization), the name and address of all persons who own, directly or indirectly, 25% or more of the shares of the entity; and

In all cases, information establishing the ownership, control, and structure of the entity.

Under the PCMLTFR, s.11.1(2), REs further need to "take reasonable measures to confirm the accuracy of the information obtained" on beneficial ownership. This requirement implies the need to use reliable sources to obtain the requisite information and the FATF standard[108] allows identification data to be obtained "from a public register, from the customer, or from other reliable sources." Also, OSFI Guideline B-8 usefully indicates that "reasonable measures" to identify ultimate beneficial owners could include not only requesting relevant information from the entity concerned, but also consulting a credible public or other database or a combination of both. This Guideline also makes clear that the measures applied should be "commensurate with the level of assessed risk."

No specific legal provisions cover beneficial ownership of personal accounts. However, the PCMLTFR, in effect, establish beneficial ownership of personal accounts: in particular, s.9 requires REs to determine whether personal accounts are being used on behalf of a third party and, for personal accounts in joint names, all authorized signatories are subject to CDD measures.

[108] FATF (2013), Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems, p. 147, www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

Criterion 10.6— PCMLTFR, s.52.1, requires every person or entity that forms a business relationship under the Regulations to keep a record of the purpose and intended nature of that business relationship. OSFI Guideline B-8 amplifies this requirement, requiring a FRFI to be satisfied that the information collected demonstrates that it knows the client.

Criterion 10.7— PCMLTFR ss.54.3 (financial entities), 56.3 (life insurance sector), 57.2 (securities dealers), 59.01 (MSBs), and 61.1 (departments or agencies of the government or provinces that sell or redeem money orders) require all covered REs to conduct ongoing monitoring of their business relationships. Section 1(2) defines this to mean monitoring on a periodic basis, according to assessed risk, by a person or entity of their business relationships with clients for the purpose of (i) detecting transactions that must be reported to FINTRAC; (ii) keeping client identification information up to date; (iii) reassessing levels of risk associated with clients' transactions and activities; and (iv) determining whether transactions or activities are consistent with the information.

Where higher risks are identified, PCMLTFR, ss.71.1(a)-(c)) require "prescribed special measures" to be taken, which include enhanced measures to keep client identification and beneficial ownership information up to date and also to monitor business relationships in order to detect suspicious transactions. The Regulations do not explicitly cover scrutiny of the source of funds.

Specific CDD Measures Required for Legal Persons and Legal Arrangements

Criterion 10.8— The PCMLTFR requirements for FIs to understand the nature of the customer's business and its ownership and control structure cover legal persons or legal arrangements.

Criterion 10.9— See c.10.3 above, which covers identification and verification of legal persons and arrangements. The PCMLTFR (ss.14(b), 14.1(b), 15(1)(c), 20, 23(1)(b), 30(b) and 49(b)) require the collection of information on power to bind the legal person or arrangement in relation to an account or transaction. However, the Regulations do not cover gathering the names of relevant persons having a senior management position in the legal person or arrangement. Where an RE is unable to obtain information about the ownership, control and structure of a trust or other legal arrangement, the PCMLTFR (s.11.1(4)(a)) require reasonable measures to be taken to ascertain the identity of the most senior managing officer of the entity concerned.

The Regulations (s.65(1)) require confirmation of a corporation's existence, and its name and address, by reference to its certificate of corporate status or other acceptable official record. The existence of an entity other than a corporation must be confirmed by referring to a partnership agreement, articles of association or other similar record. There is no specific requirement, in this case, to obtain the address of the registered office or principal place of business, if different. Consequently, for non-corporate legal persons and for legal arrangements such as trusts, the standard is only partially met. Partnership agreements, etc., are unlikely to confirm details of address and principal place of business. Similarly, while trust documents usually contain sufficient information to satisfy the account-holding FI as to name, legal form, and proof of existence; such documents usually do not provide additional information about the registered address or principal business of the trust.

In addition, trust companies are required when acting as trustee of a trust (ss.55 (a)-(c)) to (i) of the PCMLTFR) to ascertain the identity of every person who is the settlor of an inter vivos trust: (ii) confirm the existence of, and ascertain the name and address of, every corporation that is the settlor of an institutional trust; and (iii) confirm the existence of every entity, other than a corporation, that is the settlor of an institutional trust. Under the Regulations (s.55 (d)), where an entity is authorized to act as a co-trustee of any trust, the trust company must (i) confirm the existence of the entity and ascertain its name and address; and (ii) ascertain the identity of all persons—up to three—who are authorized to give instructions with respect to the entity's activities as co-trustee. Finally, under the Regulations (s.55 (e)), trust companies must ascertain the identity of each person who is authorized to act as co-trustee of any trust. However, as natural persons who are trustees are not REs under the PCMLTFA, they are not subject to CDD obligations.

PCMLTFR ss 11 (a)-(b) require trust companies, for inter vivos trusts, to (i) keep a record that sets out the name and address of each of the beneficiaries that are known at the time that the trust company becomes a trustee for the trust; (ii) if the beneficiary is a natural person, record their date of birth and the nature of their principal business or their occupation; and (iii) if the beneficiary is an entity, the nature of their principal business.

Criterion 10.10— The legal requirements for obtaining information on beneficial owners of customers that are legal persons are set out under c.10.5 above.

REs must confirm the existence of a corporation or non-corporate legal entity at the opening of an account or when conducting certain transactions. At the same time, they must obtain information about the entity's beneficial ownership and confirm its accuracy. Beneficial ownership refers to the identity of the individuals who ultimately control the corporation or entity, which extends beyond another corporation or another entity. The PCMLTFR requirements for corporations and other entities refer to "persons." PCMLTFA, s.2 defines "person" to mean an individual, which therefore requires the natural person to be identified. If the RE has doubts about whether the person with the controlling ownership interest is the beneficial owner, then it is deemed to have been unable to obtain the information referred to under PCMLTFR, s.11.1(1) or to have been unable to confirm that information in accordance with PCMLTFR, s.11.1(2). In this case, the RE is required, under PCMLTFR s.11.1(4), to: take reasonable measures to ascertain the identity of the most senior managing officer of the entity; treat that entity as high risk for the purpose of PCMLTFA, s.9.6(3) and apply the prescribed special measures set out in PMCLTFR, s.71.1. Where no individual ultimately owns or controls 25% or more of an entity, directly or indirectly, REs must nevertheless record the measures they took, and the information they obtained, in order to reach that conclusion. Also, REs must comply with PCMLTFR, s.11.1(1)(d), which requires that information "establishing the ownership, control and structure of the entity" be obtained.

Criterion 10.11— The legal requirements for collecting information on the identity of beneficial owners of customers that are legal arrangements are set out under c.10.5 and 10.9 above. It is unclear, in the case of trusts, what identification requirements apply to protectors. Beneficiaries of trusts are covered by the ongoing monitoring provisions of s. 1(2) of the Regulations, which require that client identification information and information be kept up to date.

CDD for Beneficiaries of Life Insurance Policies

Criterion 10.12— All provincial *Insurance Acts* require life insurance companies to conduct CDD on (and keep a record of) the beneficiaries of life insurance policies, so this requirement applies to insurance companies nationally. There is no specific requirement to verify the identity of the beneficiary at the time of pay-out.

Criterion 10.13— As life insurance companies are covered under the PCMLTFA, they must risk assess all their clients and business relationships, products and services, and any other relevant risk factors (which include the beneficiary of a life insurance policy). In cases of high risk, life insurance companies must apply enhanced measures (prescribed special measures—s.71.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*).

Timing of Verification

Criterion 10.14— PCMLTFR, ss.64(2), 65(2) and 66(2)) specify the timeframe for verifying the identity of individuals, corporate and non-corporate entities. With certain exceptions, the legal obligation is to verify identity either at the time of the transaction or before any transaction other than an initial deposit is carried out. There are two main exceptions: (i) in relation to trust company activities, identity may be verified within 15 days of the trust company becoming the trustee; (ii) in relation to life insurance transactions and government or provincial departments or agencies handling money orders, identity may be verified within 30 days of the client information record being created. These exceptions are not justified according to what is reasonably practicable or necessary to facilitate the normal conduct of business, nor is there any condition about managing the ML/TF risks of delaying identity verification.

Criterion 10.15— PCMLTFR, s.1(2) defines "business relationship" to commence on account opening or when a client conducts specified transactions that would require their identity to be ascertained. Consequently, it is not possible for a customer to utilize a business relationship prior to verification.

Existing Customers

Criterion 10.16— see c.10.7. These ongoing monitoring obligations apply to all clients, whether or not they were clients at the date of new CDD obligations coming into force. Consequently, the ongoing monitoring process covers clients whose identity had not previously been ascertained. REs are required to take a risk-based approach to keeping information on client identification, beneficial ownership and purpose and nature of intended business relationship up to date.

Risk-Based Approach

Criterion 10.17— PCMLTFR, s.71.1 details the "prescribed special measures" to be taken in cases of high risk. This includes, for example, cases where beneficial ownership information cannot be obtained or confirmed. These special measures comprise taking enhanced measures to (i) ascertain the identity of a person or confirm the existence of an entity; (ii) keep client identification

information up to date (including beneficial ownership information); (iii) monitor business relationships for the purpose of detecting suspicious transactions; and (iv) determining whether transactions or activities are consistent with the information. In addition, Appendix 1 to FINTRAC Guideline 4 provides a checklist of products or services that should be considered high-risk.

Criterion 10.18— No reduced or simplified CDD measures are in place. Instead, the PCMLTFR gives exemptions from the client identification and record-keeping requirements in specific circumstances assessed as low risk by the authorities. These exemptions are mainly contained in s. 9 (accounts used by, or on behalf of, a third party) and s.62 (mainly concerning life insurance business). Furthermore, PCMLTFR, ss.19 and 56 create a form of exemption by requiring that life insurers only conduct CDD in relation to the purchase of an immediate or deferred annuity or a life insurance policy for which the client may pay CAD 10 000 or more over the duration of the annuity or policy. However, these exemptions do not apply where there is a suspicion of ML or TF.

Failure to Satisfactorily Complete CDD

Criterion 10.19— The PCMLTFA, s.9.2, provides that no RE shall open an account for a client if it cannot establish the identity of the client in accordance with the prescribed measures. Consequently, an FI that failed to conduct CDD, when obliged to do so, would be in breach of the Act and could be fined. There is no explicit prohibition on REs commencing a business relationship or performing a transaction when they are unable to comply with CDD measures if the identity of an individual cannot be ascertained or the existence of an entity confirmed when they open an account, the FI cannot open the account. This also means that no transaction, other than an initial deposit, can be carried out. Also, if the RE suspects that the transaction is related to a ML or TF offense, it must file an STR with FINTRAC. Under PCMLTFA, s.7, if the RE has reasonable grounds to suspect that the client conducts or attempts to conduct a transaction that is related to the commission or the attempted commission of an ML or TF offense, even if the client cannot be identified or his/her identity cannot be properly verified, the RE must file a STR. This requirement is amplified in FINTRAC guidance.

CDD and Tipping Off

Criterion 10.20— PCMLTFR, s.53.1 (2) specifies that the identity verification obligation does not apply where the RE believes that complying with that obligation would inform the customer that the transaction is being reported as suspicious. PCMLTFA s. 7 requires an STR to be filed in these circumstances.

Weighting and Conclusion

A number of relatively minor deficiencies have been identified.

Canada is largely compliant with R.10.

Recommendation 11 – Record-keeping

In the 2008 MER, Canada was rated LC with R.10. Two deficiencies were noted. First, the record-keeping requirement did not cover all FIs as defined by the FATF (notably financial leasing, factoring and finance companies). Second, FIs must ensure that all records required to be kept under the PCMLTFA could be provided within 30 days, which did not meet the requirement to make CDD records available on a timely basis. The FATF standard has not since changed, the requirement being to make records available "swiftly".

Criteria 11.1 and 11.2— The PCMLTFRs.69 detail the obligation to keep records for a period of at least five years following completion of the transaction or termination of the business relationship.

The PCMLTFR outlines, for each type of covered entity, detailed record-keeping rules for CDD, account files and business correspondence. The Regulations do not specifically require retention of any internal analysis of client business that might lead to an STR. However, covered entities would need to keep this information to substantiate that they were not in contravention of PIPEDA and that the disclosure without consent would have been warranted. The Privacy Commissioner could request this type of information under PIPEDA, s.18 as part of a compliance audit. In addition, OSFI requires FRFIs to keep such information.

Criterion 11.3— There is no clear legal obligation that transaction records be sufficient to permit reconstruction of individual transactions. However, the Regulations do specify in detail the contents of each piece of information that must be held in various records.

Criterion 11.4— The PCMLTFR s.70 requires REs to provide records upon request of FINTRAC within 30 days. This does not meet the "swiftly" standard.

Weighting and Conclusion

The deficiencies noted in the 2008 MER remain.

Canada is largely compliant with R.11.

Recommendation 12 – Politically exposed persons

In the 2008 MER, Canada was rated NC with R.6. There were no relevant legislative or other enforceable requirements in place.

Significant changes have been introduced since then. Requirements for FIs in relation to Politically Exposed Foreign Persons (PEFPs) were introduced in June 2008 through amendments to the PCMLTFA and PCMLTFR, specifying the enhanced customer identification and due-diligence requirements for such clients.

Subsequently, as part of a package of amendments to the PCMLTFA introduced in 2014, the coverage of the Act was extended to include Politically Exposed Domestic Persons (PEDP) and heads of international organizations. The bill was enacted on 19 June 2014; however, implementing

regulations are required before the PEP provisions will come into force. These regulations, announced on 4 July 2015, will come into force one year after registration of the regulations. They will require REs to determine, under prescribed circumstances, whether a client is a PEFP, a PEDP, a head of an international organization, or a close associate or prescribed family member of any such person.

Criterion 12.1— The PCMLTFR ss.54.2, 56.1, 57.1, 59(5) require REs to take reasonable measures to determine a person's status as a PEFP. FINTRAC Guidance 6G explains the PEP determination and OSFI Guideline B-8 is also relevant.

FINTRAC Guidance (s.8.1) makes clear that reasonable measures must be taken in relation to both new and existing accounts, as well as certain electronic funds transfers (EFT). Also, those measures include asking the client or consulting a credible commercially and/or publicly available database. OSFI Guideline B-8 also details what would constitute reasonable measures to make a PEFP determination.

PCMLTFA s. 9.3.2 requires REs, when dealing with a PEFP, to obtain the approval of senior management in the prescribed circumstances and take prescribed measures. For existing accounts, PCMLTFR, s. 67.1 (b) requires FIs and securities dealers to obtain the approval of senior management to keep a PEFP account open. FINTRAC Guidance 6G explains when to obtain the approval of senior management.

The Regulations (s. 67.2) also require REs to take reasonable measures to establish the PEFP's source of funds. FINTRAC Guidance 6G explains that reasonable measures include asking the client and OSFI Guideline B-8 gives a number of examples of acceptable sources of funds. Source of wealth is not mentioned in the Regulations; however, Guideline B-8 states that FRFIs should satisfy themselves that the amount of clients' accumulated funds or wealth appears consistent with the information provided.

The Regulations (s. 67.1 (1)(c)) require FIs and securities dealers to conduct enhanced ongoing transaction monitoring of PEFP and their family members' accounts. However, no similar legal requirement applies to other REs in relation to PEFPs, although FINTRAC Guidance 6G does specify enhanced ongoing monitoring of PEFP account activities. OSFI Guideline B-8 states that enhanced ongoing transaction monitoring may involve manual or automated processes, or a combination, depending on resources and needs and gives some examples of what this could comprise.

Criterion 12.2— OSFI Guideline B-8 explains that FRFIs are not (currently) under any legal obligation to identify domestic PEPs *per se*, whether by screening or flagging large transactions or in any other way. Further, even if FRFIs know they are dealing with a domestic PEP, until new regulations come into effect, they have no legal obligation to apply enhanced measures to PEDPs as they do to PEFP accounts.

Nevertheless, this OSFI guidance states that, where a FRFI is aware that a client is a domestic PEP, it should assess any effect on the overall assessed risk of the client. If that risk is elevated, the FRFI should apply appropriate enhanced due-diligence measures.

Criterion 12.3— Currently, PCMLTFA, s.9.3 includes family members of PEFPs and PCMLTFR, (s.1.1) states that the prescribed family members of a PEFP are included in the definition of a PEFP. Until the necessary implementing regulations take effect, close associates of any kind of PEP are not covered in law or regulations.

Criterion 12.4— No provisions in law or regulations relate to beneficiaries of life insurance policies who may be PEPs.

Weighting and Conclusion

Canada is non-compliant with R.12.

Recommendation 13 – Correspondent banking

In the 2008 MER, Canada was rated PC with R.7. Deficiencies were noted in relation to: assessment of a respondent institution's AML/CFT controls; assessment of the quality of supervision of respondent institutions; and inadequate CDD for payable-through accounts.

Criterion 13.1— The PCMLTFR (s.15.1 (2)) cover correspondent banking relationships, requiring FIs to collect a variety of information and documents on the respondent institution. That information includes: the primary business line of the respondent institution; the anticipated correspondent banking account activity of the foreign FI, including the products or services to be used; and the measures taken to ascertain whether there are any civil or criminal penalties that have been imposed on the respondent institution in respect of AML/CFT requirements and the results of those measures. The Regulations contain no specific requirements about determining either the reputation of the respondent institution or the quality of supervision to which it is subject. The PCMLTFR (s.15.1(3)) require the taking of reasonable measures to ascertain whether the respondent institution has in place AML/CFT policies and procedures, including procedures for approval for the opening of new accounts. There is, however, no requirement to assess the quality of a respondent institution's AML/CFT controls. PCMLTFA s. 9.4 (1) requires senior management approval to be obtained for establishing new correspondent relationships. The Regulations (s.15.1(2)(f)) specify the collection of a copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of each entity.

Criterion 13.2— The PCMLTFR (s. 55.2) stipulate that where the customer of the respondent institution has direct access to the services provided under the correspondent banking relationship (the 'payable-through account' scenario), the FI shall take reasonable measures to ascertain whether (i) the respondent institution has met the customer identification requirements of the Regulations; and (ii) the respondent institution has agreed to provide relevant customer identification data upon request.

Criterion 13.3— PCMLTFA, s.9.4 (2) prohibits correspondent banking relationships with a shell bank. In addition, the PCMLTFR (s. 15.1 (2) (h) require FIs to obtain a statement from the

respondent institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks.

Weighting and Conclusion

Deficiencies remain under c. 13.1.

Canada is largely compliant with R.13.

Recommendation 14 – Money or value transfer services

In its 2008 MER, Canada was rated NC with SR VI. The main deficiencies were: lack of a registration regime for money services businesses (MSBs); no requirement for MSBs to maintain a list of their agents; and the sanction regime available to FINTRAC and applicable to MSBs was deemed not effective, proportionate and dissuasive. Subsequently, Canada has made significant progress, and the FATF standard has been strengthened to require countries to take action to identify unlicensed or unregistered MSBs and apply proportionate and dissuasive sanctions to them.

Criterion 14.1— PCMLTFA, s.11.1 stipulates that any entity or person covered by s.5(h) of the Act, (persons and entities engaged in the business of foreign exchange dealing, of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's checks or other similar negotiable instruments) and those referred to in s.5(l) of the Act (those that sell money orders to the public), must be registered with FINTRAC.

Criterion 14.2— Under its mandate (PCMLTFA, s. 40(e)) to ensure compliance with part 1 of the Act, FINTRAC has a process for identifying MSBs that carry out activities without registration. This includes searching advertisements and other open sources as well as through on-site visits. Additionally, MVTS whose registration status is revoked are still tracked to ensure that they are not conducting business illegally.

The PCMLTF Administrative Monetary Penalties (AMP) Regulations describe the classification of different offenses under the PCMLTFA and the Regulations. Failure to register is classified as a serious violation. These Regulations classify violations as minor, serious, and very serious, each with a varying range of monetary penalties, up to CAD 500 000. In addition to criminal sanctions and monetary penalties for non-compliance, FINTRAC uses other means to encourage compliance. Monetary penalties are only considered after giving an entity or person a chance to correct deficiencies. If a very serious violation has been committed, a fine is greater than CAD 250 000, or if there is repeat significant non-compliance, FINTRAC considers publicly naming that entity or person, using its powers under s.73.22 of the PCMLTFA.

Criterion 14.3— PCMLTFA s. 40 (e) gives FINTRAC the mandate to ensure compliance with the Act. FINTRAC uses its powers under the PCMLTFA (ss. 62, 63 and 63.1) to examine records and inquire into the business and affairs of REs to monitor MVTS providers for AML/CFT compliance.

Criterion 14.4— PCMLTFA, ss.11.12(1) and (2) require that a list of agents, mandataries or branches engaged in MSB services on behalf of the applicant be submitted upon registration of the MSB with FINTRAC. S. 11.13 of the Act stipulates that a registered MVTS must notify FINTRAC of any change to the information provided in the application or of any newly obtained information within 30 days of the MVTS becoming aware of the change or obtaining the new information. This includes information about the MVTS's agents.

This criterion is also met through the legal obligation described under c. 14.1 above.

Criterion 14.5— The PCMLTFR (s.71(1)(d)) require MVTS, who have agents or other persons authorized to act on their behalf, to develop and maintain a written ongoing compliance training program for those agents or persons. S. 71(1)(e) also requires MVTS to institute and document a review of their agents' policies and procedures, risk assessment and the training program for the purpose of testing effectiveness. Such reviews must be carried out every two years.

Weighting and Conclusion

Canada is compliant with R.14.

Recommendation 15 – New technologies

In the 2008 MER, Canada was rated NC with former R.8 due to the lack of legislative or other enforceable obligations addressing the risks of new technological developments. Since then, some 40 legislative amendments to the PCMLTFA were tabled in Parliament (e.g. measures to subject new types of entities to the PCMLTFA, including online casinos, foreign MSBs and businesses that deal in virtual currencies such as Bitcoin). Canada is currently developing regulatory amendments to cover pre-paid payment products (e.g. prepaid cards) in the AML/CTF regime. The NRA examined the ML/TF vulnerabilities of 27 economic sectors and financial products, including new and emerging technologies, both in terms of products (e.g. virtual currency and pre-paid access), and sectors (e.g. telephone and online services in the banking and securities sectors).

Criterion 15.1— REs must conduct a risk assessment that includes client and business relationships, products and delivery channels, and geographic location of activities of the RE and the client(s), and any other relevant factors (PCMLTFR. s.71(1)(c)). While the requirements capture the need to assess ML/TF risks related to products and delivery mechanisms, there is no explicit legal or regulatory obligation to similarly risk assess the development of new products and business practices, nor is there any such obligation relating to the use of new or developing technologies for new and pre-existing products. However, Canada issued regulatory amendments for public comment in July 2015 clarifying that REs must consider, in their risk assessment, any new developments in, or the impact of new technologies on, the RE's clients, business relationships, products or delivery channels or the geographic location of their activities. A risk assessment review must be conducted every two years by an internal or external auditor, or by the entity (s.71(1)(e) of the Regulations). This ensures that risk assessments are regularly evaluated to capture risks, which may include new technologies. FINTRAC Guideline 4 specifies that new technology developments (e.g. electronic cash,

stored value, payroll cards, electronic banking, etc.) must be included in a company's risk assessment.

Criterion 15.2— While there is a regulatory expectation in FINTRAC's risk-based approach guidance[109] which states that REs should reassess their risk if there are changes due to new technologies or other developments, there are no explicit requirements in law or regulation that FIs undertake risk assessments prior to the launch or use of such products, practices and technologies.

Weighting and Conclusion:

Canada is non-compliant with R.15.

Recommendation 16 – Wire transfers

In the 2008 MER, Canada was rated NC with SR VII, which had simply not been implemented. Canada made some progress since then. The requirements have also been very substantially expanded in R.16 (i.e. inclusion of beneficiary information in wire transfers and additional obligations on intermediary and beneficiary FIs and MSBs).

Ordering Financial Institutions

Criterion 16.1— PCMLTFA, s.9.5 requires FIs to include with the transfer, when sending an international EFT, the name, address, and account number or other reference number, if any, of the client who requested it. The Act has no equivalent provision about including beneficiary name, account number or unique transaction reference number in this 'ordering FI' scenario. However, Schedule 2, Part K, of the PCMLTFR, which covers outgoing SWIFT payment instructions report information, does stipulate that, for single transactions of CAD 10 000 or more, the beneficiary client's name, address and account number (if applicable) should be included. There are no enforceable provisions requiring FIs to include beneficiary information in EFTs below CAD 10 000 (either as a single transaction, or multiple transactions within a 24-hour period).

Criterion 16.2— PCMLTFA, s.9.5 is not limited to single transfers—it, therefore, also applies in cases where numerous individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries.

Criterion 16.3— There is no 'de minimis' threshold for the requirements of c.16.1.

Criterion 16.4— Originator information would be verified through CDD obligations (see R.10). In addition, s. 53.1 of the Regulations states that the identity of every person that conducts a suspicious transaction must be ascertained, unless it was previously ascertained, or unless the FI believes that doing so would inform the individual an STR was being submitted.

Criterion 16.5— The Act's s.9.5 requirements cover both domestic and international EFTs.

[109] FINTRAC (2015), Guidance on the Risk-Based Approach to Combatting Money Laundering and Terrorist Financing, www.fintrac-canafe.gc.ca/publications/rba/rba-eng.pdf.

Criterion 16.6— Canada does not permit simplified originator information to be provided.

Criterion 16.7— The PCMLTFR (ss. 14 (m) and 30 (e)) require FIs and MSBs to keep a record of the name, address and account number, or transaction reference of the ordering client for all EFTs of CAD 1 000 or more. In addition, a record must be kept of the name and account number of the recipient of the EFT, as well as the amount and currency of the transaction.

Criterion 16.8— There is no explicit prohibition on executing wire transfers where CC, ss.16.1 to 16.7 above cannot be met. However, if an RE is unable to comply with the relevant legal requirements, it cannot proceed with a wire transfer without breaking the law and being subject to AMPs.

Intermediary Financial Institutions

Criteria 16.9 to 16.12— The PCMLTFA and regulations use the terms "send/transfer" and "receive" to apply obligations to intermediaries, which are, therefore, subject to the same requirements that apply to ordering and beneficiary institutions. Thus, the implications of possible data loss and of straight-through processing are not captured, as they should be to meet the standard.

Beneficiary Financial Institutions

Criterion 16.13— PCMLTFA, s.9.5(b) requires FIs to take reasonable measures to ensure that any transfer received by a client includes information on the name, address, and account number or other reference number, if any, of the client who requested the transfer. These requirements apply equally to all EFTs, regardless of where they are situated in the payment chain. Where an FI is transmitting a transfer received from another FI, it is, therefore, required to ensure that complete originator information is included. There are no legal requirements relating to beneficiary information.

OSFI Guideline B-8 states that FRFIs that act as intermediary banks should develop and implement reasonable policies and procedures for monitoring payment message data subsequent to processing. Such measures should facilitate the detection of instances where required message fields are completed but the information is unclear, or where there is meaningless data in message fields. The Guideline cites a few examples of reasonable measures that could be taken.

Criteria 16.14 and 16.15— There are no specific obligations on beneficiary FIs involved in cross-border EFTs.

Money or Value Transfer Service Operators

Criterion 16.16— All obligations identified in CC, ss.16.1–16.9 above apply to MSBs and their agents.

Criterion 16.17— There are no specific legal requirements for MTVS providers either to review ordering and beneficiary information to decide whether to file an STR or to ensure that an STR is filed in any country affected and transaction information made available to the FIU.

Implementation of Targeted Financial Sanctions

Criterion 16.18— See the assessment of R.6 and R.7. The processing of EFTs, in terms of FIs taking freezing action and complying with prohibitions from conducting transactions with designated persons and entities, is adequately covered in law.

Weighting and Conclusion

The legal obligations applicable to ordering FIs and MSBs are broadly satisfactory, but there remain some weaknesses.

Canada is partially compliant with R.16.

Recommendation 17 – Reliance on third parties

In the 2008 MER, Canada was rated NC with R.9. In the only two scenarios where reliance on a third party or introduced business was legally allowed without an agreement or arrangement, the measures in place were insufficient to meet the FATF standard. In addition to the two reliance on third parties/introduced business scenarios contemplated by the Regulations, the financial sector used introduced business mechanisms as a business practice. However, no specific requirements, as set out in R.9, applied to these scenarios. Only minor changes have subsequently been introduced.

Criterion 17.1— The PCMLTFR (ss. 64(1)(b)(A)(I) and (II)) allow FIs, other than MSBs, and also foreign entities that conduct similar activities, to rely on affiliated third parties, or those in the same association, for the purpose of ascertaining the identity of a person.

More specific legal provisions apply to both the life insurance industry and securities dealers. A life insurance company, broker, or agent is not required to ascertain the identity of a person where that person's identity has previously been ascertained by another life insurance company, broker, or agent in connection with the same transaction or series of transactions that includes the original transaction. Similarly, a securities dealer, when opening an account for the sale of mutual funds, is not required to ascertain identity where another securities dealer has already done so in respect of the sale of mutual funds for which the account has been opened. The PCMLTFR (s.56(2) and s.62(1)(b)) refer.

Apart from the specific situations set out above, all requirements under the PCMLTFR continue to apply to the FI that has the relationship with the customer.

The PCMLTFR (s.64.1) state that, when REs use an agent or a mandatary to meet their client identification obligations, they must enter into a written agreement or arrangement with the agent or mandatary. In addition, the RE must obtain from the agent or mandatary the customer information that was obtained under the agreement or arrangement. The agent or mandatary can be any individual or entity, provided these two conditions regarding written agreement and obtaining customer information are met. Where the client is not physically present at the opening of an account, establishment of a trust or conducting of a transaction, the agent or mandatary has the same

two options, outlined in ss.64(1) and 64(1.1), that an RE does when dealing with a client who is not physically present.

In the first option, the agent or mandatary must obtain the individual's name, address, and date of birth. Then, they must confirm that one of the following has ascertained the identity of the individual by referring to an original identification document:

- a financial entity, life insurance company, or securities dealer affiliated with them;
- an entity affiliated with them and whose activities outside Canada are similar to those of a financial entity, life insurance company, or securities dealer; or
- another financial entity that is a member of their financial services cooperative association or credit union central association of which they also are a member.

To use this option, the agent or mandatary must verify that the individual's name, address and date of birth correspond with the information kept in the records of that other entity. The second option requires the use of a combination of two of the identification methods set out in Part A of Schedule 7 of the PCMLTFR.

Where agents or mandataries with written agreements are concerned, the relying entity must obtain customer information supplied under the agreement. However, life insurance companies/brokers/agents or securities dealers are not required to obtain from the relied-upon institution the necessary CDD information.

Similarly, life insurance companies/brokers/agents or securities dealers are not required to satisfy themselves that copies of CDD information will be made available to them by the third party on request without delay.

There is no explicit obligation, either for relying entities with agents and mandataries or for life insurance companies/brokers/agents or securities dealers, to satisfy themselves that the FI relied on is regulated and supervised or monitored for compliance with CDD and record-keeping obligations in line with R.10 and R.11.

Criterion 17.2— The PCMLTFA and PCMLTFR do not require life insurance companies/brokers/agents or securities dealers to assess which countries are high risk for third party reliance. The authorities state that reliance may only be placed on life insurance companies/brokers/agents or on securities dealers that are subject to the PCLMTFA, and FINTRAC's oversight. If so, the scenario outlined in Criterion 17.2 would not arise.

While ss.56(2) and 62(1) (b) of the PCMLTFR do not actually preclude the possibility of reliance being placed on third parties outside Canada, with no account taken of the level of country risk, an RE can only rely on third parties outside Canada if they are affiliated with them. Canada issued

regulatory amendments for public comment in July 2015 that included an amendment with respect to Group-Wide Compliance Programs that would require REs to take into consideration as part of their compliance programs the risks resulting from the activities of their affiliates.

Criterion 17.3— The PCMLTFR (ss.64(1)(b)(A)(I) and (II)) allow FIs, other than MSBs, and also foreign entities that conduct similar activities to rely on affiliated third parties, or those in the same association, for the purpose of ascertaining the identity of a person. PCMLTFA, ss9.7 and 9.8 require foreign branches and subsidiaries, subject to there being no conflict with local laws, to develop and apply policies to keep records, verify identity, have a compliance program, and exchange information for the purpose of detecting or deterring an ML or TF offense or of assessing the risk of such an offense. Thus, group-wide ML/TF standards should apply, providing appropriate safeguards.

Where there is a conflict with, or prohibition by, local laws, the RE must keep a record of that fact, with reasons, and notify both FINTRAC and its principal federal or provincial regulator within a reasonable time (PCMLTFA, s.9.7(4)).

Weighting and Conclusion

A number of deficiencies remain, even though that reliance on third parties appears to be of limited practical application.

Canada is partially compliant with R.17.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the 2008 MER, Canada was rated LC with R.15 due to minor deficiencies and NC with R.22 due to the lack of legal obligation to ensure that foreign branches and subsidiaries applied AML/CFT measures consistent with home country standards, and obligation to pay particular attention to branches and subsidiaries in countries, which did not, or insufficiently, applied the FATF Recommendations. The current FATF standards are broadly unchanged, although R.18 specifies in more detail what should be done to manage ML/TF risk where host country requirements are less strict than those of the home country. Significant changes came into force in Canada in June 2015.

Criterion 18.1— PCMLTFA s. 9.6 requires FIs to establish and implement a compliance program to ensure compliance with the Act. The program must include the development and application of policies and procedures for the FI to assess, in the course of their activities, the risk of an ML or TF offense. The PCMLTFR (ss. 71 (1)(a) and (b)) specify that: a person must be appointed to be responsible for implementation of the program; and the program must include developing and applying written compliance policies and procedures that are kept up-to-date and approved by a senior officer.

OSFI Guideline B-8 stipulates that FRFIs must have a Chief Anti-Money Laundering officer (CAMLO) responsible for implementation of the enterprise AML/ATF program, who should be one person positioned centrally at an appropriate senior corporate level of the FRFI. Separately, OSFI Guideline E-13 requires that FRFIs must have a Chief Compliance officer with a clearly defined and

documented mandate, unfettered access and, for functional purposes, a direct reporting line to the Board.

Neither the PCMLTFA nor PCMLTFR contain any specific obligations regarding FIs' screening procedures when hiring employees. Similarly, there are no measures in place in sector legislation at the federal or provincial level. OSFI Guideline E-17 details OSFI's expectations in respect of screening new directors and senior officers of FRFIs at the time of hiring. However, this applies only to a defined set of "Responsible Persons," not to all employees.

The PCMLTFR (s. 71(1)(d)) require REs that have employees, agents or other persons authorized to act on their behalf to develop and maintain a written ongoing training program for those individuals. In addition, OSFI Guideline B-8 advises FRFIs to ensure that written AML/ATF training programs are developed and maintained. Appropriate training should be considered for the Board, Senior Management, employees, agents and any other persons who may be responsible for control activity, outcomes or oversight, or who are authorized to act on the Company's behalf, pursuant to the PCMLTFR.

The PCMLTFR (s.71 (1) (e)) oblige all REs to institute and document a review of their policies and procedures, the risk assessment and the training program for the purpose of testing effectiveness. That review must be carried out every two years by an internal or external auditor of the RE, or by the RE itself, if it has no auditor. OSFI Guideline B-8 amplifies the requirement in a number of ways and also sets out an expected standard of self-assessment of controls applicable to FRFIs.

Criterion 18.2— Measures which came into effect in June 2015 expanded section 9.7 of the PCMLTFA to cover foreign branches as well as subsidiaries. The effect was to require FIs, securities dealers and life insurance companies to implement policies and procedures for CDD, record-keeping and compliance programs that are consistent with Canadian requirements and apply across a financial group.

A new s.9.8(1) of the Act introduced requirements for REs to have policies and procedures in place for how they will share information with affiliates for the purpose of detecting or deterring an ML or TF offense or of assessing the risk of such an offense. This provision is sufficiently widely drawn to cover the kind of customer, account and transaction information stipulated in the FATF standard. There are no prohibitions in either the PCMLTFA or PIPEDA on sharing of information, including STRs, within financial groups, domestically or cross-border.

The new law did not cover safeguards on the confidentiality and use of information exchanged. However, the necessary safeguards already exist under PIPEDA (s.5 and Schedule 1), which apply equally to client information received from a branch or subsidiary under the PCMLTFA.

Criterion 18.3— Under newly amended s.9.7(4) of the PCMLTFA, when local laws would prohibit a foreign branch or foreign subsidiary from implementing policies that are consistent with Canadian AML/ATF requirements, the RE must advise FINTRAC and their principal regulator. (In the case of FRFIs, this is OSFI; for provincially regulated FIs, the relevant provincial supervisor).

Weighting and Conclusion

There is a remaining deficiency regarding the internal controls aspect of R.18.

Canada is largely compliant with R.18.

Recommendation 19 – Higher-risk countries

In the 2008 MER, Canada was rated PC with R.21, because there were no general enforceable requirement for FIs to give special attention to transactions or business relationships connected with persons from higher-risk countries, no measures advising of other countries with AML/CFT weaknesses, and no requirement to examine the background and purpose of transactions and to document findings. The FATF standard remains broadly the same, but there have been major changes in Canada since 2008.

Criterion 19.1 and 19.2— Part 1.1 of the PCMLTFA, which entered into force in June 2014, introduced two new authorities for the Minister of Finance: (i) the authority to issue directives requiring REs to apply necessary measures to safeguard the integrity of Canada's financial system in respect of transactions with designated foreign jurisdictions and entities. The measures contemplated included CDD, monitoring and reporting of any financial transaction to FINTRAC; (ii) the authority to recommend that the Governor-in-Council issue regulations limiting or prohibiting REs from entering into financial transactions with designated foreign jurisdictions and entities. These authorities enable Canada to take targeted, legally enforceable, graduated and proportionate financial countermeasures against jurisdictions or foreign entities with insufficient or ineffective AML/ATF controls. These measures can be taken in response to a call by an international organization, such as the FATF, or unilaterally. The Minister has not issued any countermeasures under Part 1.1; however, OSFI and FINTRAC have regularly drawn the attention of FRFIs and REs to the FATF calls on members, and have issued regular guidance in Notices and Advisories following each FATF meeting. OSFI has issued prudential supervisory measures against FRFIs it believes have not implemented FATF expectations (PCMLTA (s.11.42) and PCMLTFR (s.71.1)).

Criterion 19.3— Risk assessments on jurisdictions with AML/ATF weaknesses are conducted through the IFAC Under s.11.42(3) of the Act, the Minister's decision to issue a Directive may require the Director of FINTRAC to inform all REs. Additional guidance is provided through FINTRAC advisories and OSFI notices, available online, encouraging enhanced CDD with respect to clients and beneficiaries involved in transactions with high-risk jurisdictions.

Weighting and Conclusion:

Canada is compliant with R.19.

Recommendation 20 – Reporting of suspicious transaction

In the 2008 MER, Canada was rated LC with R.13 and SR. IV because some FIs (e.g. financial leasing, factoring and finance companies) were not covered by the obligation to report and there was no requirement to report attempted transactions. Some improvements have been made since then.

Criterion 20.1— PCMLTFA, s.7 requires REs to report to FINTRAC every financial transaction that occurs, or that is attempted, in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML or TF offense. The scope of the PCMLTFA still excludes certain sectors (financial leasing, finance and factoring companies), but this represents an ongoing minor deficiency. ML is defined by reference to CC, s.462.31(1), which, in turn, is defined in CC, s.462.31(1) to mean any offense that may be prosecuted as an indictable offense under this or any other Act of Parliament, other than an indictable offense prescribed by regulation. As described under c.3.2, ML now applies to a range of offenses in each FATF designated category of predicate offenses, including tax evasion.

Suspicious transactions must be reported "within 30 days" of detection of a fact that constitutes reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of an ML offense or a TF offense. (PCMLTF Suspicious Transaction Reporting Regulations, s.9(2)).This does not meet the standard of reporting "promptly."

Criterion 20.2— Attempted transactions are now covered by the reporting requirement.

Weighting and Conclusion

The reporting requirement covers several, but not all elements, of the standard.

Canada is partially compliant with R.20.

Recommendation 21 – Tipping-off and confidentiality

In the 2008 MER, Canada was rated C with R.14.

Criterion 21.1— The PCMLTFA (s.10) states that no criminal or civil proceedings lie against a person or an entity for making an STR in good faith or for providing FINTRAC with information about suspicions of ML or TF activities. However, the requirement does not explicitly extend to reporting related to ML predicate offenses.

Criterion 21.2— PCMLTFA s.8 specifies that no person or entity can disclose that they have made an STR, or disclose the contents of a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. The law does not, however, cover a situation where a person or entity is in the process of filing a STR but has not yet done so. Neither does the legal obligation explicitly extend to reporting related to ML predicate offenses.

Weighting and Conclusion

The tipping off and confidentiality requirements do not explicitly extend to the reporting of suspicions related to ML predicate offenses.

Canada is largely compliant with R.21.

Designated Non-Financial Businesses and Professions (DNFBPs)

Since the 2008 MER, Canada has extended the AML/CFT requirements to BC Notaries and DPMS. The following DNFBPs are now subject to AML/CFT obligations: land-based casinos, accountants (defined as chartered accountant, certified general accountant, certified management accountant)[110] and accounting firms, British Columbia Notaries Public and Notary Corporations (hereinafter referred to as BC Notaries), real estate brokers or sales representatives, dealers in precious metals and stones (hereinafter DPMS) and certain trust companies, which fall under PCMLTFA, s.5 (e). Legal counsel and legal firms are covered as obliged AML/CFT entities, pursuant to PCMLTR, s.33.3, but, on 13 February 2015,[111] the Supreme Court of Canada concluded that the AML/CFT provisions are inoperative, as they are unconstitutional, for lawyers and law firms in Canada. Canada extended the AML/CFT regime to real estate developers when, under certain conditions, they sell to the public real estate (PCMLTFR, s.39.5). Notaries in provinces other than Québec and British Columbia are restricted to certifying affidavits under oath, and document certification. These notaries do not conduct any financial transactions and the transfer of property is done exclusively through lawyers in these provinces (see 2008 MER, para. 150). TCSPs are not a distinct category under the PCMLTFA and PCMLTFR. The definition of casino (PCMLTFR, s.1(1)), which excludes registered charities authorized to perform business temporarily, provides an unclear exemption.[112]

All gambling is illegal,[113] unless specifically exempted under CC, s.207. Several provinces (British Columbia, Quebec, Manitoba Nova Scotia, Prince Edward Island, New Brunswick and Newfoundland) have introduced online gambling through an extensive interpretation of the notion of "lottery scheme" allowed to them under CC, s.207(4)(c), which includes games operated through a computer. When these provinces introduced internet gambling, FINTRAC sent them a letter to inform them that

[110] PCMLTFR, Section 1. (2).

[111] The Supreme Court of Canada on 13 February 2015 has concluded that the search provisions of the Act infringe Section 8 of the Canadian Charter of Rights and Freedoms, while the information gathering and retention provisions, in combination with the search provisions, infringe Section 7 of the Charter Canada (Attorney General) v. Federation of Law Societies of Canada, 2015 SCC 7.

[112] There is no definition of "charitable purposes" and the notion of "temporary" business, does not give an exact timeframe, making unclear the reference to "not more than two consecutive days at a time," without fixing any further limit per week or per year. The exemption involving registered charities is to avoid duplication in the AML/CFT regime, as the Provincial Authority or its designate are RE of FINTRAC. Nevertheless, taking into account the possible operational models of casinos operating in Canada, the current definition of casino and the resulting AML/CFT requirements lack clarity in addressing the respective AML/CFT responsibilities of the different persons or entities that could be simultaneously involved in the business of the same casino (Crown corporations or regulators branches involved in the conduct and management of lotteries schemes, charitable organizations, First Nation organizations, casino's service providers).

[113] CC, Section 206 (1).

they were considered subject to AML/CFT obligations. Subsequently, these casinos started sending to FINTRAC Casino Disbursement Reports (for example, FINTRAC has received 988 such reports in the last 24 months). Nevertheless, the amendment to the definition of casinos that makes reference to online gambling operators is not yet entered into force.[114]

There are also land-based gaming and on line gambling[115] sites actually operating within Quebec, whose legal status is unclear which are not supervised by the province and which are not subject to AML/CFT obligations. These activities are authorized by the Kahnawake Gaming Commission operating on the basis of an asserted jurisdiction by the Mohawks over their territory. They are considered illegal by the authorities. Offshore gambling sites are deemed to be illegal as each casino must be licensed by a Canadian province. The authorities clarified that these activities are a matter for law enforcement to oversee.

Cruise ships that offer gambling facilities in Canadian waters are not obliged entities for AML/CFT purposes. (See 2008 MER, para. 1186-1187). Lottery schemes cannot be operated within five nautical miles of a Canadian port at which the ship calls (s.207.1 of the CC). Of note, there are no Canadian cruise ships. The exemption of cruise ship casinos is based on a proven low risk.

Trust and company services are provided by trust companies, legal counsels, legal firms and accountants—the PCMLTFA therefore does not identify TCSPs separately. Twenty-two trust companies (covered by a provincial Act, falling under of PCMLTFA, s.5(e)) are subject to AML/CFT obligations, but lawyers and accountants are not, despite the high vulnerability rating highlighted in the NRA.[116]

Recommendation 22 – DNFBPs: Customer due diligence

In the 2008 MER, Canada was rated NC with these requirements due to deficiencies in the scope of DNFBPs covered and in CDD and record-keeping requirements. Since then, Canada has extended the scope of the AML/CFT requirements to BC Notaries and DPMS and addressed some deficiencies in CDD requirements applicable to DNFBPs.[117]

Criterion 22.1— Scope issue: Internet casinos, TCSPs are not covered and the relevant provisions are inoperative with respect to legal counsels, legal firms and Quebec notaries (PCMLTFR, ss.33.3,

[114] Steps are being taken in this respect. Bill C-31 introduced legislative amendments to PCMLTFA s.5 k 1, which will come into force once the regulations are finalized, aimed at establishing AML/CFT obligations for online gambling conducted and managed by the provinces and covering those lottery schemes other than bingo and the sale of lottery tickets that are conducted and managed by provinces in accordance with CC, s.207(1)(a). These amendments will also extend the notion of relevant business to include other electronic devices similar to slot machines (such as video lottery terminals, currently excluded from the AML/CFT regime) but establishing a relevant threshold of "more than 50 machines per establishment" (PCMLTFA, s.5(k)(ii)).

[115] Online gaming operators that are licensed by the Commission must be hosted at Mohawk Internet Technologies, a data centre, located within the Mohawk Territory of Kahnawake.

[116] NRA, p.32.

[117] In particular, introducing the obligation to collect information on the purpose and intended nature of the business relationship and ongoing due diligence, extending the circumstances in which CDD is required, providing for enhanced measures in higher risk scenarios, excluding the exemption regime in case of suspicion.

33.4, 33.5, 59.4, 59.41, 59.4). As regards accountants and BC notaries, not all the relevant activities under the criterion are taken into account.

DNFBPs[118] are not required to obtain, take reasonable measures to confirm, and keep records of the information about the beneficial ownership of legal persons and legal arrangements, nor as to understand the ownership and control structure of the latter. DNFBPs are only required to confirm the existence of and ascertain the name and address of every corporation or other entity on whose behalf a transaction is being undertaken, and in the case of a corporation the names of its directors.[119] The rule of "third party determination" (PCMLTFR, s.8) is limited to individuals and is not applied to all relevant circumstances when CDD is required under the criterion. DNFBPs are not explicitly required to establish that the person purporting to act on behalf of the customer is so authorized. There are additional deficiencies for each relevant category. Casinos can perform a large variety of financial services, including wire transfers (see 2008 MER, para. 138). The following measures for ascertaining identity are carried out in line with the following threshold: on account opening (no threshold), when dealing with EFTs (CAD 1 000) and, dealing with foreign exchange or extension of credit (CAD 3 000).[120] The CAD 10 000 thresholds for ascertaining identity for cash financial transactions and casinos disbursement[121] are higher than the FATF standard. Not all the range of non-cash occasional transactions are covered: in particular, the purchase of chips through checks, credit, and debit cards, as well as prepaid cards are not captured. The redemption of "tickets" under PCMLTFR, s.42(1)(a) is not included, even if some kind of tickets (TITO tickets)[122] have been detected by FINTRAC in typologies of ML. There are no enforceable provisions requiring casinos to include beneficiary information in wire transfers, and no obligation for all REs to ascertain the identity of authorized signers (PCMLTFR, ss.54(1)(a) and 62(1)(a)). As regards, accountants and BC Notaries, not all the relevant activities under the criterion are included. In particular, no requirement is provided in relation to activities related to organization of contributions for the creation, operation and management of companies, legal persons and arrangements, and the scope of "purchasing or selling" securities, properties and assets is more limited than the notion of "management" included under the criterion. The definition of accountant (PCMLTFR, s.1(1) does not include "Chartered Professional Accountant."[123] In a real estate transaction, when the purchaser and the vendor are represented by a different real estate broker, each party to the transaction is identified by their own real estate broker. Real estate agents, in case of unrepresented party are required to take reasonable measures only to ascertain the identity of the party (PCMLTFR, s.59.2 (2, 3, and 4)), rather than applying reasonable risk-based CDD measures to the party that is not their client. DPMS are covered as required by the standards when they engage in the purchase or sale of

[118] With the exception of legal counsel and legal firms for which however the provisions are inoperative (Section 11.1 (1) of the PCMLTFR.
[119] PMCLTFR 59.1(b) & (c), 59.2(1)(b) &(c), 59.3 (b) & (c), 59.5 (b) & (c), 60 (e) &(f)
[120] PCMLTFR, Sections 60(a), 60(b)(iv), 60(b)(iii), 60(b)(ii)
[121] PCMLTFR, Sections 53 and 60(b)(i).
[122] Ticket In Ticket Out (TITO) "tickets" are also an increasingly popular casino value instrument used in many Canadian casinos (FINTRAC, ML Typologies and Trends in Canadian Casino, Nov. 2009, p.8).
[123] The unified new professional designation replaces the former three (Chartered Accountants, Certified General Accountants and Certified Management Accountants), and it is currently completed in several provinces (Quebec, New Brunswick, Saskatchewan, Newfoundland and Labrador). Further work is underway and expected to be included in forthcoming regulatory amendments.

precious metals, precious stones or jewellery in an amount of CAD 10 000 or more in a single transaction, other than those pertaining to manufacturing jewellery, extracting precious metals or precious stones from a mine, or cutting, or polishing precious stones..

Criterion 22.2— Scope issue: see 22.1. The circumstances under which relevant DNFBPs have to keep records do not fully match the list of activities required under R.10 (see 22.1). Furthermore, a non-account business relationship is established when transactions are performed in respect of which obliged entities are required to ascertain the identity of the person, rather than being based on a mere element of duration. The said definition entails that, apart from the case of suspicion, the record keeping requirements on a business relationship arise only when the prescribed thresholds for the transactions are reached. The deficiencies identified in R.11 apply also to DNFBPs.

Criteria 22.3, 22.4 and 22.5— There are no requirements for DNFBPs to comply with specific provisions covering PEPs, new technologies and reliance on third parties.

Weighting and Conclusion:

Canada is non-compliant with R.22.

Recommendation 23 – DNFBPs: Other measures

In its 2008 MER, Canada was rated NC with these requirements, due to the limited scope of DNFBPs included as well as to deficiencies with the underlying recommendations and to concern about the effectiveness of the STR regime in these sectors. Canada has since extended the scope of DNFBPs to some extent (See R.22), included attempted transactions in the STR regime and empowered the Department of Finance to take financial countermeasures with respect to higher-risk countries.

Criterion 23.1— PCMLTFA, s.7 (transaction where reasonable grounds to suspect) does not apply to all relevant categories of DNFBPs, nor to all relevant activities of accountants and BC Notaries as described under R.22.[124] The analysis in relation to R.20 above equally applies to reporting DNFPBs. There are no key substantive differences between the reporting regime for FIs and DNFBPs. FINTRAC Guidelines no. 2 (Suspicious Transactions) includes industry-specific indicators.

Criterion 23.2— Scope issue: see 23.1. Accountants, accounting firms, legal counsels and legal firms, BC Notaries, real estate agents and developers, land-based casinos, DPMS are all required to establish and implement a compliance program (PCMLTFA, s.9.6 (1); PCMLTFR, s.71(1)). While compliance procedures must be approved by a senior officer, PCMLTFA, ss.9.6 and PCMLTFR, s.71(1)(a) do not stipulate that the designation of the compliance officer shall be at the management level. DNFBPs, other than land-based casinos, are not required to have adequate screening procedures to ensure high standards when hiring employees. Also, there is no specific requirement that review of the compliance regime be performed by an independent audit function, as it can also be carried out through a procedure of self-assessment (PCMLTFR, s.71(1)(e)).

[124] Under PCMLTA, Section 5, Part 1 of the Act (including the STRs obligations) applies while carrying out the activities described under the regulations.

Criterion 23.3— Scope issue: see 23.1. See R.19 for a description of this requirement.

Criterion 23.4— Scope issue: see 23.1. The requirements for DNFBPs are the same as those applied to FIs under R.21.

Weighting and Conclusion:

Canada is non-compliant with R.23.

Recommendation 24 – Transparency and beneficial ownership of legal persons

Canada was rated NC with former R.33 based on concerns over a lack of transparency for legal entities, the availability of bearer shares without adequate safeguards against misuse, and a lack of powers by the authorities to ensure the existence of adequate, accurate and timely beneficial ownership information for legal entities. Since 2008, the obligations for FIs to obtain information on the identity of beneficial owners and the CRA's ability to disseminate information on legal entities to the RCMP have been strengthened.

Canada's corporate legal framework consists of federal, provincial and territorial laws: (i) Legal entities may be established at the federal level under the Canada Business Corporation Act (CBCA); the Canada Not-for-Profit Corporations Act (NFP Act), or the Canada Cooperatives Act (CCA). Federally incorporated entities are entitled to operate throughout Canada but in addition to registration at the federal level, are also subject to registration with the province or territory in which they carry out business. (ii) Each of the thirteen territories and provinces regulates the types of legal entities that can be established at the local level. Eight provinces and territories have enacted specific laws that provide for the establishment of corporations and NPOs. Prince Edward Island, Newfoundland and Labrador, Alberta, Manitoba, Quebec, and New Brunswick do not have specific NPO legislation in place but regulate NPOs through the relevant provincial company law.

Legal entities incorporated at the provincial or territorial level enjoy business name protection only in the province or territory where they are incorporated. To operate in another province in Canada, they have to register with that province but there is no guarantee that they will be able to use their corporate name (e.g. a business entity with the same name may already be operating in that province). Federal, provincial and territorial corporate entities may carry out business internationally if the foreign country recognizes the type of corporate entity.

In addition to legal entities, all provinces provide for the establishment of general and limited partnerships pursuant to common law rules; and all provinces, but Yukon, Prince Edward Island and Nunavut have passed statutes to provide for the establishment of limited liability partnerships. Partnerships are not subject to registration as part of the establishment process, but most provinces and territories require registration of businesses before a partnership may operate there. Business registration obligations under provincial and territorial laws also apply to foreign entities wishing to carry out business in Canada.

Criterion 24.1— *Federal legal persons:* Innovation, Science and Economic Development Canada (ISED), formerly Industry Canada, provides a comprehensive overview and comparison on its internet homepage of the various legal entities available and their forms and basic features. All legal entities established at the federal level are subject to registration. Given that corporations are by far the most utilized type of legal entity in Canada, particular emphasis is put on information pertaining to federal corporations under CBCA and their incorporation and registration process, which can be initiated online or by sending all required documents to the competent registrar via email, fax, or mail. [125] ISED also offers a search tool, which makes some basic information of federal companies publicly available. The search function also indicates the legislation the corporation is incorporated under, which in turn clarifies basic regulating powers. *Provincial legal persons:* Similar information and services are provided through the homepages of all provincial governments except that of New Brunswick. The relevant web links are easy to find through ISED's homepage and provide public access to the relevant provincial laws that describe the various legal entities available; the name and contact information for the relevant authority competent for registration; and the procedures to be followed to establish a legal entity or to register a corporation. *Partnerships and foreign entities:* Partnerships and foreign entities operating in any of Canada's provinces or territories are subject to registration at the provincial level. The Canada Business Network maintains a homepage that provides links to the various provincial and territorial business registries.

Criterion 24.2— The NRA identified privately held corporations as being highly vulnerable to misuse for ML/TF purposes. The conclusion was reached based on the understanding that such corporations can easily be established and be used to conceal beneficial ownership. The risk assessment determines the inherent risks involved with legal persons based on factors such as the products and services offered by legal entities, the types of persons that may establish or control a legal person, the possible geographic reach of a Canadian legal entity, and taking into account FINTRAC statistics on typologies involving legal entities in Canada.

Basic Information

Criterion 24.3— Both federal and provincial corporations, NPOs with legal personality and cooperatives are established through incorporation by the relevant incorporating department or agency. *Federal legal persons:* On the federal level, ISED, as part of the incorporation and annual filing process, collects and publishes information comprising the corporation's name, type, status, corporation number, registered office address in Canada, name and address of all directors, and governing legislation. The regulating powers for federal corporations are set out in the legislation or in the corporation's articles, which are approved by the Director appointed under the relevant Act. *Provincial legal persons:* Company information including the corporate name, type, status, registered office in Canada, and name and address of directors is collected through the same process as on the federal level, which is through annual filing procedures. *Partnerships and foreign entities:* Business registration requirements vary between the different provinces and territories, but usually require the provision of the name, registered office, mailing address, place of business in the province/territory, the date and jurisdiction of incorporation (for extraterritorial companies) or type

[125] www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs04843.html#articles.

of partnership, the name and address of directors or partners and a copy of the partnership contract or the incorporation certificate or other proof of existence. Partnerships not carrying out any business in Canada are not required to register as part of the establishment process.

Criterion 24.4— Record-keeping obligations extend to the corporation's articles and by-laws and any amendments thereof, of minutes of shareholder meetings and resolutions, share registers, accounting records, and minutes of director meetings and resolutions. Pursuant to CBCA, s.50, companies must also keep a share register that indicates the names and address of each shareholder, the number and class of shares held, as well as the date and particulars of issuance and transfer for each share. Similar provisions are set out in provincial legislation. Federal as well as provincial companies are required to keep records of basic information either in a location in Canada or at a place outside Canada, provided the records are available for inspection by means of computer technology at the registered office or another place in Canada and the corporation provides the technical assistance needed to inspect such records (CBCA, s.20). There is no legal requirement to inform the incorporating department or agency, or where applicable, the company register of the location at which such records are being kept.

Criterion 24.5— Under CBCA, s.19 (4) federal corporations are required to inform the Director appointed under the CBCA within 15 days of any change of address of the registered office. Changes in legal form, name or status as well as amendments to the articles of incorporation take effect only after they have been filed with the Director. More or less the same updating requirements are especially provided for under provincial legislation, except in Quebec and Nova Scotia.[126] In Nova Scotia, the updating requirement applies but changes to the registered office have to be filed within 28 days and there is only a general obligation to notify the Registrar "from time to time" of any changes among its directors, officers, or managers. Directors, shareholders and creditors have access to these documents and are permitted at all times to check their accuracy. However, no formal mechanism is in place to ensure that shareholder registers are accurate. For partnerships and extraterritorial corporations, some provinces and territories impose an annual filing obligation, others require renewal of the license and updating of relevant information on a multi-year basis.

Beneficial Ownership Information

Criterion 24.6— Canada uses existing information to determine a legal entity's beneficial ownership, if and as needed, including as follows:

(i) FIs providing financial services to legal entities, partnerships or foreign companies. Since 2014, obligations under the PCMLTFA for FIs to obtain ownership information of customers or beneficiaries that are legal entities have been strengthened. Prior to 2014 FIs identified beneficial owners of legal entities mostly based on a declaration of the customer. For those companies established prior to 2014, it is, thus, questionable whether this measure did indeed result in the availability of accurate and updated beneficial ownership information. Ongoing CDD obligation under the PCMLTFA have resulted in BO information becoming available for a number of companies that opened bank accounts in Canada prior to 2014, but most FIs interviewed by the assessors

[126] For example Section 2 Ontario Corporations Information Act; Article 20 Alberta Business Corporation Act; Article 19 Nova Scotia Companies Act.

indicated that the ongoing CDD process has not yet been completed for all legal entities. For some DNFBPs as outlined in R.22, certain limited CDD obligations apply as discussed under R.22 but those do not amount to a comprehensive requirement to identify and take reasonable measures to verify beneficial ownership information and the obligations also are inoperative with regards to lawyers.

(ii) The federal and provincial company registries record some basic information as discussed above, but do not generally collect information on beneficial owners. Verification mechanisms for registered information are not in place. The CRA as part of its general obligations, collects information on legal entities that file tax returns. As indicated in the 2008 MER, however, this information generally does not comprise beneficial ownership information. Furthermore, not all legal entities in Canada file tax returns with the CRA; and

(iii) Legal entities themselves are required to collect certain information on holders of shares but no mechanisms are in place to ensure that the registered information is accurate.

(iv) For public companies listed on the stock exchange, disclosure requirements exist for shareholders with direct or indirect control over more than 10% of the company's voting rights.

As outlined under R.9 and 31, LEAs have adequate powers to obtain information from FIs, DNFBPs and any other types of companies and the CRA. However, the process of linking a specific FI with a legal entity or partnership subject to the investigation and accessing beneficial ownership information may not be timely in all cases. In sum, while some of the information collection mechanisms have been strengthened since 2008, deficiencies with regards to the collection and availability of full and updated beneficial ownership information remain and timely access by law enforcement authorities to such information is not guaranteed in all cases.

Criterion 24.7— As indicated under criterion 24.6, FIs are required to collect and update beneficial ownership information. The registries, the CRA and legal entities themselves are not required to ensure that accurate and updated beneficial ownership information is collected.

Criterion 24.8— Companies on both federal and provincial levels are obliged to grant the Director under the relevant Act access to certain information, including in relation to company share registers (Article 21 CBCA). There is no legal obligation on corporations or partnerships to authorize one or more natural person resident in Canada to provide to competent authorities all basic information and available beneficial ownership information; or for authorizing a DNFBP in Canada to provide such information to the authorities.

Criterion 24.9— Legal entities are required to maintain accounting records for six years, but not from the date of dissolution, but of the financial year to which they relate. In addition, pursuant to s.69 of the PCMLFTR FIs/some DNFBPs holding information on legal entities must keep that information for five years from termination of the business relationship or completion of the transaction. The Director retains corporate records submitted under the CBCA for a period of six years, except for articles and certificates which are kept indefinitely. In addition, s.225 of the CBCA requires a person who has been granted custody of the documents or records of a dissolved corporation to produce those records for six years following the date of its dissolution or such

shorter period as ordered by a court. Non-financial documents or records must be kept by the corporation until the corporation is dissolved; and then for another six years or less period as ordered by a court. The CRA, in partnership with the National Archivist of Canada, retains documents obtained or created by the CRA for various periods of time depending on the nature of the information. In relation to questions of beneficial ownership, the relevant retention periods are five to ten years, in some instances indefinitely.

Other Requirements

Criterion 24.10— Some basic company information is publicly available on various federal and provincial government websites and is therefore available to the authorities in a timely fashion. For information that is not publicly available, a wide range of law enforcement powers are available to obtain beneficial ownership information, including search warrants, using informants, surveillance techniques, wiretaps and production orders, and public sources (e.g.: law enforcement databases, city databases, corporate companies, civil proceedings, bankruptcy records, divorce records, civil judgments, land titles and purchase, building permits, credit bureau, insurance companies, liquor and gambling licenses, death records, inheritance, shipping registers, federal aviation, trash searches, automobile dealerships) and private source information searches. To be able to compel an FI to produce records pertaining to the control or ownership structure of a legal entity or legal arrangement, LEAs must first establish the link between a legal entity and a specific FI. Several tools are available to this effect (e.g.: grid search request to all D-SIBs to establish if they count the target person amongst their customers, VIRs to FINTRAC, requests to Equifax, mortgage and loan checks , consultations of NEPS to obtain an economic profile of an individual or private or public company). Investigative techniques may also be used (e.g. informants, witnesses, wiretaps). The RCMP may also request information from the CRA once charges have been laid in a criminal case, and on the basis of a judicial authorization. Prior to the prosecution stage, a tax order under the CC can be obtained for the RCMP to receive tax information from the CRA on a specific entity. Since 2014, the CRA may also share information with the RCMP on its own motion in cases where the CRA considers that there are reasonable grounds to believe that the information in its possession would provide evidence of listed serious offenses, including ML, bribery, drug trafficking and TF. In relation to tax crimes, the CRA CID may also obtain information. The relevant Director under each corporate statute—in the case of the CBCA the Director of Corporations Canada— also has the authority to inspect a corporation's records. Once it is established that a specific RE maintains a business relationship with a legal entity, LEAs may obtain a court order and deploy the measures available under criminal procedures to obtain, compel the production of, or seize relevant information—including beneficial ownership information—from any person, as discussed under R.31.

Criterion 24.11— Bearer shares are permitted both under the CBCA and several provincial company laws (for companies limited by shares).[127] While the CBCA generally requires the issuance of shares to be in registered form, the CBCA also makes provision for the issuance of certain types of shares in bearer form. In the absence of an express prohibition, the CBCA, therefore, still leaves some

[127] Quebec, Prince Edward Island, North-Western Territories and Nunavut allow for the issuance of registered shares only.

room for the issuance of bearer shares and no safeguards are in place to ensure that such shares are not being misused for ML or TF purposes.

Criterion 24.12— The CBCA requires corporations to keep shareholder registers in relation to registered shares, whereby the term "holder" of a security is defined as "a person in possession of a security issued or endorsed to that person." Under Part XIII of the CBCA, the holder of a share is permitted to vote at a meeting using someone else to represent them. The CBCA permits a registered shareholder to authorize another person to vote on their behalf. The proxy form itself lists the registered shareholder and the name of the "proxyholder" or person acting on their behalf. The proxy is recorded at the shareholder meeting, which provides transparency in respect of the identity of these individuals. However, the outlined arrangement still allows for nominee shareholding arrangements if the relevant shares are not voted. CBCA, s.147 permits, for example, securities brokers, FIs, trustees, or any nominees of such persons or entities to hold securities on behalf of another person who is not the registered holder but beneficial owner of that security. Similar provisions are found in provincial legislation such as, for example, Alberta Business Corporations Act, s.153 and Quebec's Business Corporations Act, s.2. Corporate directors are not permitted under the CBCA and provincial statutes. Nominee director arrangements in form of one natural person formally acting as director on behalf of another person may, however, still exist. Nominees (whether shareholders or directors) are not required to be licensed, or disclose their status, or to maintain information on or disclose the identity of their nominator. However, under the PCMLFTR, legal entities when opening a bank account, are required to provide details on the natural person that owns or controls a legal entity, which would include the nominating shareholder or director. For publicly listed companies, the risk of abuse of nominee shares is properly mitigated based on rigid reporting obligations for change of shares in excess of 10%. In sum, for companies other than those listed on the stock exchange, there are insufficient mechanisms in place to ensure that nominee shareholders are not misused for ML or TF purposes.

Criterion 24.13— Under the CBCA and provincial company laws violation of a company's disclosure, filing or record-keeping obligations may be fined with up to CAD 5 000 and/or imprisonment for up to six months in case of a violation by a natural person acting on behalf of the company. FIs and those DNFBPs covered under the law are subject to criminal (imprisonment for up to six months and/or a fine of up to CAD 50 000) as well as administrative sanctions if they fail to comply with their identification obligations with regards to legal entities (PCMLTFA, ss.73.1 and 74). In addition, officers, directors and employees of FIs and DNFBPs may be subject to sanctions regardless of whether the FI or DNFBP itself was prosecuted or convicted, as discussed under R.35. In summary, the statutory sanctions available are proportionate and dissuasive.

Criterion 24.14— Some basic information in the federal and provincial company registers is publicly available and can be directly accessed by foreign authorities. For other information, the powers and mechanisms described under criteria 37.1 and 40.9, 40.11, and 40.17 to 40.19 apply.

Criterion 24.15— Information on the quality of assistance received from other countries in the context of MLA and in response to ownership information requests is kept by the International Assistance Group (IAG) at the Department of Justice. The IAG maintains a copy of the requests made,

the follow-up that takes place with regards to each request, and keeps copies of all documents and information provided in response to the request. When forwarding the relevant information to the requesting agency, the IAG inquires with that agency, whether the request should be considered fulfilled. The authorities stated that the information collected by IAG suggests that the assistance received is generally adequate, although the result vary according to the particular component of basic/beneficial ownership sought.

Weighting and Conclusion

Serious gaps remain under criterion 6 with respect to the availability of beneficial ownership information for legal entities and partnerships.

Canada is partially compliant with R.24.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Canada was rated PC with former R.34 as the obligations to obtain, verify, and retain beneficial ownership information was considered to be inadequate. Since then, changes have been introduced to the PCMLTFR to strengthen FI obligations with regards to the identification and verification of beneficial ownership information for legal arrangements (whether created in Canada or elsewhere). In addition, the CRA's power to disseminate tax information to LEAs have been enhanced, taxpayer information can be shared at the discretion of the CRA if the CRA has reasonable grounds to believe that the information will afford evidence of certain designated offenses, including ML under CC s. 462.31. However, it is not clear for how many of the millions of trusts estimated to exist under Canadian law beneficial ownership information is available and access to such information is in any case difficult to obtain as there is no requirement for trustees to be licensed or registered.

Canada allows for the establishment of common law trusts as well as civil law fiducie (in Quebec). There is no general registration requirement for trusts, and trustees may but do not have to be licensed individuals or entities under the PCMLTFA. No specific statutes regulate the operation of foreign trusts in Canada, or require the registration of such foreign trusts.

Criterion 25.1— In the case of professional trustees, the customer due-diligence obligations vary depending on the trustee's profession: TCSPs are not subject to the general identification and verification obligations under the PCMLTFA as outlined under R.22. The CDD obligations applied to accountants have limitations as discussed in R.22. The requirements for lawyers are inoperative as a result of a Supreme Court decision. Trustees other than professional trustees are not subject to any statutory customer due diligence or record-keeping obligations.

Criterion 25.2— TCSPs are not covered under the scope of the PCMLFTR. Accountants are subject to basic ongoing CDD measures that do not amount to a comprehensive obligation to obtain and take reasonable measure to verify the identity of beneficial owners. Other trustees are not subject to comprehensive CDD or record-keeping requirements, as indicated under criterion 1.

Criterion 25.3— There is no obligation on trustees to disclose their status without being prompted, but under the PCMLFTR, FIs are required to determine whether a customer is acting on behalf of someone else, to establish the control and ownership structure of legal entities they are providing services to, and to obtain the names and addresses of all trustees, known beneficiaries and settlors.

Criterion 25.4— There is no prohibition under Canadian law for trustees to provide trust-related information to competent authorities, except in the case of lawyers where legal privilege may prevent authorities from accessing such information.

Criterion 25.5— Where there are suspicions of a crime, LEAs may deploy a wide range of investigative measures to obtain, compel the production of, or seize relevant information from any trustee, whether subject to the PCMLFTR or not. The extent to which the information available would include beneficial ownership information and information on the trust assets is unclear, as apart from the PCMLFTR, no legal requirements to maintain such information exist. Furthermore, linking a specific FI or DNFBP with a legal entity or partnership subject to the investigation and accessing beneficial ownership information may not be timely in all cases. With regards to FIs and accountants and trust companies acting as trustees, LEAs may also obtain information available to FINTRAC in its capacity as FIU through a request for voluntary information records. FINTRACs powers to access such information are, however, limited as outlined under criterion 29.2. In situations where a trust owes taxes and is required to file income tax returns, the CRA also has access to certain trust information, including the name and type of the trust and certain financial information on the trust. Information available to the CRA typically includes beneficiary, but not beneficial ownership information. The CRA may share taxpayer information upon request by LEAs either based on a court order or after criminal charges have been laid; or upon its own initiative if the CRA has reasonable grounds to believe that the information will afford evidence of certain designated offenses, including ML under CC, s462.31.

Criterion 25.6— The authorities may exchange information on trusts with foreign counterparts based on the procedures outlined under criteria 37.1 and 40.9, 40.11, and 40.17 to 40.19 and 11. LEAs have wide powers to exchange information with foreign counterpart. FINTRAC as well as the CRA may also share information with foreign counterparts as part of their respective functions. Investigative measures to obtain beneficial ownership can be taken upon foreign request.

Criterion 25.7— Under the PCMLFTR, failure to comply with the identification, verification or record-keeping requirements is subject to a range of criminal and administrative sanctions (see write-up under R.35 for more details). Trustees other than accountants are not subject to the AML/CFT framework. Violations of the principles of a trustees' breach of fiduciary duties may give rise to claims by the beneficiary and legal liability of the trustee based on these claims. However, in the absence of a specific obligation to collect and maintain beneficial ownership or general trust information there are also no sanctions available to authorities for a failure of the trustee to do so.

Criterion 25.8— For accountants, a the PCMLFTR sanctions may be applied by supervisory authorities as discussed under criterion 27.4. For other trustees, however, no sanctions are in place in the case of a failure to grant competent authorities timely access to trust related information.

Weighting and Conclusion:

Canada is non-compliant with R.25.

Recommendation 26 – Regulation and supervision of financial institutions

In the 2008 MER, Canada was rated PC with former R.23 due to the exclusion from the AML/CFT regime of certain sectors without proper risk assessments, an unequal level of supervision of AML/CFT compliance, lack of a registration regime for MSBs and concerns around fit and proper screening requirements. Canada made significant progress since then.

Criterion 26.1— FINTRAC is the AML/CFT supervisor for all REs subject to the PCMLTFA. It is assisted in the regulation and supervision of FIs by other federal and provincial regulators that are responsible for prudential and conduct supervision. However, ultimate responsibility for supervision and sanctioning under the PCMLTFA remains with FINTRAC. It is estimated that 80% of Canada's financial sector market is controlled by FRFIs. FRFIs are under the supervision of OSFI and include six large conglomerates (DSIBs) that hold a substantial share of the financial sector and other financial entities such as banks, insurance companies, cooperative credit and retail associations, trust companies and loan companies. OSFI's powers are mandated under the OSFI Act and governing legislation for the various financial sectors such as the *Bank Act*, *Trust and Loan Companies Act, Insurance Companies Act* and *Cooperative Credit Associations Act*. Non-FRFIs (e.g. credit unions) are regulated and supervised by provincial regulators under provincial statute.

AML/CFT supervisory functions are concentrated in FINTRAC and have not been delegated to primary regulators in Canada. At the federal level, OSFI and FINTRAC concurrently assess FRFI's for compliance with AML/CFT compliance obligations and are moving to a joint examination process (see further details below). At the provincial level, FINTRAC conducts AML/CFT supervision on non-FRFIs with the cooperation of other supervisors and has signed 17 MOUs with supervisors in relation to non-FRFIs. FINTRAC is authorized to share information with primary regulators at national and provincial levels relating to AML/CFT to monitor compliance with the PCMLTFA, and such regulators are also authorized to share information with FINTRAC.

Market Entry

Criterion 26.2— Federal and provincial authorities are the primary regulators of FIs with responsibility for prudential and conduct supervision including the licensing and registration of market entrants. FINTRAC is responsible for the registration and supervision of MSBs (along with AMF for MSBs operating in Quebec).

Market entry rules for FRFIs are set out in the relevant federal governing legislation and the process is entirely under the control and direction of OSFI. The Minister of Finance is responsible for approving Letters Patent creating domestic FRFIs, and for authorizing foreign banks and life insurance companies to operate branches in Canada by means of Ministerial Orders. OSFI is responsible for managing the process leading up to Ministerial actions. Authorized banking is

regulated both at the federal and provincial levels and it is not possible for the process to permit the creation or authorization of shell banks.

The following table sets out the licensing or registration requirements in Canada.

Reporting Entities	Primary Regulator	Licensed/Registered	Legislation
Banks	Federal-OSFI	Licensed. Domestic banks are created by the Minister pursuant to an incorporation process discussed below. Authorized foreign banks receive certificates to operate by one or more branches in Canada.	Bank Act
Cooperative Credit and Retail Associations [128]	Federal-OSFI for Cooperative Retail Associations; Provincial-Cooperative Credit Associations	Same as domestic banks	Cooperative Credit Associations Act
Credit Unions and *caisses populaires*	Provincial authorities	Registration	Legislation includes Credit Unions Act; Financial Institutions Act; Credit Union Incorporation Act; Credit Unions and *Caisses Populaires* Act; Deposit Insurance Act; An act respecting financial services cooperatives; An Act respecting the Mouvement Desjardins
Life Insurance Companies	Federal-OSFI Provincial authorities	Licensed [129] Either licensed or registered	Insurance Companies Act Legislation includes Insurance Act; Financial Institutions Act; Insurance Companies Act; Life Insurance Act; Registered Insurance Brokers Act; An Act respecting insurance (Quebec); An Act respecting the distribution of financial products and services(Quebec); Saskatchewan Insurance Act

[128] OSFI's oversight of Cooperative Credit Associations, commonly referred to as credit union centrals, is limited and quite different from its oversight of banks and other FRFIs. Cooperative Credit Associations are organized and operated based on cooperative principles. With the exception of the Credit Union Central of Canada ('CUCC'), the Cooperative Credit Associations are provincially incorporated, and regulated and supervised at the provincial level. The CUCC, which is federally incorporated, functions as the national trade association for the Canadian credit union system and does not provide any financial services. Cooperative Retail Associations are federally incorporated and supervised by OSFI in the same way as for banks and other FRFIs.

[129] Domestic life insurance companies under OSFI's jurisdiction are created by the Minister pursuant to an incorporation process discussed below. Authorized foreign life insurance companies only operation under the federal legislation and receive Ministerial Orders permitting one or more branches in Canada.

Reporting Entities	Primary Regulator	Licensed/Registered	Legislation
Life Insurance Brokers and Agents	Provincial authorities	Licensed or registered	Legislation includes Insurance Act; Financial Institutions Act; Insurance Companies Act; Life Insurance Act; Registered Insurance Brokers Act; Saskatchewan Insurance Act; An Act respecting insurance (Quebec); An Act respecting the distribution of financial products and services (Quebec)
Trust and Loan Companies	Federal-OSFI Provincial authorities	Licensed Licensed or registered	Trust and Loan Companies Act Legislation includes Loan and Trust Corporations Act; Financial Institutions Act; Corporations Act; Trust and Loan Companies Act; Trust and Loan Companies Act; Deposit Insurance Act; An act respecting trust companies and savings companies (Quebec)
Investment Dealers	IIROC Provincial authorities	Registration Licensed (Northwest Territories) or registered	IIROC Dealer Member Rules Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Mutual Fund Dealers	Mutual Funds Dealers Association Provincial authorities	Registered Licensed (Northwest Territories) or registered	MFDA Rules Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Investment Counsel and Portfolio Management Firms	Provincial authorities	Licensed (Northwest Territories) or registered	Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Other securities firms	Provincial authorities	Licensed (Northwest Territories) or registered	Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Money Service Businesses	FINTRAC *Autorité des marchés financiers* (Québec)	Registration Licensed	PCMLTFA and PCMLTF Registration Regulations Money-Services Business Act

Criterion 26.3— Federal and provincial regulators are responsible for carrying out fit-and-proper tests on persons concerned in the management or ownership of FIs in Canada. The measures are used to prevent criminals or their associates from holding a significant or controlling interest in an FI in Canada.

OSFI conducts fit-and-proper tests on FRFIs at the application stage to assess the fit-and-proper status of applicants, their principals (beneficial owners), senior management and Boards of Directors. Fit-and-proper tests are conducted under the Bank Act (ss.27, 526 and 675), Trust and Loan Companies Act (s.26), Cooperative Credit Associations Act (s.27) and Insurance Companies Act (ss.27 and 712). OSFI requires that applicants provide details of whether applicants have been the subject of any criminal proceedings or administrative sanction and it conducts security screening.

OSFI has the authority to apply fit-and-proper tests during the lifetime of a FRFI but only applies this authority directly to changes of ownership and/or shareholding. To address changes in directors or senior managers, OSFI has issued Guideline E-17 "Background Checks on Directors and Senior Managers of Federally Regulated Entities" in that regard. These requirements are applied throughout the life of FRFIs. After an FRFI is licensed, fit-and-proper testing on new senior officers and Directors is conducted by the FRFI rather than by the regulator. However, OSFI continues to apply fit-and-proper checks on new shareholders. OSFI assesses FRFIs' compliance with the Guideline and has issued prudential findings on background checks conducted by FRFIs on responsible persons. Since 2014, FRFIs are required to notify OSFI of plans to appoint or replace senior managers or directors.[130]

Persons and entities operating and controlling MSBs are required to register with FINTRAC under the PCMLTF Registration Regulations. FINTRAC conducts criminal record checks when assessing applications for registration as MSBs and it can refuse or revoke registrations where a person has been convicted of certain criminal offenses.

Provincial regulators apply fit-and-proper controls to assess the suitability of persons who control, own or are beneficial owners of provincially regulated FIs. General fit-and-proper requirements apply in the securities and insurance sectors. For example, the Investment Industry Regulatory Organization of Canada (IIROC) evaluates whether an individual appears to be "fit and proper" for approval/registration and /or whether the individual's approval is otherwise not in the public interest. Included in the criteria are the evaluation of an individual's integrity and criminal record. Provincial securities regulators apply similar criteria. In addition, MSBs located in Quebec are subjected to a "fit-and-proper" test by the *Autorité des marches financiers* (AMF) under the *Money Services Business Act* (Quebec).

Provincial regulators have not adopted fitness and probity requirements for persons owning or controlling financial entities after market entry to the same extent as what is achieved at federal level.

Risk-Based Approach to Supervision and Monitoring

Criterion 26.4— OSFI and provincial regulators are responsible for prudential and conduct supervision of Core Principle institutions in Canada under the OSFI Act, provincial legislation and other governing legislation. OSFI applies an AML/CFT assessment program as part of the Core Principles-based prudential supervision of FRFIs. All FRFIs are supervised by OSFI on a consolidated

[130] OSFI issued an Advisory on Changes to the Membership of the Board or Senior Management.

or group basis, as required by the Core Principles. Canada underwent an IMF FSAP in 2013 and OSFI was found to comply with the implementation of the Core Principles in the banking and insurance sectors and was rated LC.

FINTRAC is responsible for the supervision of all REs for AML/CFT compliance under the PCMLTFA, including Core Principles institutions supervised by OSFI and provincial prudential regulators. OSFI and FINTRAC have a coordinated approach to supervision of Core Principles institutions that are FRFIs. FINTRAC consults and coordinates with other federal and provincial prudential supervisors and has signed 17 MOUs with regulators to exchange compliance related information.

Both OSFI and provincial regulators adopt a risk-based approach to identify firms that have a higher risk of AML/CFT activities. In 2013, OSFI and FINTRAC adopted a concurrent approach to conduct AML/CFT examinations in the FRFI sector. Non-Core Principles institutions are supervised by FINTRAC for compliance with the PCMLTFA. FINTRAC also receives information from provincial regulators arising from their prudential/conduct supervisory activities that may be relevant to AML/CFT compliance. MSBs are registered and supervised by FINTRAC (and AMF in Quebec) for compliance with the PCMLTFA.

Criterion 26.5— AML/CFT supervision is conducted in Canada on a risk-sensitive basis. A shorter version of the NRA identifying the inherent ML/TF risks in Canada has recently been published and the findings are being incorporated into supervisors' compliance activities. Supervisors have their own operational risk assessment models and they use a range of programs, activities and tools to supervise and monitor compliance with AML/CFT requirements. There has been an increase in the frequency and intensity of on-site and offsite supervision of FIs in recent years. There has also been an increase in resources at FINTRAC to carry out compliance activities since the last MER.

FINTRAC has developed an AML/CFT Supervisory Program that is risk-based to ensure that REs are complying with their obligations under the PCMLTFA. It uses an enhanced risk-assessment model to assign risk ratings to REs that allows the allocation of resources according to higher-risk areas. Its risk model relies on information such as media information, ML/TF intelligence, financial transaction reporting behaviour, information received from law enforcement and regulatory partners that have MOUs with FINTRAC. It is updated regularly using information it collects through intelligence and examinations and is adjusted following on-site and off-site examinations. The risk assessment carried out on FRFIs is done in collaboration with OSFI.

FINTRAC's Supervisory Program is influenced and guided by a number of factors including the risk rating of the RE using the enhanced risk-assessment model and using other tools such as the examination selection strategy. FINTRAC focuses its supervisory activities on a risk-based approach using higher-intensity activities for higher-risk REs and using other lower-intensity activities for medium- and lower-risk entities. FINTRAC's primary tool to supervise for AML/CFT compliance is its examinations strategy that is well developed. The examination strategy developed by FINTRAC prioritized activities aimed at REs that have been found to be non-compliant previously and those with high-risk ratings. It also focuses on key industry players with large market shares, which are examined regularly, given the inherent risks that are associated with their size and respective

business models and the consequences of non-compliance. FINTRAC also has a range of offsite mechanisms to conduct supervision of FIs including compliance assessment reports (CAR), desk-based reviews, monitoring of financial transactions, observation letters, compliance enforcement meetings, IT tools, voluntary self-disclosures of non-compliance and other awareness/assistance tools. CARs are used to segment REs within a sector, with results being used to initiate desk and on-site exams.

OSFI applies a risk-based approach to AML/CFT supervision. It has an AML/CFT risk assessment separate from its prudential risk assessment model for FRFIs and directs its assessment program at Canada's largest banks and insurance companies and other FRFIs considered at highest risk of ML and TF. OSFI's risk assessment methodology focuses on the vulnerabilities of FRFIs to ML and TF, looking at factors such as size, geographical spread, products, services and distribution channels and quality of risk management generally. It assigns a risk profile on each institution considering the risk factors and the quality of its risk management. OSFI's risk assessment results in a classification of FRFIs into categories of high, medium and low risk based on a combination of inherent risk, coupled with broader prudential views on the quality of risk management. OSFI supervises FRFIs on a group-wide basis and it conducts examinations of FRFI's on a cyclical basis depending on an FRFI's risk ratings and when information is received from prudential supervisors and other regulators including FINTRAC. OSFI also monitors major events or developments impacting the management or operations of FRFIs that informs both the content of AML/CFT assessments and also the assessment planning cycle.

FINTRAC and OSFI have agreed a concurrent approach to AML/CFT supervision of FRFIs allowing for concurrent examinations in addition to individual examinations that both supervisors can conduct of FRFIs. Both OSFI and FINTRAC exchange information that is relevant to FRFI's compliance with AML/CFT obligations. FINTRAC and provincial regulators also exchange information and FINTRAC can conduct AML/CFT follow-up activities with provincially regulated REs when AML/CFT issues are reported to it. Other supervisors also adopt risk assessments and supervision that are related to AML/CFT. For example, IIROC uses a risk assessment model for IIROC-regulated firms to determine priority focus and can apply an AML examination module by IIROC that is judged to present an AML/CFT risk. The primary responsibility for AML/CFT supervision remains with FINTRAC and any supervisory activity conducted by other supervisors' supplements, but does not replace, FINTRAC's responsibility to ensure compliance with the PCMLTFA and Regulations made thereunder.

Criterion 26.6— FINTRAC reviews its risk model on an ongoing basis and recently reviewed its sectoral analysis. FINTRAC also reviews its understanding of ML/TF risks for individual REs through reviewing the institution's compliance history, reporting behaviour and risk factors. In its ongoing review of the risk assessment, FINTRAC regularly monitors and assesses actionable intelligence, ML/TF risks and trigger events. OSFI reviews its AML/CFT risk profiles of FRFIs periodically. Risk assessments are applied to DSIBs on a continuous basis, reflecting their dominance of the FRFI sector and their very high-risk level. On-site assessments of DSIBs are conducted on a regular basis and DSIBs may be subject to more intensive supervision (staging) where deficiencies have been identified. The review of the risk profiling of other high-risk FRFIs is updated at less frequent

intervals, due to their less complex risk profiles. Provincial regulators are also kept apprised of ML/TF risks by FINTRAC and through the recently published NRA.

Weighting and Conclusion

Further fitness and probity controls are required.

Canada is largely compliant with R.26.

Recommendation 27 – Powers of supervisors

In the 2008 MER, Canada was rated LC with these requirements, notably because FINTRAC had no power to impose AMPs on REs. This has been remedied in December 2008.

Criterion 27.1— FINTRAC has authority to ensure compliance by all REs with parts 1 and 1.1 of the PCMLTFA (s.40). OSFI and provincial supervisors also have supervisory powers over REs under their own supervisory remit under federal and provincial legislation: e.g. the OSFI Act indicates the Superintendent's powers and duties in relation to the Bank Act, Trust and Loan Companies Act, the Cooperative Credit Associations Act and the Insurance Companies Act and the supervisory powers of the Superintendent are uniform under these Acts.

Criterion 27.2— FINTRAC has the authority to conduct inspections of FIs under the PCMLTFA. It can carry out on-site examinations of REs under PCMLTFA, s.62(1). Such examinations can be routine (with notice) but FINTRAC also has the authority to conduct unannounced examinations of REs under the PCMLTFA. OSFI has no mandate under PCMLTFA, but it supervises FRFIs under the OSFI Act and FRFIs' governing legislation (e.g. Bank Act) to determine whether they are in sound financial condition, are managed safely and are complying with their governing statute law. IIROC and provincial regulators conduct audits of registered firms to ensure compliance with Canadian securities laws.

Criterion 27.3— FINTRAC is authorized under the PCMLTFA to compel production of any information relevant to monitoring compliance with AML/ATF requirements. It can enter any premises (except a dwelling house) to access any document, computer system and to reproduce any document "at any reasonable time" (PCMLTFA, ss.62(1) and (2)). FINTRAC also has the authority to require REs to provide any information that FINTRAC needs for compliance purposes (s.62). There is a 30-day period given to deliver the information (PCMLTFR, s.70). OSFI has general powers to compel information from REs under OSFI Act, s.6 and federal governing legislation. While not mandated under the PCMLTFA, other regulators have the power to compel information under provincial or governing legislation to protect the public and market integrity. FINTRAC can exchange information on compliance with Parts 1 and 1.1 of the PCMLTFA with federal and provincial agencies that regulate entities.

Criterion 27.4— FINTRAC and OSFI have a range of supervisory tools to sanction REs for non-compliance. These tools include supervisory letters, action plans for FRFIs, staging by OSFI, compliance agreements, revocation of registration of MSBs by FINTRAC, revocation of FRFIs'

licenses by the AG of Canada[131] and criminal penalties. The PCMLTFA AMP Regulations provide FINTRAC with the power to apply AMPs to any FI and DNFBPs subject to the AML/CTF regime for non-compliance with the PCMLTFA. Provincial regulators, IIROC and MFDA have the power under their own governing legislation to conduct investigations and undertake enforcement action where necessary to protect the public and market integrity. They have the power to restrict, suspend and cancel registration. Further information is provided under the analysis of R.35.

Weighting and Conclusion:

Canada is compliant with R.27.

Recommendation 28 – Regulation and supervision of DNFBPs

In the 2008 MER, Canada was rated NC with these requirements (pages 229–243) notably because of deficiencies in the scope of the DNFBPs covered and not subject to FINTRAC supervision, and the sanction regime and resources available to FINTRAC were considered inadequate. Since then, the scope of DNFBPs under the supervision of FINTRAC has been extended to BC Notaries and DPMS, and FINTRAC was granted the power to impose sanctions under the PCMLTF AMP Regulations.

Casinos

Criterion 28.1— *a)* Gambling activities are illegal in Canada, except if conducted and managed by the province or pursuant to a license issued by the province on the basis of CC, ss.207(1)(a) to (g), and three different models are in place (charity, commercial casinos, First Nation casinos, as described in the 2008 MER pages 214–215). Internet gambling are not subject to AML/CFT obligations, as the amendment to the definition of casino under PCMLTFA[132] is not yet into force, as well as ship-based casinos (the latter is a very minor issue, considering that, according to the authorities, no Canadian cruise ship are currently being operated, and lottery schemes cannot be operated within 5 nautical miles of the Canadian shore). Several provinces have introduced internet gambling (British Columbia, Quebec, Manitoba, Nova Scotia, Prince Edward Island, New Brunswick, and Newfoundland). Under the provincial legislation, also lottery schemes performed through Internet are required to be licensed.

b) All provinces and territories have regulation on terms and conditions for obtaining the license and a regulatory authority empowered to administer the relevant provincial legislation. Due-diligence requirements of the applicants (casino operator, key persons associated with the applicants and executive members) are part of the licensing process, where financial, business information, information referring to criminal proceedings, and reputational elements are required and subject to a review conducted by the competent provincial regulatory authorities. The licensing provisions make reference to due-diligence procedure related to an extensive notion of "associates" of the applicant, and when the applicant is a company or a partnership controls are extended to partners, directors, as well as to any subject who directly or indirectly control the applicant or has a beneficial

[131] This authority is subject to a number of conditions as set out in federal governing legislation.
[132] In particular, PCMLTFA, Section 5, k, (i).

interest in the applicant. Notice of changes in directors, officers, associated of the registrants are submitted to the approval of the competent regulatory authority. Notification of charges and convictions of the licensee, as well as of its officers, shareholders, owners are required. In respect of charities that require a license to conduct casino events eligibility requirements must be met both where a charitable model has been adopted[133] and where a corporation model is in place.[134] Charitable events may be licensed also by First Nations Authority under the agreement with the relevant provincial legislator (Manitoba, Saskatchewan),[135] where the authority to issue license to charitable gaming has been delegated by the competent provincial authorities in favour of First Nations commissions. Under the Agreements (Part 10.1) the parties agree that the terms and conditions that apply to licenses off and on reserve are essentially the same. Audits are performed in order to ensure that the operators comply with the terms and conditions of the license.

Under the relevant provincial legislation, the same provisions apply also to lottery schemes performed through Internet.

The table below summarizes the list of casino's regulators identified under the provincial gaming legislation and the relevant legislation. Licensing authorities do not have express AML/CFT responsibility to qualify as competent authorities.

Province	Regulator	Provincial Legislation
Alberta	Alberta Gaming &Liquor Commission	Gaming and Liquor Act
British Columbia	Gaming Policy and Enforcement Branch	Gaming Control Act
Manitoba	Liquor and Gaming Authority of Manitoba First Nations Gaming Commissions at reserve charitable gaming within the municipality or on reserve	Liquor and Gaming Control Act
New Brunswick	Gaming Control Branch-Department of Public Safety	Gaming Control Act
Nova Scotia	Nova Scotia Alcohol and Gaming Division	Gaming Control Act

[133] Pursuant to Section 20.(1) of the Gaming and Liquor Regulation in Alberta charitable or religious organisation in order to qualify for the license must satisfy the board that the proceeds generated from the gaming activities must be used for charitable and religious activities. In this context, the volunteers of charities are allowed to work in key positions at the casino events only if licensed, thus being subject to criminal record checks. The Commission must ensure that the licensed organisation comply with the relevant legislation.
[134] Where Lottery Corporations are empowered to conduct and manage gaming on behalf of the provincial government, group or organization can be licensed to hold a gaming event by the competent regulator. In British Columbia background investigations may be conducted also in respect of the eligible organisation, its directors, officers employees or associated (Section 80 (1) (g) (vi) of the Gaming Control Act. Audit of the licensee are performed conducted by the Charitable Gaming Audit Team of the Gaming Policy and Enforcement Branch.
[135] In Saskatchewan the Provincial regulatory authority, SLGA, owns and manage the slot machines at six casinos operated by the Saskatchewan Indian Gaming Authority, a non-profit corporation licensed by SLGA, while the Indigenous Gaming Regulator has a delegated authority under 207 (1) (b) of the CC to issue charitable gaming licenses on designated reserves.

Province	Regulator	Provincial Legislation
Ontario	Alcohol and Gaming Commission of Ontario	Gaming Control Act Alcohol and Gaming Regulation and Public Protection Act
Quebec	*Régie des alcools des courses et des jeux*	Act Respecting Lotteries, Publicity Contest and Amusement Machines An Act respecting the *Société des lotteries du Québec.*
Saskatchewan	Saskatchewan Liquor and Gaming Authority IGR responsible for licensing and regulating charitable gaming on First Nations, operating through a Licensing Agreement with SLGA (2007).	The Alcohol and Gaming Regulation Act
Yukon	Professional Licensing & Regulatory Affairs Branch	Lottery Licensing Act Sec 2 (Eligibility) and Sec 10 (Regulations) of the Lottery Licensing Act
Newfoundland and Labrador	Department of Government Services and Lands, Trades Practices and Licensing Division (no specific provisions)	Lottery schemes-General rules
Prince Edward Island	PEI Lotteries Commission /Department of Community and Cultural Affairs for casinos charities	Lotteries Commission Act
Northwest territories	Consumer Affairs, Department of Municipal and Community Affairs	Lotteries Act Lottery Regulations
Nunavut	Department of Community and Government Services	The Lotteries Act and Regulations

c) FINTRAC is the only competent supervisory authority for compliance of casinos with AML/CFT requirements. It has signed the MOUs with the following regulators: Alcohol and Gaming Commission of Ontario (AGCO); British Columbia Gaming Policy Enforcement Branch (GPEB); Alcohol and Gaming Division of Service Nova Scotia; Saskatchewan Liquor and Gaming Authority (SLGA). Online gambling is not covered by the definition of casino currently into force under PCMLTFA.

DNFBPs Other than Casinos

Criterion 28.2— FINTRAC is the designated competent authority under PCMLTFA and PCMLTFR for the AML/CFT supervision of all DNFBPs. FINTRAC supervises 26,000 DNFBPs in total, including casinos (discussed under 28.1), trust and loan companies, accountants, dealers in precious metals and stones, BC Notaries, and real estate agents and developers. As described under R.22 lawyers and Quebec notaries, trust and company service providers that are not included among the trust and loan companies are not monitored for AML/CFT purposes.

Criterion 28.3— All the categories of DNFBPs that fall into the scope of AML/CFT regime are monitored by FINTRAC for compliance with AML/CFT requirements. Apart from real estate dealers under certain condition, the AML requirements have not been extended to other categories in addition to those provided for in the FATF standards.

Criterion 28.4— *a)* FINTRAC powers to monitor and ensure compliance are the same for FIs and DNFBPs (PCMLTFA s. 62). For details, see R.27.

b) The powers to prevent criminals or their associates from being accredited, or from owning, controlling or managing a DNFBPs other than casinos are more limited. No specific measure is in place for DPMS. Referring to accountants the current process of creating a unified new professional designation, the Chartered Professional Accountant, replacing the former three (Chartered Accountants, Certified General Accountants and Certified Management Accountants), is at different stages in the various provinces. The provincial associations are in charge of ensuring high professional standards also through investigation of complaints and enforcement actions. In the admission to membership disclosure of investigations and disciplinary proceedings is required and consent must be provided permitting the Registrar to access the relevant information.[136] Members are also required to promptly inform CPA after having being convicted of criminal offenses.[137] Allegations for a wide set of crimes, included ML, financial frauds, TF, entail a rebuttable presumption of failing to maintain good reputation of the profession.[138] Accounting firms (partnerships, limited liability partnerships and professional corporations) are required to disclose investigations involving any partners[139] or shareholders and consent shall be provided permitting the Registrar to access information regarding such investigation. Any change in partners, shareholder must be notified and failure to provide such disclosure are considered breach of memberships obligations. Regarding BC Notaries, under the Notaries Act of BC, the Society of Notaries Public of BC is empowered to maintain standards of professional conduct. The procedure for the enrolment include screening procedure conducted by the Credentials Committee of the Society, where consent for disclosure of criminal records information in favour of the RCMP must be provided. Under the Notary Act also Notary Corporation (Notary Act, ss.57 and 58(f) of) are subject to a permit and the procedure imply controls on the voting shares members (that must be members of the Society in good standing, thus having passed the screening procedures described above related to disclosure of criminal records) as well as the non-voting members (who can be only members of the Society or relatives). The Society is empowered to impose fines, as well as take disciplinary action and revoke the permits (Notary Act, s.35). In respect of real estate agents, as shown in the attached each province has suitability requirements for licensee that apply as individual,[140] which in most cases entail the provision of Certified Criminal Records Checks. Nevertheless, in some cases the relevant provisions make reference both as a condition of refusal to issuing and to suspending or cancelling a license to the notion of "public interest,"[141] which, despite the authorities, consider broad to include a large number of factors, seems to be too vague and left to the discretion of the competent regulatory authorities. The integrity requirements in respect of

[136] Section 2 of Reg. 4-1 of CPA Ontario.
[137] Rule 102. 1 of the Rules of professional conduct CPA Ontario.
[138] Rule 201.2 of 1 of the Rules of professional conduct CPA Ontario.
[139] Regulations 4-6, Section 11, CPA Ontario.
[140] No specific integrity requirement under the Real Estate Agents Licensing Act. The convictions of offenses against the CC shall be related to qualifications, functions or duties of the agent/sales persons (Section 18, (k) and are cause for suspension or cancellation of license.
[141] Manitoba, Section 11(1) of the Real Estate Brokers Act, New Brunswick, Section 10 (2) of the Real Estate Act; Prince Edward Islands, Section 4 (3) of the Real Estate Trading Act.

corporations and partnerships are not always expressly extended to partners, directors, officers.[142] Not always changes in the directors, officers, shareholders, partners must be notified to the competent provincial Authority.[143] Furthermore, the relevant legislation is essentially orientated in a perspective of consumer's protection so that in some cases the condition for refusal of the license are previous convictions of indictable offense "broker-related,"[144] as well as the notification of licensee makes reference to convictions involving a limited set of offenses.[145] Moreover, as the presence of criminal records is not necessarily a bar to registration, a case-by-case approach is taken by the regulatory authority. Provincial legislation establishes an express exemption regime in favour of lawyers, trust companies[146] and in some cases accountants from the requirement for license in respect of real estate services provided in the course of their practice.

DNFBPS Category	Designated Competent Authority	Relevant Legislation	Market Entry Safeguards
Real Estate	**Regulatory Authority**	**Provincial Legislation**	
Alberta	Real Estate Council of Alberta	Real Estate Act, in particular Part 2, s. 17, Real estate Act Rules (20 (1) for individuals, ss 30 and 34 for real estate brokerage. s. 10.3 of Real Estate Regulations	All the provinces have suitability requirements for licensee that apply as individual. The integrity requirements in respect of corporations and partnerships are not always expressly extended to partners, directors, officers. Not always changes in the directors, officers, shareholders, partners must be notified to the competent provincial Authority
British Columbia	Real Estate Council of British Columbia	Real Estate Services Act ss 3 (1) and 10	
New Brunswick	New Brunswick Financial and Consumer Services Commission Division	New Brunswick Real Estate Act ss 3 and 4.2	
Newfoundland and Labrador	The Financial Service Regulation Division	Real Estate Trading Act, s. 7	
Manitoba	Manitoba Securities Commission for licensing	The Real Estate Brokers Act and The Mortgage Brokers Act	
Nova Scotia	Nova Scotia Real Estate Commission	Real Estate Trading Act ss.4, 12	
Ontario	Real Estate Council of Ontario	Real Estate and Business Brokers Act s. 9.1, 10 (19)	

[142] In Saskatchewan, for example, under Section 26.1 (b) of the Real Estate Act the integrity requirements are limited to officers and directors. The same requirement is established in Nova Scotia under 12 (1) (b) of the Real Estate Trading Act.
[143] Only change in officials and partners in New Brunswick, Section 15 (1) (b) and (c) of Real Estate Act partners in Prince Edward Island Section 14 of Real Estate Trading Act.
[144] Quebec, Section 37 of the Real Estate Brokerage Act.
[145] New Brunswick, Section 15 (2) of the Real Estate Act (frauds, theft or misrepresentation).
[146] See, for example in British Columbia, Real Estate Service Act, Section 3, (3) lett. e) and f) the exemption regime in favour of FI that has a trust business authorization under the Financial Institutions Act and practicing lawyers.

DNFBPS Category	Designated Competent Authority	Relevant Legislation	Market Entry Safeguards
Prince Edward Island	Office of the Attorney General, Consumer and Corporate and Insurance Services	Real Estate Trading Act, ss.4 (3), 8 (2) b); 14	
Quebec	*Organisme d'autoréglementation du courtage immobilier du Québec*	*Loi sur le courtage immobilier* ss.4, 6, 37	
Saskatchewan	Real Estate Commission	The Real Estate Act s. 18 (1) and 26 (1)	
Yukon Territories	Professional Licensing and Regulatory Affairs	Real Estate Agents Act, ss.6, 7	
Northwest Territories	Municipal and Community Affairs-Superintendent of Real Estate	Real Estate Agents Licensing Act, ss.2, 1; 8 (1); 18	
Nunavut	Consumer Affairs	Real Estate Agents Licensing Act	
Accountants and Accounting Firms	Chartered Professional Accountant, the Certified Management Accountant, the Certified General Accountant and provincial associations	conducts (as),	As regards admission to Membership see, for example, Certified Management Accountants of Ontario (Regulation 4-1); CMA Regulations of Alberta (s. 2 (2), where it is stated that each applicant for registration shall provide evidence on conviction of a criminal offense.
DPMS	**No designated competent authority**	-	**No measure in place**
BC Notaries	The Society of Notaries Public	the Notary Act	The procedure for the enrolment include screening procedure conducted by the Credentials Committee of the Society, where consent for disclosure of criminal records information in favour of the RCMP. Notary Corporation (ss 57 and 58 f the Notary Act) are subject to a permit and the procedure imply controls on the voting shares members (that must be in good standing) as well as the non-voting members (who can be only members of the Society or relatives)

c) There are civil and criminal sanctions[147] available for failure to comply with AML/CFT obligations for DNFBPs as described under R.35, as well as the public notice of AMPs imposed. The AMP regime allows administrative sanctions to be applied to REs although the maximum threshold raises doubts about the dissuasiveness and/or proportionality of sanctions for serious violations or repeat offenders. However, there is a range of measures available to supervisors to ensure compliance that are both proportionate and dissuasive.

All DNFBPs

Criterion 28.5— FINTRAC has further developed its risk model that lead to a risk classification (low, medium, high) of activity sectors and entities and the frequency and intensity of supervision is a function of FINTRAC's risk assessment. FINTRAC has started to integrate the results of inherent NRA for 2015/2016. The risk model takes into account numerous sources of information in order to assess the risk factor of specific REs. Further details on how the risk profile affects the scope and frequency of controls are provided under IO.3.

Weighting and Conclusion

AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. Online gambling, ship-based casinos, trust and company service providers that are not included among the trust and loan companies are not subject to AML/CFT obligations and not monitored for AML/CFT purposes. The entry standards and fit-and-proper requirements are absent in DPMS and TCSPs, while for the real estate brokerage they are not in line with the standards. Taking into account the deficiencies identified in the scope of DNFBPs and subsequent coverage of AML/CFT supervision and in the fit-and-proper requirements for DPMS, TCSPs and for the real estate brokerage

Canada is partially compliant with R.28.

Recommendation 29 - Financial intelligence units

In its third MER, Canada was rated PC with former R.26 (see paragraphs 364–418) notably due to the fact that the FIU (i) had insufficient access to intelligence information from administrative and other authorities, and (ii) was not allowed to gather additional information from REs. The first deficiency has since been addressed. The FATF standard was strengthened by new requirements which focus on the FIU's strategic and operational analysis functions, and the FIU's powers to disseminate information upon request and request additional information from REs.

Criterion 29.1— In 2000, Canada established an administrative FIU—Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which is a national centre for receiving, analysing and disseminating information in order to assist in the detection, prevention, and deterrence of ML, associated predicate offenses and TF activities: PCMLTFA, s.40. The definition of an ML offense

[147] Sections 73.1 to 73.24 of PCMLTFA.

under the PCMLTFA is based on the definition of the offenses established in the CC, which includes information related to associated predicate offense.[148]

Criterion 29.2— FINTRAC serves as a national agency authorized to receive STRs and other systematic reporting required by the PCMLTFA or the PCMLTF regulations, including Terrorist Property Reports, Large Cash Transaction Reports (of CAD 10 000 or more), SWIFT and Non-SWIFT Electronic Funds Transfer Reports (of CAD 10 000 or more), Casino Disbursement Reports (of CAD 10 000 or more), physical cross-border currency or monetary instruments reports and seizures reports and any financial transaction, or any financial transaction specified in PCMLTFA. In addition, FINTRAC is authorized to receive voluntary information records (VIRs), i.e. information provided voluntarily by LEAs[149] or government institutions or agencies, any foreign agency that has powers and duties similar to those of the Centre (i.e. FINTRAC), or by the public about suspicions of ML or TF activities.[150]

Criterion 29.3— *a)* FINTRAC may request the person or entity that filed a STR to correct or complete its report when there are quality issues such as errors or missing information, but not in other instances where this would be needed to perform its functions properly. According to the authorities, Canada's constitutional framework prohibits FINTRAC from requesting additional information from REs. This deficiency was highlighted in Canada's Third MER, and Canada's Sixth Follow-up Report concluded that, despite the information-sharing mechanism put in place by FINTRAC since its last evaluation, the deficiency has not been adequately addressed.

b) PCMLTFA, ss.54 (1) (a) to (c), states that FINTRAC may collect information stored in a database maintained, for purposes related to law enforcement or national security, by the federal government, a provincial government, the government of a foreign state or an international organization, if an agreement to collect such information has been concluded. FINTRAC has direct or indirect access to a wide range of law enforcement information, as the Canadian Police Information Centre (CPIC), the Public Safety Portal (PSP), CBSA's cross-border currency reports and seizure reports databases, RCMP's National Security systems and *Sûreté du Québec*'s criminal information and the Canada Anti-fraud Centre of the RCMP databases, as well as to the CSIS database. However, FINTRAC still has insufficient access to the information collected and/or maintained by–or on behalf of–administrative and other authorities, such as CRA databases.

Criterion 29.4— *a)* FINTRAC must analyse and assess the reports and information received and/or collected under PCMLTFA, ss.54(1)(a) and (b), namely, STRs, Large Cash Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports, physical cross-border currency or monetary instruments reports and seizures reports, information provided voluntarily by LEAs and

[148] See subsection 462.31(1) of the criminal code where "designated offence" means "a primary designated offence or a secondary designated offence" under section 487.04 of the CC.
[149] FINTRAC receives information provided voluntarily by CSIS, CBSA, CRA–Criminal Investigation Directorate–and the RCMP, as well as provincial and municipal police.
[150] VIRs are the mechanism used by LEAs and other partners of FINTRAC to send information to and advise FINTRAC of investigative priorities without creating an obligation on FINTRAC to respond so as to respect the principle of independence of the FIU. The majority of VIRs that FINTRAC receives focus on priority investigations. VIRs are often the starting point of FINTRAC's analysis (however, FINTRAC always maintains its ability to proactively develop cases).

other regime partners (i.e. the VIRs), queries from, foreign FIUs, as well as information collected from several databases or open source information (s. 54(1) (c) PCMLTFA).

b) FINTRAC is also required to conduct research into trends and developments in the area of ML and TF activities and to undertake strategic analysis (s. 58(1)(b) PCMLTFA). It does so by leveraging a range of open and classified sources of information. It publishes Typologies and Trends Reports[151] on a broad array of issues. From 2010 to 2015, it produced 62 strategic intelligence and research products, which identify ML/TF methods and techniques used by listed terrorist groups and criminal networks, emerging technologies, as well as vulnerabilities in different sectors (both covered and non-covered by the PCMLTFA). These reports provide feedback to REs, respond to Canada's intelligence priorities and build the evidence base for new policy development. FINTRAC has also participated to the working out of Canada's first formal NRA.

Criterion 29.5— FINTRAC is able to disseminate "designated information,"[152] either spontaneously or in response to a VIR, to the appropriate police force,[153] the CRA, CBSA, Communications Security Establishment, Provincial Securities Regulators (as of 23 June 2015) and CSIS, through secure and protected channels (ss.55(3)(a) to (g) and 55.1(1)(a) to (d) PCMLTA). It is also able to disseminate information upon request to LEAs with a court order issued in the course of court proceedings in respect of an ML, TF, or another offense (PCMLTFA, s.59(1). This process has not been used in recent years, as LEAs obtain sufficient information from FINTRAC in response to their VIRs. FINTRAC's AML/CFT supervisory unit and FIU unit are able to exchange information in the exercise of their respective functions. As indicated under R.30, some competent authorities, such as Environment Canada or Competition Bureau, cannot request information from the FIU.

Criterion 29.6— Information held by FINTRAC is securely protected and is disseminated in accordance with the PCMLTFA (s.40(c)). FINTRAC has internal procedures (FINTRAC's Privacy framework) governing the security and confidentiality of information, the respect of the confidentiality and security rules by its staff members and limiting access to information, including access to the IT system, to those who have a need to know in order to effectively perform their duties.

Criterion 29.7— FINTRAC was established as an independent agency that acts at arm's length and is independent from LEAs and other entities to which it is authorized to disclose information under ss.55(3), 55.1(1) or 56.1(1) or (2) (PCMLTFA, s.40(a)).

[151] Mass Marketing Fraud: Money Laundering Methods and Techniques (January 2015), Money laundering trends and typologies in the Canadian securities sector (April 2013), Money Laundering and Terrorist Financing Trends in FINTRAC Cases Disclosed Between 2007 and 2011 (April 2012), Trends in Canadian Suspicious Transaction Reporting (STR) (April and October 2011), Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (July 2010), Money Laundering Typologies and Trends in Canadian Casinos (November 2009), Money Laundering and Terrorist Financing Typologies and Trends in Canadian Banking (May 2009).
[152] The terms "designated information" cover a range of information, including the name and criminal records of a person or entity involved in the reported transaction, the amounts involved, etc.
[153] The appropriate police force means the police force that has jurisdiction in relation to the ML offense. This includes federal, provincial and municipal police forces, as they receive their power from the province.

a) The Director of FINTRAC is appointed by the Governor in Council for a reappointed term of no more than five year with a maximum term of ten years, and has supervision over and direction of the Centre regarding the fulfilment of its mission (internal organization, decisions taken, etc.) and in administrative matters (staff and budget).

b) FINTRAC is able to make arrangements or engage independently with other domestic competent authorities. Agreements or arrangements with foreign counterparts on the exchange of information are entered either into by the Minister or by the Centre with the approval of the Minister (PCMLTFA, s.56 (2)).

c) FINTRAC is not located within an existing structure of another authority: the FIU is an independent agency under the responsibility of the Minister with legally established and distinct core functions (PCMLTFA, ss.42 and 54).

d) The Minister is responsible for FINTRAC (PCMLTFA, s.42(1)) and the director of FINTRAC is the chief executive officer of the Centre, has supervision over and direction of its work and employees and may exercise any power and perform any duty or function of the Centre (PCMLTFA, s.45(1)).

Criterion 29.8— FINTRAC has been a member of the Egmont Group since 2002.

Weighting and Conclusion

FINTRAC has limited access to some information.

Canada is partially compliant with R.29.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 2008 MER, Canada was rated LC with former R.27 due to an effectiveness issue. Minor changes have since been made. There are also significant changes in the standard.

Criterion 30.1— LEAs are designated with the responsibility for investigating ML, predicate offenses and TF. There is one national police force (the RCMP) and two provincial LEAs (respectively, in Ontario and Quebec). The RCMP is a federal, provincial, and municipal policing body. All Canadian police forces are potential recipients of FINTRAC disclosures under the PCMLTFA and can investigate ML/TF offenses.

Most predicate offenses are investigated by provincial and municipal police forces, including the RCMP when they are acting as provincial police (except Ontario and Quebec). Serious or proceeds-generating crime investigations can be done by the RCMP either exclusively or in parallel with provincial or municipal forces.

The RCMP has the primary law enforcement responsibility to investigate both terrorism and TF. The Terrorist Financing Team of the RCMP's Federal Policing Criminal Operations (FPCO) is responsible for, inter alia, monitoring and coordinating major ongoing investigational projects related to

terrorist organizations on financial and procurement infrastructures.

Criterion 30.2— All national, provincial and municipal police forces are authorized, under the CC, as "peace officers" to conduct parallel financial investigations related to their criminal investigations. They may refer the ML/TF case to other police units for investigation, regardless of where the predicate offense occurred.

Criterion 30.3— All police forces are empowered to identify, trace, seize, and restrain property that is, or may subject to forfeiture, or is suspected of being proceeds of crime. They are empowered with a wide range of measures under the CC (see Criterion 4.2).

Criterion 30.4— Other agencies, including the CRA (Income Tax Act), Competition Bureau (Competition Act, ss.11-21) and Environment Canada (Environmental Protection Act 1999), have the authority to conduct financial investigations related to the predicate offenses that they respectively specialize in. In addition, law enforcement agencies in Canada have the authority under Common Law to investigate crime and criminal offenses such as ML. They may seek judicial authority to seize and freeze assets. For the CBSA, although it does not have the responsibility for pursuing financial investigations of predicate offenses included in the Immigration Refugee Protection Act (IRPA), the Customs Act and border related legislations, a referral mechanism is in place for RCMP to follow up on the financial investigations. PCMLTFA, s.18 authorizes the seizure and forfeiture of cash by CBSA. Section 36 of the same Act also authorizes the disclosure of the information to the RCMP for criminal investigations into ML or TF.

Criterion 30.5— All police forces are responsible for investigating corruption offenses (CC, ss.119-121 and Corruption of Foreign Public Officials Act, s.3). As mentioned in R.4 and above, they have the powers to identify, trace, and initiate the freezing and seizing of assets.

Weighting and Conclusion:

Canada is compliant with the R.30.

Recommendation 31 - Powers of law enforcement and investigative authorities

In its 2008 MER, Canada was rated C with former R.28. Minor changes have since been implemented in the Canadian legal framework as well as in the standard.

Criterion 31.1— *a)* CC, ss.487.014 (production order) and 487.018 (production order for financial and commercial information) empower a justice or judge to order a person other than a person under investigation to produce specified documents or data within the time to any peace or public officer. S.487.018 production order for financial data is also available to compel a particular person or entity to disclose the identity of the account holder of a given account number.

b) Search warrant under CC, s.487 is available for peace and public officers to search any prescribed places for available information.

c) Law enforcement officers are authorized to take statements from voluntary witnesses under the powers conferred by the Common Law and in accordance with the Charter of Rights and Freedoms and the Canada Evidence Act. However, a witness cannot be compelled to provide a statement to police in an investigation of ML or its associated predicate offenses. For TF investigations, witnesses are bound to provide a statement in an investigative hearing under Part II.1 of the CC (Terrorism).

d) Search warrants under CC, s.487 (search and seizure of evidence) and 462.32 (search and seizure of proceeds of crime) empower investigators to search and seize evidence. The General Warrant under CC, s.487.01 further authorizes the use of any device or means to collect evidence.

Criterion 31.2— *a)* RCMP can mount undercover operations to infiltrate crime syndicates and collect evidence for prosecution. Based on the principles in common law, the police are deemed to have common law powers where such powers are reasonably necessary in order for them to execute the mandate of investigating the commission of serious offenses, and undercover operations fall into this category.

b) Law enforcement can intercept communications pursuant to an Order made under CC, s.186 without the consent of the targeted person. It applies to organized crime offenses or an offense committed for the benefit of, at the direction of, or in association with a criminal organization; or a terrorism offense. It applies to both ML and TF offenses.

c) Computer systems can only be accessed with the consent of the owner or by a search warrant / General Warrant under the CC, but the courts[154] have found that particular considerations apply to computers and the stored content therein, which may require authorities to obtain specific prior judicial authorization to search computers found within a place for which a search warrant has been issued.

d) Similar to (a) above, Canadian Police are conferred with the power to conduct controlled delivery and is subject to stringent RCMP's internal policy.

Criterion 31.3— *a)* CC, s.487.018 (production order for financial and commercial information) empower a justice or judge to order a FI or DNFBP other than a lawyer to produce specified data within the time to any peace or public officer. The s. 487.018 production order for financial data is also available to compel a particular person or entity to disclose the identity of the account holder of a given account number. Search warrant under the provision of CC, s.487 is also available for peace and public officers to search any prescribed places for available information. However, the mechanism used to identify whether legal or natural persons hold or control accounts is not timely and deficient. In identifying whether a subject holds or controls accounts, law enforcement agencies will apply for a court order and serve it to the FI/DNFBP they reasonably suspect of holding such information and wait for the FI/DNFBP to respond. Each order can only be served to one specified FI/DNFBP. In urgent cases, the order can be drafted to obtain an initial response within days or otherwise it will take a longer time. The time required for such identification is considered not timely enough and the mechanism is not exhaustive to identify all accounts held with FIs/DNFBPs.

[154] (R. v. Vu, 2013 SCC 60 (CanLII))— www.canlii.org/en/ca/scc/doc/2013/2013scc60/2013scc60.html. .

LEAs may also use other informal processes, such as surveillance or FINTRAC disclosures, to identify the FIs/DNFBPs. These informal processes are sometimes lengthier and again not exhaustive to identify accounts held by the subject.

b) Warrants and production orders are normally obtained on an ex-parte basis. If the order is directed to a third party, a condition may be added specifically to prohibit the third party from revealing the fact of the warrant to the account holders. Assistance Order, under CC, s.487.02, can also be applied by the law enforcement agencies to seek assistance from a person and request that he/she refrain from disclosing the information to the suspect.

Criterion 31.4— Most law enforcement agencies can ask for information from FINTRAC by submitting VIRs. FINTRAC is able, under PCMLTA, ss.55(3)(a) to (q) and 55.1(1)(a), to disseminate "designated information" by responding to these VIRs. However, these provisions do not allow other competent authorities such as Environment Canada or Competition Bureau conducting investigations of ML and associated predicate offenses to ask for information held by the FINTRAC.

Weighting and Conclusion

LEAs generally have the powers that they need to investigate ML/TF but there are some shortcomings.

Canada is largely compliant with R.31

Recommendation 32 – Cash Couriers

In its 2008 MER, Canada was rated C for former SR IX (para 559–607).

Criterion 32.1— Canada has implemented a declaration system[155] for both incoming and outgoing physical cross-border transportation of currency and bearer negotiable instrument. A declaration is required for all physical cross-border transportation, whether by travellers or through mail, courier and rail or by any other means of transportation. The declaration obligation applies to both natural and legal persons acting on their own and behalf of a third party, and applies to the full range of currency and BNI, as defined in the Glossary to the FATF Recommendations.

Criterion 32.2— The reporting of currency and bearer-negotiable instrument of an amount of CAD 10 000 or more must be made in writing on the appropriate form and must be signed and submitted to a CBSA officer.[156] The reporting requirements of the PCMLTFA are met once the completed report is reviewed and accepted.

Criterion 32.3— This criterion is not applicable in the context of Canada, as it only applies to disclosure systems.

[155] Part 2 of the *PCMLTFA.*

[156] The PCMLTFA Sec. 12(3) outlines who must report; this applies to conveyances regardless of mode (air; marine; rail; land or postal).

Criterion 32.4— Upon discovery of a false declaration of currency or BNIs, or a failure to declare, CBSA officers have the authority to request and obtain further information from the carrier with regard to the origin of the money and its intended use, as to ask for the documents supporting the legitimacy of the source of funds (Customs Act s. 11).

Criterion 32.5— Under PCMLTFA, s.18, when persons make a false declaration or fail to make a declaration, CBSA officers have the power to seize as forfeit the currency or monetary instruments and to impose an administrative fine. The officer shall, on payment of a penalty in the prescribed amount (CAD 250, CAD 2 500, or CAD 5 000, depending of the circumstances, including the particular facts and circumstances of any previous seizure(s) the individual has had under the PCMLTFA), return the seized currency or monetary instruments to the individual from whom they were seized or to the lawful owner. If the officer has reasonable grounds to suspect that the currency or monetary instruments are proceeds of crime within the meaning of CC, s.462.3(1) or funds for use in TF activities, there are no terms of release and the funds are forfeited. Overall, the administrative sanctions could appear to be nor proportionate and nor dissuasive for undeclared or falsely declared cross-border transportation of cash over the threshold.

Criterion 32.6— CBSA forwards all Cross-border Reports submitted by importers or exporters as well as seizure reports to FINTRAC electronically. If the currency or monetary instruments have been seized under PCMLTFA, s.18, the report is sent without delay to FINTRAC, in order to undertake an analysis on seizure information.

Criterion 32.7— CBSA officers undertake customs as well as immigration matters. Under PCMLTFA s. 36, CBSA is allowed to communicate information to FINTRAC, to the appropriate police force and to the CRA. Reports and seizure reports are systematically sent to the FIU and reports are communicated to the RCMP. The RCMP has a formal MOU with CBSA and a Joint Border Strategy which stipulates the roles and responsibilities of each partner and how they will cooperate.

Criterion 32.8— When persons make a false declaration or fail to make a declaration, CBSA officers have the power to seize as forfeit the currency or bearer negotiable instrument. No terms of release are offered on funds that are suspected to be proceeds of crime within the meaning of CC, s.462.3(1) or TF (PCMLTFA, s.18(2)). When an individual fully complies with the requirement to report on currency above the threshold, but there are reasonable grounds to believe the funds are related to ML/TF or predicate offenses, the CBSA contacts the RCMP who may carry out a seizure under the CC. The CBSA is empowered to restrain currency or BNIs for a reasonable time in order to allow the RCMP to ascertain whether evidence of ML/TF may be found, but there is no clear process is in place to engage any authority in ascertaining these evidences following false declaration or undeclared cross-border transportation of cash, nor where there is a suspicion of ML/TF or predicate offenses.

Criterion 32.9— False declaration leading to seizures of currency and bearer negotiable instruments are entered and maintained into the Integrated Customs Enforcement System. These information are also sent by CBSA to FINTRAC, which incorporates them into its database. These

reports include information that must be provided in the mandatory reports.[157] Under PCMLTFA, ss.38 and 38.1, within an agreement or arrangement signed by the Minister, cross-border seizure reports where ML/TF is suspected are provided to foreign counterparts if the CBSA has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a ML or a TF offense, or within Custom Act s. 107 in accordance with an agreement. Declaration which exceeds the prescribed threshold are not retained by CBSA, but are forwarded to FINTRAC that should be in position to disclose CBCRs to its foreign counterparts, what may complicate international cooperation between customs regarding cash couriers.

Criterion 32.10— The information collected pursuant to the declaration obligation is subject to confidentiality.[158] There are no restrictions on the amount of money that can be imported into or exported from Canada; however, once the amount has reached or exceeded the threshold it must be reported.

Criterion 32.11— When there is reasonable grounds to believe the funds are related to ML/TF or predicate offenses, the CBSA contacts the RCMP who may carry out subsequent criminal investigation and laying of charges under the CC. If the suspicion is confirmed, seizure and confiscation measures may be decided by the judicial authority under the conditions described in R.4.

Weighting and Conclusion

There are some minor deficiencies.

Canada is largely compliant with R.32.

Recommendation 33 – Statistics

In its 2008 MER, Canada was assessed as LC with former R.32 because the absence of statistical information on ML investigations and sentencing, confiscation, response times for extradition and mutual legal assistance (MLA) requests, response times for requests to OSFI by its counterparts. Some changes were introduced in the standard as well as in Canada.

Criterion 33.1— The compilation of AML/CFT related statistics are coordinated by Finance Canada and provided by all regime partners including FINTRAC, the RCMP, the PPSC and Statistics Canada at the federal and provincial level. The authorities maintain a comprehensive set of statistics that appears suitable to assist in the evaluation of the effectiveness of its AML/CTF framework. As a consequence of the NRA process, the authorities have improved the usefulness of existing data sets and developed new ones. The authorities intend to maintain the AML/CFT related statistics with a focus on periodically measuring the effectiveness of the AML/CFT regime.

[157] Including amount and type of currency or BNI, identifying information on the person transporting, mailing or shipping the currency or monetary instruments, as well as information on the person or entity on behalf of which the importation or exportation is made.
[158] PCMLTFA, article 36 and followings.

Sub-criterion 33.1 a: FINTRAC keeps statistics of STRs received and disseminated. Statistics on STRs received by regions is also available. Regarding the statistics provided on the dissemination of information by FINTRAC, it is unclear whether these disclosures derive from STRs, as required by the FCFT standard statistics related to the FIU.

Sub-criterion 33.1 b: Canada maintains acceptable statistics regarding ML/TF investigations, prosecutions and convictions. Statistical data on ML, proceeds of crime and TF investigations and prosecutions is generated at the national, federal and provincial levels. It is generated from various sources, such as Statistics Canada's Uniform Crime Reporting Survey (UCR), the RCMP Occurrence Data (a records management system), the Public Prosecution Service's iCase, its case management and timekeeping system. The RCMP has employed its Business Intelligence program to provide statistical information on ML/TF investigations that is more detailed than UCR. This information is derived from the RCMP's various Operational Record Management Systems.

Sub-criterion 33.1 c: Canada maintains statistics on assets seized, forfeited and confiscated as proceeds of crime and offense-related property (the equivalent of "instruments" or "instrumentalities" in other countries). However, there is no legal requirement for the AG to keep statistics on seizures.

Sub-criterion 33.1 d: Statistics on made and received mutual legal assistance or other international requests for cooperation are maintained by the Department of Justice Canada. These statistics are used by Justice Canada to track the timeliness of response and the nature of underlying predicate crime.

Weighting and Conclusion

Canada is compliant with R.33.

Recommendation 34 – Guidance and feedback

In its 2008 MER, Canada was rated LC with these requirements due to the lack of specific guidelines intended for sectors such as life insurance companies and intermediaries, and insufficient general feedback given outside the large FIs sector. There has been a substantial increase in guidance and feedback by Canadian authorities since the last MER.

Criterion 34.1— Canada provides guidance to industry on AML/CFT principally through regulators. FINTRAC provides guidance to both FIs and DNFBPs that is accessible on its website. A range of guidance has been published in the form of guidelines, trends and typologies reports, frequently asked questions, interpretation notices, sector specific pamphlets, brochures and information sheets on general topics such as the examination process. Guidance information is tailored to the different reporting sectors and deals with reporting, record-keeping, customer due diligence, general compliance information and questionnaires. Issues such as suspicious transaction reporting, terrorist property reporting, record-keeping, client identification, and implementing compliance

regime to comply with AML/CFT obligations. Global Affairs Canada has issued guidance for countering proliferation (CP) sanctions regimes.

OSFI has a dedicated section of its website for AML/CFT and sanctions issues and it has issued prudential guidance that includes guidance on AML/CFT. A number of other guidelines issued by OSFI are either directly or indirectly applicable to AML/CFT requirements of the FRFI sector. In addition, OSFI's Instruction Guide Designated Persons Listings and Sanction Laws sets out OSFI's expectations for FRFIs when implementing searching and freezing CP and sanctions reporting obligations under the Criminal Code, UN Regulations and other sanctions laws. Other regulators such as IIROC have issued AML guidance to IIROC Dealer members in 2010. OSFI's guidance for FRFIs focuses on prudent risk management and internal controls to address the risk of ML and TF. It includes guidance on deterring and detecting ML and TF, background checks on directors and senior management, oversight of outsourced AML/CFT functions, corporate governance and screening of designated persons under the CC and UN Regulations. While FINTRAC is the main authority responsible for issuing AML/CFT guidance, other regulators also provide guidance on AML issues[159] and consult FINTRAC for policy interpretations.

Feedback is given by FINTRAC to industry through an outreach and assistance program for REs. This includes participating in conferences, seminars, presentations and other events providing feedback on compliance with AML/CFT legislation. REs can liaise with FINTRAC and OSFI by email or an enquiries telephone line. Each RE has a designated FINTRAC Compliance Officer to contact with any queries. FINTRAC's guidance and feedback to REs, in particular MSBs, is also reported as having increased significantly. The RCMP provides guidance through lectures to various businesses throughout Canada on recognizing and reporting suspicious transactions and has given conferences and seminars on identifying, reporting, and investigating ML and materials produced by it on AML related issues.

Since 2008, Canada has provided guidance to the life insurance sector that is very similar to what is provided to other sectors. The guidance on AML/CFT provided by OSFI is applicable to all FRFIs subject to the PCMLTFA including life insurance companies. The guidance provided by FINTRAC is relevant to FIs and DNFBPs and there is sector specific guidance for the financial sector including life insurance companies and brokers and MSBs.

Weighting and Conclusion

There is more specific guidance needed in certain sectors.

Canada is largely compliant with R.34.

[159] Quebec: AMF published a notice on AML/CFT requirements of their regulated entities; Nova Scotia Credit Union Deposit Insurance Corporation, Financial Institutions Commission of British Columbia, British Columbia Gaming Policy Enforcement Branch, Deposit Insurance Corporation Ontario, Prince Edward Island Credit Union Deposit Insurance Corporation have all published guidance on their websites.

Recommendation 35 – Sanctions

In its 2008 MER, Canada was rated PC because: administrative sanctions were not available to FINTRAC; OFI used a limited range of sanctions; and effective sanctions had not been used in cases of major deficiencies. Several changes occurred since then, e.g. FINTRAC was granted the power to apply AMPs for non-compliance with the PCMLTFA.

Criterion 35.1— Civil and criminal sanctions are available in addition to remedial actions. FINTRAC is responsible for imposing AMPs for non-compliance with the PCMLTFA and its regulations.

The PCMLTFA and related legislation provide for penalties for non-compliance with AML/CFT measures. Part V of the PCMLTFA sets out penalties for non-compliance with the Act. The United Nations Act provides that, when the United Nations Security Council passes a resolution imposing sanctions, such measures automatically become part of domestic law, and sets out penalties for non-compliance with its provisions.

The PCMLTFA covers a range of criminal offenses and a series of sanctions for contraventions of the provisions of the Act. Criminal penalties for non-compliance can lead up to CAD 2 million in fines and up to five years in prison. The criminal sanctions regime applies to most of the law and regulations provisions in the PCMLTFA. LEAs can conduct investigations and lay criminal charges in cases of non-compliance with the PCMLTFA.

The PCMLTF AMP Regulations govern the imposition of administrative sanctions for non-compliance with the PCMLTFA and related regulations. They provide for penalties, classifying violations as minor, serious or very serious. The maximum penalty for a violation by a person is set at CAD 100 000 and for a RE it is CAD 500 000. The imposition of a penalty is on a per violation basis: therefore, where there are multiple violations, an entity is potentially exposed to the maximum penalty for each individual violation. The maximum AMP thresholds for serious violations raises doubts whether it is proportionate or dissuasive (notwithstanding it relates to each instance of violation), given that there may be circumstances where a single egregious breach (or a few) may occur and the cumulative threshold might not be either a proportionate or dissuasive sanction. The threshold may also not be dissuasive in circumstances of repeat offending.

There are also other non-monetary methods used by FINTRAC, in addition to the AMP procedure, to apply corrective measures or sanction REs, including issuing deficiency letters, action plans for FRFIs, compliance meetings and enquiries, public naming, revocation of registration of MSBs and non-compliance case disclosures to LEAs.

OSFI has a range of powers as set out in OSFI Act, s.6. OSFI can apply written interventions, staging (more intense/frequent supervision), put in place compliance agreements and directions of compliance, place terms and conditions on a FRFI's business operations and direct independent auditors to extend the scope of their audit and guidance, which are enforceable. The staging process, involving more intensive supervision of an FRFI, does have a dissuasive affect, as it attracts an increase in the deposit insurance premiums paid by the FRFI concerned. OSFI can also remove

directors and/or officers from office, and/or take control of an FRFI in extreme cases of non-compliance with federal legislation, including the PCMLTFA. While OSFI does have the power to impose monetary penalties for non-compliance with general prudential provisions under an FRFI's governing legislation, violations of the PCMLTFA are dealt with by FINTRAC through the AMP procedure. OSFI has regulatory guidelines for AML compliance and background checks of directors and senior managers. OSFI cannot apply AMPs for non-compliance with the PCMLTFA.

Other regulators, such as securities regulators, can impose sanctions under securities legislation in circumstances where a market intermediary fails to meet legal requirements. The measures that can be taken include terminating the intermediary's license and imposing terms and conditions that restrict the intermediary's business. Sanctions can also be imposed on members for contraventions of self-regulatory organizations' requirements, including AML and supervision requirements.

Criterion 35.2— PCMLTFA, s.78 provides that sanctions are applicable to any officer, director, or agent of the person or entity that directed, assented to, acquiesced in, or participated in its commission.

Weighting and Conclusion

The dissuasiveness and/or proportionality of some of the sanctions is unclear.

Canada is largely compliant with R.35.

Recommendation 36 – International instruments

Canada was rated LC with former R.35 and SR I in the 2008 MER, because the ML offense did not cover all designated categories of predicate offenses and contained a purposive element that was not broad enough to meet the requirements of the Conventions, and because of inadequate measures to ascertain the identity of beneficial owners.

Criterion 36.1— Canada is party to the conventions listed in the standard.[160]

Criterion 36.2— Bill C-48 amended to the CC to meet the requirements of the Merida Convention, especially by providing for the forfeiture of property used in the commission of an act of corruption and to clarify that it may be direct or indirect, and that it is not necessary that the person who commits the corrupt act receive the benefit derived from the act. Canada also addressed the deficiencies identified in 2008 (see R. 3 and 10).

Weighting and Conclusion:

Canada is compliant with R.36.

[160] Canada ratified the Vienna Convention on 5 July 1990, the Palermo Convention on 13 May 2002, and the Merida Convention on 2 October 2007, the Convention on the Suppression of Terrorist Financing Convention on 19 February 2002, and the Inter-American Convention against Terrorism. It has also signed the Council of Europe Convention on Cybercrime (2001), on 23 November 2001.

Recommendation 37 - Mutual legal assistance

In its third MER, Canada was rated LC with former R.36 and SR. V due to concerns about Canada's ability to handle MLA requests in a timely and effective manner and about the lack of adequate data that would establish effective implementation. Canada's legal framework for MLA was supplemented by Canada's new Protecting Canadians from Online Crime Act (PCOCA, in force 9 March 2015). The requirements of the (new) R.37 are more detailed.

Criterion 37.1— Canada has a sound legal framework for international cooperation. The main instruments used are the Mutual Legal Assistance in Criminal Matters Act (MLACMA); the relevant international conventions, the Extradition Act; 57 bilateral treaties on MLA in criminal matters, extradition and asset sharing; and MOUs for the other forms of assistance to exchange financial intelligence, supervisory, law enforcement or other information with counterparts. These instruments allow the country to provide rapid and wide MLA. In the absence of a treaty, Canada is able to assist in simpler measures (interviewing witnesses or providing publicly available documents), or, based in the MLACMA, to enter in specific administrative arrangements, that would provide the framework for the assistance.

Criterion 37.2— Canada uses a central authority (the Minister of Justice, assisted by the International Assistance Group—IAG) for the transmission and execution of requests. There are clear processes for the prioritization and execution of mutual legal assistance requests, and a system called "iCase" is used to manage the cases and monitor progress on requests.

Criterion 37.3— MLA is not prohibited or made subject to unduly restrictive conditions. Canada provides MLA with or without a treaty, although MLA without a treaty is less comprehensive. Requests must meet generally the "reasonable grounds to believe standard, in relation for example to MLACMA ss 12 (search warrant) and 18 (production orders). However, certain warrants (financial information, CC, s.487.018, tracing communications, and new s.487.015) may be obtained on the lower standard of "reasonable ground to suspect."

Criterion 37.4— Canada does not impose a restriction on MLA on the grounds that the offense is also considered to involve fiscal matters, nor on the grounds of secrecy or confidentiality requirements on FIs or DNFBPs.

Criterion 37.5— MLACMA, s.22.02 (2) states that the competent authority must apply *ex parte* for a production order that was requested in behalf of a state of entity. In addition to that, the international Conventions signed, ratified and implemented by Canada include specific clauses requiring the confidentiality of MLA requests be maintained.

Criterion 37.6— Canada does not require dual criminality to execute MLA requests for non-coercive actions.

Criterion 37.7— Dual criminality is required for the enforcement of foreign orders for restraint, seizure and forfeiture or property situated in Canada. MLACMA, ss.9.3 (3) (a) and (b) and 9.4 (1) (3) (5) (a) (b) and (c) allow the Attorney General of Canada to file the order so that it can be entered as a

judgment that can be executed anywhere in Canada if the person has been charged with an offense within the jurisdiction of the requesting state, and the offense would be an indictable offense if it were committed in Canada. This applies regardless of the denomination and the category of offenses used.

Criterion 37.8— Most, but not all of the powers and investigative techniques that are at the Canadian LEAs' disposal are made available for use in response to requests for MLA. The relevant powers listed in core issue 37.1 are available to foreign authorities via an MLA request, including the compulsory taking of a witness statement (according to MLACMA, s.18). Search warrants are not possible to obtain via letters rogatory. However, the Minister may approve a request of a state or entity to have a search or a seizure, or to use any device of investigative technique (MLACMA, s.11). The competent authority who is provided with the documents of information shall apply *ex parte* for the warrant to a judge of the province in which the competent authority believes evidence may be found. Regarding the investigative techniques under core issue 37.2, undercover operations and controlled delivery are possible through direct assistance between LEAs from the foreign country and Canada. Production orders to trace specified communication, transmission data, tracking data and financial data are possible by approval of the Minister in response to a foreign request. The authorities will not grant interception of communications (either telephone, emails or messaging) solely on the basis of a foreign request (this special investigative technique is not provided for in the MLACMA and will not be provided for in bilateral agreements. According to MLACMA, s.8.1, requests made under an agreement may only relate to the measures provided for in the bilateral agreement). The only possibility to intercept communications is within a Canadian investigation in the case of organized crime, or a terrorism offense, which would require that the criminal conduct occurred, at least in part, in Canadian territory (including a conspiracy to commit an offense abroad). Foreign orders for restraint, seizure and confiscation can be directly enforced by the Attorney General before a superior court, as if it were a Canadian judicial order.

Weighting and Conclusion

The range of investigative measures available is insufficient.

Canada is largely compliant with R.37.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

Canada was rated LC with R.38 in the 2008 MER due to the limited evidence of effective confiscation assistance, the rare occurrence of sharing of assets and the fact that Canada executed requests to enforce corresponding value judgments as fines. The framework remains the same.

Criterion 38.1— Canada has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize or confiscate laundered property and proceeds from crime (MLACMA, ss.9.3, 9.4 and CC, ss.462.32, 462.33), and instrumentalities used in or intended for use in ML, predicate offenses or TF. There is, however, no legal basis for the confiscation of property of corresponding value. As was the case during its previous assessment, Canada still treats value-based

forfeiture judgement as fines, which has limitations and cannot be executed against the property. If the fine is not paid, it can be converted into a prison sentence. Regarding the identification of financial assets new CC, s.487.018 allows the production of financial registration data in response to requests from foreign states.

Criterion 38.2— In Canada, MLA is based on the federal power in relation to criminal law. Therefore, the enforcement of some foreign non-conviction based confiscation orders is not possible under the MLACMA because they were not issued by a "court of criminal jurisdiction." However, in cases where the accused has died or absconded before the end of the foreign criminal proceedings, the MLACMA applies because the matter would still be criminal in nature. Due to Canada's constitutional division of powers, the Government of Canada cannot respond to a request for civil forfeiture as such requests fall within the jurisdiction of Canada's provinces. However, most of the Canadian provinces have already adopted legislation on a civil confiscation regime. Even if Canada is not able to provide assistance to requests for cooperation based on NCB proceedings, non-conviction based confiscation is possible under Canadian law. Should a foreign state seek to recover assets from Canada though NCB asset forfeiture, it must hire private counsel to act on its behalf in the province where the property or asset is located.

Criterion 38.3— *a)* No particular legal basis is required in Canada for the coordination of seizure and confiscation actions. It is a matter primarily for national and foreign police authorities at the stage of seizure. Thus, via direct police-to-police contact, arrangements are made in relation to any relevant case.

b) The Seized Property Management Act sets out the mechanisms for the management and, when necessary, the disposition of property restrained, seized and forfeited. The Minister of Public Works and Government Services is responsible for the custody and management of all property seized at the federal level. The Minister may make an interlocutory sale of the property that is perishable or rapidly depreciating, or destroy property that has little or no value. Property seized in the provincial level is managed by the provincial prosecution services.

Criterion 38.4— Canada shares confiscated property on a mutual agreement basis, under the Seized Property Management Act, s.11. Canada has 19 bilateral treaties regarding the sharing and transfer of forfeited or confiscated assets and equivalent funds.

Weighting and Conclusion

The seizure and confiscation regime has a deficiency, which is the impossibility of confiscation of equivalent value.

Canada is largely compliant with R.38.

Recommendation 39 – Extradition

Canada was rated LC with R.39 in the 2008 MER, mostly because of the difficulties in establishing the delay element, due to insufficient statistical data. The legal framework remains unchanged.

Criterion 39.1— Canada is able to execute extradition requests in relation to ML/TF without undue delay. Statistics provided to this assessment have shown that at least 40% of the requests are executed on a timely basis, what shows that the existing legal framework allows for extraditions without delay.

a) Both ML and TF are extraditable offenses (Extradition Act, ss.3(1) (a) and (b) of the combined with CC, ss.83.02, 83.03, 83.04 and 462.31).

b) Canada has a case management system (iCase) and clear processes in place for timely execution of extradition including prioritization of urgent cases. The Extradition Act sets out timelines for specific steps to ensure minimal delays, and requires judges to set an early date for the extradition hearing when the person has been provisionally arrested (s.21(1)(b)(3).

c) Canada does not place unreasonable or unduly conditions on the execution of extradition requests.

Criterion 39.2— Nationality does not constitute grounds for refusal to extradite under the Extradition Act, ss.44, 46, and 47 of the, but the Charter of Fundamental Rights and Freedoms gives Canadian citizens the right to remain in Canada. The Supreme Court decided in *U.S. v. Cotroni* that extradition is a reasonable limitation of the right to remain in Canada, and the decision whether to prosecute or not in Canada and allow the authorities in another country to seek extradition is made following consultations between the appropriate authorities in the two countries when various factors, including nationality, are considered in weighing the interests of the two countries in the prosecution. Historically, the result of most of these assessments has been to favour extradition, but when it is not, the Canadian citizen can be prosecuted in Canada.

Criterion 39.3— Dual criminality is required for extradition. It is not relevant whether the extraditable conduct is named, defined or characterized by the extradition partner in the same way as it is in Canada (Extradition Act, s.3(2)).

Criterion 39.4— Direct transmission of an extradition request to Canada's IAG or via Interpol is possible unless a treaty provides otherwise. Requests for provisional arrest may be made via Interpol by virtually all of Canada's extradition partners. The extradition process is simplified when the person consents to commit and surrender. Canada does not grant extradition based solely on a foreign warrant for arrest, such as in an Interpol Red Notice, or a foreign judgment, or in the absence of a treaty, based on reciprocity. There must be an assessment of the evidence, which takes place in the course of the judicial phase, which is followed by the Ministerial phase of the extradition proceedings.

Weighting and Conclusion:

Canada is compliant with R.39.

Recommendation 40 – Other forms of international cooperation

In the 2008 MER, Canada was rated LC with these requirements (para. 1551–1612). The main deficiency raised was related to FINTRAC as a supervisory authority.[161]

General Principles

Criterion 40.1— Canada's competent authorities can broadly provide international cooperation spontaneously or upon request related to ML/TF[162]. Referring to FINTRAC as FIU, PCMLTFA allows the Centre to disclose information to a foreign FIU spontaneously and makes reference to a disclosure of designated information "*in response to a request*."

Criterion 40.2— *a)* Competent authorities have the legal basis to provide international cooperation (see criterion 40.1).

b) Nothing prevents competent authorities from using the most efficient means to cooperate.

c) FINTRAC as a FIU and as a supervisor, OSFI, CBSA, and RCMP use clear and secure gateways, mechanism or channels for the transmission and execution of requests.

d) FINTRAC as an FIU has put in place processes for prioritizing and executing requests and answers in five business days if the Centre has transaction information in its database and FINTRAC as a supervisory authority processes the request and provides a response in a matter of days. In regard to TF, RCMP prioritize, assign and respond to such requests in the most efficient and effective manner on a National Level. It has not been established that LEA and supervisor authorities have clear procedures for the prioritization and timely execution of bilateral requests.

e) Competent authorities have clear processes for safeguarding the information received. FINTRAC policies and procedures for the safeguard of information apply to both the FIU and the supervisory side of FINTRAC. All supervisory information received by OSFI is subject to the same standard of confidentiality as domestic information (OSFI Act, s.22). RCMP has policies for handling requests and sharing or exchanging criminal intelligence and information with foreign partners and agencies (RCMP Operational manual Chapter 44.1s).

Criterion 40.3— Under the Privacy Act, competent authorities need bilateral or multilateral arrangements to cooperate with foreign counterparts where a disclosure of personal information about an individual is involved. FINTRAC as a FIU, RCMP and CBSA have signed a comprehensive network of MOUs and letters of agreement with foreign counterparts, but FINTRAC as a supervisory authority has entered into two MOUs so far. The Canadian authorities indicated that these bilateral agreements were signed mostly in a timely way. Examples of MOUs signed promptly have been

[161] *FINTRAC* as a supervisory authority had the legal capacity to exchange information with foreign counterparts but had not put the arrangements and agreements in place.
[162] FINTRAC as a FIU: *PCMLTFA*, section56; FINTRAC as a supervisory authority: *PCMLTFA*, section.65.1; RCMP: *Privacy Act and Memoranda of understanding or Letters of agreements*; CBSA: *PCMLTFA*, art.38 and 38.1 and *Custom Act*; OSFI: OSFI Act, section 22.

provided to the assessors. The OSFI Act does not require that the Superintendent enter into a MOU with a foreign counterpart in order to be able to cooperate.

Criterion 40.4— FINTRAC provides feedback upon requests to its foreign counterparts on the use and usefulness of the information obtained (PCMLTFA, ss.56.2 and 65.1(3)). Canadian authorities indicated that FINTRAC generally provides feedback to its foreign counterparts on the usefulness of the information obtained within five to seven days. There is no restriction on OSFI's ability to provide feedback. There is no general impediments, which prevents Canada's LEAs from providing feedback regarding assistance received.

Criterion 40.5— Competent authorities do not prohibit or place unreasonable or unduly restrictive conditions on information exchange or assistance on any of the four grounds listed in this criterion.

Criterion 40.6— Competent authorities have controls and safeguards to ensure that information exchanged is used for the intended purpose for, and by the authorities, for whom the information was provided.[163]

Criterion 40.7— Competent authorities are required to maintain appropriate confidentiality for any request for cooperation and the information exchanged, consistent with data protection obligations

Criterion 40.8— FINTRAC as an FIU, may conduct inquiries on behalf of foreign counterparts, by accessing its databases (all report types, federal and provincial databases maintained for purposes related to law enforcement information or national security, and publicly available information), under PCMLTFA, s.56.1(2.1). FINTRAC as a supervisory authority can conduct inquiries on behalf of foreign counterparts with which it has an MOU under PCMLTFA, ss.65.1(1)(a) and 65.1(2), but only two MOUs have been signed so far. The RCMP can use a number of criminal intelligence and police databases to conduct inquiries on behalf of foreign counterparts, under sharing protocols that aim at protecting the right to privacy of the individuals mentioned in the databases.

Exchange of Information Between FIUs

Criterion 40.9— FINTRAC exchanges information with foreign FIUs in accordance with the Egmont Group principles or under the terms of the relevant MOU, regardless of the type of its counterpart FIU. The legal basis for providing cooperation is in PCMLTFA, s.56(1), which stipulates that the Centre exchanges information if it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a ML or TF offense, or an offense that is "*substantially similar to either offense.*"

Criterion 40.10— FINTRAC provides feedback on the usefulness of information obtained, when feedback is specifically requested by foreign FIUs (PCMLTFA, s.56), and whenever possible as well as on the outcome of the analysis conducted, based on the information provided.

[163] *Privacy Act*—FINTRAC as a FIU: PCMLTFA, para 56 (3) and MOUs template; FINTRAC as a supervisory authority: PCMLTFA, s.65.1 (1) (b) and MOUs template; RCMP: Operational manual on information sharing; OSFI: OSFI Act, s.22.

Criterion 40.11— FINTRAC have the power to exchange:

a) The information held in its database (c. 40.8), which does not cover the scope of the information required to be accessible or obtainable directly or indirectly under R.29, as it does not include additional information from REs.

b) The information FINTRAC has the power to obtain or access directly or indirectly at the domestic level (c. 40.8), subject to the principle of reciprocity.

Exchange of Information Between Financial Supervisors

Criterion 40.12— PCMLTFA, allows FINTRAC to enter into information sharing arrangements or agreements under new s.65(2) with any agency in a foreign state that has responsibility for verifying AML/CFT. OSFI has broad authority to share supervisory information with domestic and foreign regulators or supervisors of FIs, including SROs.

Criterion 40.13— FINTRAC, as the AML/CTF supervisor for entities covered by the PCMLTFA, has the authority to share with foreign supervisors compliance-related information that FINTRAC has in its direct possession about the compliance of persons and entities. The information that FINTRAC may exchange with foreign supervisors is defined by "FINTRAC supervisory MOU Template." Canadian authorities indicated that FINTRAC can exchange information domestically available, including information held by FIs. As regards OSFI, under the OSFI Act a broad exemption is provided under s.22(2) in favour of the exchange of supervisory information with any government agency or body that regulates or supervises FIs.

Criterion 40.14— *a)* FINTRAC and OSFI do not require legislation to exchange regulatory information, and that they currently exchange such information. Examples were given by FINTRAC of cross-border cooperation with other regulators.

b) OSFI, under OSFI Act, s.22 can exchange supervisory information with foreign government agency or body that regulates or supervises FIs which meets this Criterion.

c) PCMLTFA, subsection 65.1 enables FINTRAC to exchange supervisory information with other supervisors about the compliance of persons and entities, record-keeping and reports. Through its supervisory examinations and compliance assessment reports, FINTRAC normally obtains information on REs' internal AML/CFT procedures and policies, CDD, customer files and sample accounts and transaction information. FINTRAC is able to exchange this information with other supervisors. However, this possibility is limited to exchanges with counterparts who are MOU partners.

Criterion 40.15— FINTRAC can conduct inquiries on behalf of foreign counterparts with which it has an MOU under PCMLTFA, ss.65.1(1)(a) and 65.1(2).

Criterion 40.16— FINTRAC can enter into agreements or arrangement with other supervisors to exchange information pursuant to the PCMLTF.[164] Under such agreements or arrangements, there is an obligation to keep such information confidential and not further disclose the information. FINTRAC's tactical MOU sets out the requirements for use and release and confidentiality of information exchanged between financial supervisors. It is provided in the tactical MOU that information that has been exchanged will not be disclosed without the express consent of the requested authority. It is also provided that if an authority has a legal obligation to disclose information, it will notify and seek the consent of the other authority. OSFI can exchange information with other supervisors on the basis that such information satisfies the requirements of the Act and will be kept confidential.

Exchange of Information Between Law Enforcement Authorities (LEAs)

Criterion 40.17— Under article 44.1 of the RCMP Operational Manual on "Sharing of information with Foreign Law Enforcement," RCMP and other Canadian LEAs are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to ML, associated predicate offenses or TF, including the identification and the tracing of proceeds and instrumentalities of crime. Nevertheless, CBSA does not retain CBCRs, which have to be obtained through international cooperation between FIUs, what could complicate their access by CBSA's foreign counterparts. PS works with other countries on national security, border strategies and countering crime, including ML and TF. PS also participates in a number of fora and initiatives to foster its international cooperation, including violent extremism and foreign fighters.

Criterion 40.18— Canadian LEAs can use the legislative powers available under the CC[165] and other Acts[166] including investigative techniques available in accordance with domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. However, it appears than the range of powers and investigative techniques that can be used by LEA to conduct enquiries and obtain information on behalf of foreign counterparts are very limited.[167] Both the PPOC and ML offense definitions allow that the offense need not to have occurred in Canada "so long as the act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence." Canada extensively cooperates with foreign law enforcement counterparts based on multilateral agreements in the context of Interpol and on bilateral MOUs.

Criterion 40.19— Canadian LEAs are able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangement to enable such joint investigations on the basis of RCMP Act (and the RCMP Operational policy Chapter 15 provides guidance on joint forces operation). Joint Forces Operations (JFO) involve one or more

[164] PCMLTFA, s.40 (c). PCMLTFA, s.65.1 (1) (b) also provides a limit on how the information can be used by both parties to a supervisory MOU. MOU Supervisory Template, Section 6 on Permitted Uses and Release of Exchanged Information, and Section 7 on Confidentiality are also relevant.
[165] CC, s.462.31 allows police to perform reverse sting operations to obtain information on ML cases and CC, s.462.32 to seize POC.
[166] Mutual Legal Assistance in Criminal Matters Act, RCMP Act and Canada Evidence Act.
[167] The only provisions which can be used allows police to perform reverse sting operations to obtain information on ML cases and to seize POC (CC, ss.462.31 and 462.32).

police/enforcement agencies working with the RCMP on a continuing basis over a definite period. A JFO should be considered in major multi-jurisdictional cases that are in support of national priorities and must be consistent with the mandated responsibility of the particular resource.

Exchange of Information Between Non-Counterparts

Criterion 40.20— Under PCMLTFA, FINTRAC as a FIU and a supervisor may enter into an agreement or arrangement, in writing, with an institution or agency of a foreign state that "*has powers and duties, similar to those of the Centre,*" which seems to exclude diagonal cooperation. Nevertheless, Canadian authorities indicate than when FINTRAC receives a request from a non-counterpart, the Centre address it either through its domestic partners or through the foreign FIU or supervisor. RCMP operational manual 44.1 outlines that sharing information will be managed on a case-by-case basis and there is no element that prevents RCMP to exchange information indirectly. OSFI has a broad ability to share information diagonally based on the wording of the OSFI Act, s.22. The "any government agency that regulates or supervises FIs" wording does not seem to limit disclosure to prudential regulators. However, OSFI would have to determine on a case-by-case basis whether such agency "regulates or supervises FIs." OSFI has shared information with foreign FIUs where they are also AML/CFT supervisors.

Weighting and Conclusion

There is room for improvement in regard to non-MLA international cooperation.

Canada is largely compliant with R.40.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• Lawyers, legal firms and Quebec notaries are not legally required to take enhanced measures to manage and mitigate risks identified in the NRA.
2. National cooperation and coordination	C	• The Recommendation is fully met.
3. Money laundering offence	C	• The Recommendation is fully met.
4. Confiscation and provisional measures	LC	• The legal provisions do not allow for the confiscation of property equivalent in value to POC.
5. Terrorist financing offence	LC	• CC, s. 83.03 does not criminalize the collection or provision of funds with the intention to finance an individual terrorist or terrorist organization.
6. Targeted financial sanctions related to terrorism & TF	LC	• Persons in Canada are not prohibited from providing financial services to entities owned or controlled by a designated person or persons acting on behalf or at the discretion of a designated person. • No authority has been designated for monitoring compliance by FIs and DNFBPs with the provisions of the UNAQTR, CC and RIUNRST.
7. Targeted financial sanctions related to proliferation	LC	• No mechanisms for monitoring and ensuring compliance by FIs and DNFBPs with the provisions of the RIUNRI and RIUNRDPRK. • Little information provided to the public on the procedures applied by the Minister to submit delisting requests to the UN on behalf of a designated person or entity.
8. Non-profit organisations	C	• The Recommendation is fully met .
9. Financial institution secrecy laws	C	• The Recommendation is fully met.
10. Customer due diligence	LC	• Exclusion of financial leasing, factoring and finance companies from scope of AML/CTF regime. • Minor deficiency of existence of numbered accounts whose use is governed only by regulatory guidance. • Minor deficiency of limited application, to natural persons only, of requirements to reconfirm identity where doubts arise about the information collected. • No explicit legal requirements to check source of funds. • No requirement to identify the beneficiary of a life insurance payout. • Minor deficiency of exceptions to the timing requirements for verifying identity are not clearly justified in terms of what is reasonably practicable or necessary to facilitate the normal

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		conduct of business. • Minor deficiency of the lack of a requirement to obtain the address and principal place of business of non-corporate legal persons and legal arrangements such as trusts.
11. Record keeping	LC	• The legal obligation requiring REs to provide records to FINTRAC within 30 days does not constitute "swiftly", as the standard specifies.
12. Politically exposed persons	NC	• Only one element of the FATF standard is currently largely met, although new legislation covering domestic PEPs will come into force in July 2016.
13. Correspondent banking	LC	• No requirement for a FI to assess the quality of AML/CFT supervision to which its respondent institutions are subject.
14. Money or value transfer services	C	• The Recommendation is fully met.
15. New technologies	NC	• No explicit legal or regulatory obligation to risk assess new products, technologies and business practices, before or after their launch.
16. Wire transfers	PC	• No specific requirements for intermediary and beneficiary FIs to identify cross-border EFTs that contain inadequate originator information, and take appropriate follow-up action. These are significant deficiencies.
17. Reliance on third parties	PC	• No explicit requirements on life insurance entities and securities dealers in relation to either necessary CDD information to be provided by the relied-upon entity or supervision of that entity's compliance with CDD and record-keeping obligations. • No requirements on life insurance entities or securities dealers to assess which countries are high risk for third party reliance.
18. Internal controls and foreign branches and subsidiaries	LC	• No specific legal requirements in relation to screening procedures when hiring employees.
19. Higher-risk countries	C	• The Recommendation is fully met.
20. Reporting of suspicious transaction	PC	• Minor deficiency that financial leasing, finance and factoring companies are not required to report suspicious activity to FINTRAC. • Lack of a prompt timeframe for making reports.
21. Tipping off and confidentiality	LC	• The tipping off and confidentiality requirements do not explicitly extend to the reporting of suspicions related to ML predicate offenses.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
22. DNFBPs: Customer due diligence	NC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • On line gambling, TCSPs that are not trust companies are not obliged entities. • No requirement on beneficial owner, PEP, new technologies, reliance on third parties. With the exception of a limited set of transactions the fixed threshold (CAD 10,000) of cash financial transactions and casinos disbursement exceeds that provided in the Recommendation. • The circumstances in which accountants and BC notaries are required to perform CDD are not in line with the FATF requirement.
23. DNFBPs: Other measures	NC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • TSCPs that are not trust and loan companies and on line gambling are not subject to the AML/CFT obligations; the circumstances under which accountants and BC notaries are required to comply with STRs are too limitative. • Further deficiencies identified under R.20 for DNFBPs that are subject to the requirements.
24. Transparency and beneficial ownership of legal persons	PC	• No appropriate mechanism to ensure that updated and accurate beneficial ownership information is collected for all legal entities in Canada, whether established under provincial or federal legislation. • Timely access by competent authorities to all beneficial ownership information is not warranted, in particular in cases where such information is held by a smaller or provincial FI, or a DNFBP. • Insufficient risk mitigating measures in place to address the ML/TF risk posed by bearer shares and nominee shareholder arrangements. • No obligation for legal entities to notify the registry of the location at which company records are held. • In some provinces, there is no legal obligation to update registered information within a designated timeframe. • No legal obligation on legal entities to authorize one or more natural person resident in Canada to provide to competent authorities all basic information and available beneficial ownership information; or to authorize a DNFBP in Canada to provide such information to the authorities.
25. Transparency and beneficial ownership of legal arrangements	NC	• No obligation for trustees to obtain and hold adequate, accurate and current beneficial ownership information for all legal arrangements in Canada, whether established under provincial or federal legislation, or basic information on other regulated agents or and service providers to the trust. • Professional trustees, including lawyers, are not required to maintain beneficial ownership information for at least five

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		years. • Insufficient mechanism in place to facilitate timely access by competent authorities to all beneficial ownership information and any trust assets held or managed by the FI or DNFBP. • No requirement for trustees to proactively disclose their status to FIs and DNFBPs when forming a business relationship or carrying out a financial transaction for the trust. • Proportionate and dissuasive sanctions for a failure by the trustee to perform his duties are not available in most cases.
26. Regulation and supervision of financial institutions	LC	• There are further fitness and probity controls needed for persons owning or controlling financial entities after market entry at provincial level.
27. Powers of supervisors	C	• The Recommendation is fully met.
28. Regulation and supervision of DNFBPs	PC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • Online gambling, cruise ship casinos, TSCPs not included among trust and loan companies are not subject to AML/CFT obligations and thus not monitored for AML/CFT purposes. • The entry standards and fit and proper requirements are absent in DPMS and TCSPs than trust companies, and they are not in line with the standards for real estate brokerage.
29. Financial intelligence units	PC	• FINTRAC is not empowered to request further information to REs. • FINTRAC has a limited or incomplete access to some administrative information (e.g. fiscal information), • FINTRAC is not able to disseminate upon request information to some authorities (e.g. Environment Canada, Competition Bureau)
30. Responsibilities of law enforcement and investigative authorities	C	• The Recommendation is fully met.
31. Powers of law enforcement and investigative authorities	LC	• No mechanism in place to timely identify whether a natural or legal person holds / controls accounts • No power to compel a witness to give statement in ML investigation • Only LEAs can ask for designated information from FINTRAC
32. Cash couriers	LC	• Administrative sanctions are not proportionate, nor dissuasive. • It has not been established that a clear process was in place to analyse or investigate cross-border seizures. • Cross-border currency reports are not retained by CBSA and can only be exchanged with foreign Customs authorities through FIUs' international cooperation.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
33. Statistics	C	• The Recommendation is fully met.
34. Guidance and feedback	LC	• There is more specific guidance needed in certain sectors such as DNFBPs to ensure that they are aware of their AML/CFT obligations, the risks of ML/TF and ways to mitigate those risks. There is also further feedback required arising out of the submitting of STRs.
35. Sanctions	LC	• The maximum threshold of administrative sanctions raises doubts about the dissuasiveness of sanctions for serious violations or repeat offenders.
36. International instruments	C	• This Recommendation is fully met.
37. Mutual legal assistance	LC	• The MLACMA does not allow for the interception of communications (either telephone or messaging) based solely on a foreign request, what hampers foreign investigations.
38. Mutual legal assistance: freezing and confiscation	LC	• Canada cannot respond to requests for the seizure and confiscation of property of corresponding value.
39. Extradition	C	• The Recommendation is fully met.
40. Other forms of international cooperation	LC	• The impediments raised in R.29 for FINTRAC, notably the fact that the FIU is not empowered to request further information from REs and the fact that some RE are not requested to fulfil STRs, impacts negatively the international cooperation with its counterparts. • LEAs are not able to use a large range of powers and investigative techniques to conduct inquiries and obtain information on behalf of foreign counterparts.

TABLE OF ACRONYMS

AMF	*Autorité des Marchés Financiers*
AML/CFT	Anti-money laundering and combating the financing of terrorism
APG	Asia/Pacific Group on Money Laundering
BC	British Columbia
CBCR	Cross-border currency report
CBSA	Canada Border Services Agency
CDR	Casino Disbursement Report
CDSA	Controlled Drugs and Substances Act
CRA	Canada Revenue Agency
CRA-CID	Canada Revenue Agency—Criminal Investigations Directorate
CSIS	Canadian Security Intelligence Service
DAR	Detailed Assessment Report
DOJ	Department of Justice
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea
DNFBP	Designated Non-Financial Businesses and Professions
D-SIB	Domestic Systematically Important Bank
EFTR	Electronic Funds Transfer Report
FATF	Financial Action Task Force
FI	Financial institution
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial intelligence unit
FRFI	Federally Regulated Financial Institution
GAC	Global Affairs Canada
IAG	International Assistance Group
ICC	Interdepartmental Coordinating Committee on Listings
IMF	International Monetary Fund
IO	Immediate Outcome
IPOC	Integrated Proceeds of Crime Initiative

ISEDC	Innovation, Science and Economic Development Canada (former Industry Canada)
LCTR	Large Cash Transaction Report
LEA	Law Enforcement Agency
MER	Mutual Evaluation Report
MSB	Money service business
ML	Money laundering
MLA	Mutual legal assistance
NPO	Non-profit organisation
NRA	National risk assessment
OCG	Organised criminal group
OPC	Office of the Privacy Commissioner
OSFI	Office of the Superintendent of Financial Institutions
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
PCMLTFR	Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
PEFP	Politically exposed foreign persons
PEP	Politically exposed person
PF	Proliferation financing
PIPEDA	Personal Information Protection and Electronic Documents Act
POC	Proceeds of crime
PPSC	Public Prosecution Service of Canada
PS	Public Safety Canada (former Public Safety and Emergency Preparedness)
PSPC	Public Services and Procurement Canada (former Public Works and Government Services Canada)
RBA	Risk-based approach
RCMP	Royal Canadian Mounted Police
RE	Reporting entity
RIUNRST	Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism
STR	Suspicious transaction report
TCSP	Trust and company service provider
TF	Terrorist financing
TFS	Targeted financial sanction

UNSCR	United Nations Security Council Resolution
UNAQTR	United Nations Al-Qaida and Taliban Regulation
US	United States of America
VIR	Voluntary Information Record

www.fatf-gafi.org | www.apgml.org

September 2016

Anti-money laundering and counter-terrorist financing measures - Canada
Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Canada as at the time of the on-site visit on 3-20 November 2015. The report analyses the level of effectiveness of Canada's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.

Appendix O:

APG & FATF, *FATF Report: Vulnerabilities of Casinos and Gaming Sector* (Paris: FATF, 2009)

The Asia/Pacific Group on Money Laundering

Financial Action Task Force Groupe d'action financière

FATF Report

Vulnerabilities of Casinos and Gaming Sector

March 2009

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

ASIA PACIFIC GROUP ON MONEY LAUNDERING

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organisation founded in 1997 in Bangkok, Thailand consisting of 39 member jurisdictions and a number of international and regional observers. The member jurisdictions and observers of the APG are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations and Nine Special Recommendations on Terrorist Financing of the Financial Action Task Force (FATF).

For more information about the APG, please visit the website:

WWW.APGML.ORG

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The vulnerability of casinos was recognised in the revision of the FATF 40 Recommendations, with obligations on casinos being significantly enhanced. However, there remained a lack of recent regional or global typologies on casinos and gaming, which this report seeks to address.

This APG/FATF report considers casinos with a physical presence and discusses related money laundering (ML) and terrorist financing (TF) methods, vulnerabilities, indicators to aid detection and deterrence, international information exchange. The report considers vulnerabilities from gaps in domestic implementation of anti-money laundering / combating the financing of terrorism (AML/CFT) measures. Data in the report was derived from members of the FATF, APG, other FSRBs and open sources.

Online gaming and illegal gambling are beyond the scope of this study.

Overall, there is significant global casino activity that is cash intensive, competitive in its growth and vulnerable to criminal exploitation. This paper identifies significant gaps in awareness of ML typologies, gaps in regulatory and law enforcement responses, gaps in online gaming typologies, issues with controls over junkets / VIP programs, and significant issues with controls over 'high seas' gaming. The report identifies significant gaps in global coverage of AML/CFT controls over the sector, which represents a significant vulnerability. The report is a resource for policy formation.

The report identifies significant ML vulnerabilities and related case studies and typologies, but does not identify any instances of TF through the sector.

Chapter 1, *The Casino Sector*, presents a global overview of casinos organised by regions (some 100 countries). The overview sets out the numbers, locations and, in some cases, ownership of each sector and coverage of AML/CFT controls. The chapter discusses some statistics and estimates of revenues (over USD70 billion globally) and profits (where known). The chapter discusses emerging casino markets, including a number of developing countries with governance and capacity challenges.

Chapter 1 briefly discusses casino sector risk assessments as a basis for allocating regulatory and law enforcement resources. The report highlights the need to identify ML risks for both those jurisdictions with or without a casino sector.

Chapter 2, *Money laundering Methodologies and Indicators*, considers vulnerabilities such as casino chips, casino cheques, casino accounts and facilities, structuring through the casino, currency exchange, employee complicity, etc. The paper describes typologies, case studies, and includes a summary of practical indicators for the industry, regulators and law enforcement.

Casinos undertake high volume/speed financial activities that are similar to financial institutions, but in an entertainment context. Casinos are generally large cash-based businesses. Foreign exchange facilities and reduced transparency of 'high rollers' in VIP rooms present substantial challenges. The use of foreign holding accounts where funds in one jurisdiction are available for use in a casino in another jurisdiction without the need for a cross border remittance presents further issues.

Chapter 3, *Sector Vulnerabilities and emerging Issues*, explores a number of additional

vulnerabilities and emerging issues. Casino-based tourism or "junkets" are identified as a vulnerability as they involve the cross border movement of people and funds and often target high net-worth / VIP clients. Transparency of the movement of funds is an issue with junkets, due to gaps in controls, and weak implementation and supervision.

The emerging issue of high-seas cruise ship casinos and associated junkets is a challenge for regulators and law enforcement. The question of who has jurisdiction is prominent, including where the vessel is registered, where it operates from and where it visits. The paper notes that few jurisdictions regulate this sector.

With respect to VIP rooms and 'high roller' customers, vulnerabilities are noted with identifying source of funds and movement of funds. In many casino markets high-roller clients make up a large majority of casino turnover, yet only a very small percentage of casino patrons.

Other vulnerabilities discussed include corrupt or inadequately trained staff, new markets opening and terrorist financing.

Chapter 4, *Policy Implications*, reiterates various key findings of the report and discusses a number of policy implications, including:

- Online gaming requires further typologies study and sharing of cases and regulatory models is needed;
- A significant number of jurisdictions do not subject their casino sector to AML/CFT controls;
- When casinos are subject to AML/CFT controls, many jurisdictions lack effective implementation of preventative measures (CDD, STRs, internal controls);
- There is a lack of regulatory tools that carry effective, proportionate and dissuasive sanctions;
- AML/CFT controls over casino foreign branches, offices or subsidiaries are not well regulated and there is a need for international guidance and best practice;
- Casino foreign holding accounts are not clearly covered for AML/CFT, which allows movement of funds without sending a cross-border wire transfer;
- Controls over VIP rooms vary and some jurisdictions lack clear powers regarding collecting and sharing information of VIP program participants;
- High-seas gaming is a large market over which there is little regulatory control;
- Many jurisdictions' casino regulators lack AML/CFT capacity and experience;
- International cooperation between casino regulators on AML issues is lacking and it is not always clear who are the competent authorities for information sharing.

INTRODUCTION

1. The APG and FATF have undertaken a joint study of vulnerabilities in the gaming and casinos sector. The project is led by New Zealand, with Ms Rachael Horton of New Zealand Department of Internal Affairs leading the work, including the drafting of this report. The work arose due to FATF and APG mutual evaluations and earlier typologies work, which noted a range of ML/FT risk factors related to gaming and casinos.

2. The project has examined and illustrated areas of vulnerabilities in the gaming and casino sectors with an emphasis on legal sectors that have a physical presence. The project has sought to identify sector-specific money laundering or terrorist financing indicators; and to highlight possible policy implications for effective implementation of the FATF standards to cover casinos and gaming.

Scope of Research

3. Typologies produced by the FATF and APG over the last 10 years have consistently identified a money laundering risk from casinos and gaming. The casino and gaming sector is characterised by diverse types of gambling activity, size and rate of development, as well as public and private sector ownership models.

4. Within the sector, the FATF recognised that casinos represent the greatest risk for money laundering activities and this was reflected in the revision of the FATF 40 Recommendations 2003, with obligations on casinos being significantly enhanced in relation to Customer Due Diligence (CDD), record keeping, reporting of suspicion, and comprehensive regulation and supervision.

5. Casinos are the only form of gaming or gambling explicitly covered by the FATF standards, however the FATF standards do not define casinos or gaming, nor do they set out the activities undertaken by casinos. It is left to each jurisdiction to determine the forms of gaming included in its coverage of "casinos".

Magnitude of casino sector globally

6. Statistics from 2007 show that over 150 countries participate in some kind of legal gambling, 100 of those countries have legalised casino and card room gambling. Over 100 countries offer some kind of lottery product and over 60 countries participate in the race and sports betting industry.[1]

7. Casinos generate enormous revenue streams for providers and for government through taxation and licensing fees. The size of the global casino business was estimated at over USD 70 billion in revenue in 2006, although a figure for overall turnover of funds was not available. Casinos in North America (US and Canada) account for almost half of that figure. Macao China is the fastest growing casino jurisdiction, and recorded more than USD 10 billion in gaming revenue in 2007. In addition there is a proliferation of Internet gambling sites, with global revenues estimated

[1] "Overview of Gaming Worldwide", *Casino City, Global Gaming Almanac*, 2007, http://www.casinocitypress.com/GamingAlmanac/globalgamingalmanac.

around USD 15 billion,[2] plus a significant amount of illegal gambling occurring around the world, which is largely unmeasured.

8. The nature and expanding scope of the casino sector presents a number of challenges for AML/CFT implementation. In particular:

- Casinos are cash intensive businesses, often operating 24hrs per day, with high volumes of large cash transactions taking place very quickly.
- Casinos offer many financial services (accounts, remittance, foreign exchange, cash issuing etc), but in some jurisdictions may only be regulated as 'entertainment' venues, rather than financial institutions.
- In some jurisdictions casinos are poorly regulated or unregulated for AML/CFT.
- A number of jurisdictions with well regulated casino sectors continue to identify significant levels of money laundering.
- Many casinos are located in geographic areas characterised by poor governance, political instability or bordering regions with significant crime or terrorist problems.
- The movement of funds associated with gaming-related tourism is poorly understood and may pose particular money laundering risks, *e.g.* international movement of funds for casino 'junket' operations[3].
- In some jurisdictions casino staff turnover is high, sometimes due to seasonal factors, which can lead to weaknesses in staff training and AML/CFT competencies.

9. A significant number of countries have recently established, expanded, or are considering expanding their gaming and casino sectors.

10. In response to these issues the FATF and APG began a project to consider money laundering and terrorist financing vulnerabilities in the Casino and Gaming sector.

11. This paper examines ML and TF vulnerabilities with legally operating casinos. The paper does not consider issues related to online gaming, but rather is concerned with casinos that have a physical presence. The aim of the project is to share information on the casino sector for the following purposes:

- Assist jurisdictions to understand money laundering and terrorist financing methods.
- Increase understanding in the casino sector of money laundering and terrorist financing vulnerabilities.

---

2 "eGaming Data Report: Global Internet Gambling Revenue Estimates and Projections", *Christensen Capital Advisors 2005*, http://www.cca-i.com.

3 The term Junket has its origins in Chinese where Jin literally means introducing and Ke means customers. It is a method of casino marketing developed in the late 1930s for introducing customers to the expanding Macao, China gaming industry. Over time this method has been adopted elsewhere and the term has gradually evolved to be known as Junkets.

- Assist law enforcement and gatekeepers in the industry to detect and deter forms of money laundering.
- Strengthen capacity and international information exchange.
- Provide evidential basis to support domestic implementation of AML/CFT measures in the sector.

12. The following chapters will:

- Examine the scope and nature of regional casino sectors.
- Identify and examine money laundering methodologies from known cases.
- Identify related indicators to support operational and policy objectives.
- Examine sector vulnerabilities and emerging issues.
- Highlight possible policy implications for effective implementation of the revised FATF 40 + 9 recommendations to cover casino operations.

13. Unless otherwise referenced, all data contained in this report is sourced from jurisdictional reports and research questionnaires submitted to APG and FATF.

Project scope / methodology

14. The APG began initial work on money laundering typologies in the casino sector in November 2006 during the Annual Typologies Workshop in Jakarta. At that time the APG commenced some preliminary scoping work and a number of APG jurisdictions shared their experience of AML/CFT issues in casino and gaming sectors.

15. The 2007 FATF/APG Typologies Meeting included a workshop on casinos and gaming. The workshop was very well supported by members of the FATF, APG and other FSRBs. The following jurisdictions were involved in the 2 day breakout session which considered issues in depth: Australia; Austria; Belgium; Canada; Ireland; Japan; Netherlands; New Zealand; Spain; United States; China; Hong Kong, China; India; South Africa; OECD; Cambodia; Macao, China; Malaysia; Papua New Guinea; Philippines; Thailand; and Vietnam.

16. Following on from the workshop in Bangkok, the FATF and APG distributed a short survey to FATF and FSRB members. The survey results were in addition to materials provided by APG member jurisdictions. The following jurisdictions provided a response to the survey:

Austria	Latvia	Spain
Belgium	Malta	Sweden
Brazil	Mexico	Ukraine
Finland	Poland	United Kingdom
Germany	Romania	
Iceland	Slovenia	

17. This project would like to acknowledge the particular input of New Zealand (Department of Internal Affairs), Australia (NSW Casino Control Authority and AUSTRAC); Canada (RCMP); Macao, China (Gaming Inspection & Coordination Bureau and Financial Intelligence Office); Hong Kong, China; Belgium; Austria; Spain; Vietnam; US; and the OECD.

CHAPTER 1: THE CASINO SECTOR

Introduction

18. There is very wide range of legal gaming / gambling across the globe. This includes various games of chance and gambling forms ranging from casino and card room gaming, lotteries, online gaming, race and sports wagering and charitable gaming, such as raffles, bingo and other low technology games. Legalised gambling has become more prevalent over the last 25 years as more jurisdictions take advantage of the revenue sources from the taxation and regulated gambling industries. Over this time many governments have allowed for the expansion of legal gambling, including casinos, or introduced regulatory regimes over existing gambling.

19. Based on information generated by the gaming sector, it is estimated that over 150 countries participate in some form of legal gambling and 100 of those countries participate in legalised casino and card room gambling. The broad AML/CFT network of FATF and FATF-style regional bodies includes over 180 jurisdictions globally. At least 77 of these 180+ jurisdictions have been indentified from the responses to research questionnaires and other requests for information, as having legally operating casino sectors.

20. *Appendix 1* provides summary tables of each the casino sectors operating in each region.

21. The casino market is in a major growth phase in most regions. At least three jurisdictions (Albania, Singapore and Papua New Guinea) have newly passed legislation and a greater number have recently expanded their casino sectors (South Korea; Macao, China; and Chile are examples). At least five jurisdictions have been identified as taking active steps towards legalising or giving consideration to legalising casinos (see section Emerging Markets).

22. A number of jurisdictions report significant problems from illegal gaming. Illegal gaming is largely beyond the focus of this study. It is recognised that illegal gaming is a factor in governments considering regulated gambling. A number of jurisdictions have casinos operating outside of legal frameworks. These include Sri Lanka (not clearly legal) and Myanmar.

23. A number of countries, recognising the social harms associated with gambling, have recently moved to restrict gambling growth in an effort to curb rising social costs (UK in relation to its 'super' casino and Russia through its four designated gaming zones).

24. There are a significant number of jurisdictions where gambling is illegal for religious and other reasons. In a number of these jurisdictions proponents are making a case for legal and regulated gambling to be introduced.

Regional Overviews

Africa

25. Sector studies view Africa as a significant growth region for casinos. This is the case in both the major casino market in South Africa and in smaller developing markets in other African jurisdictions. A number of casino jurisdictions in Africa do not regulate the sector for AML/CFT and a greater number appear to be poorly regulated. A number of jurisdictions have sought to restrict casinos only to foreigners.

26. Based on information from FSRBs, commercial databases and commercial studies casinos are known to be legally operating in Egypt (25), Morocco (8+) and Tunisia (4) (MENAFATF members).

27. Casinos operate in Cameroon (3), Central African Republic (2), Gambia, Ghana (3), Liberia (1), Mali (1) and Senegal (4) (all GIABA countries). Casinos operate in Botswana (11), Comoros (3), Kenya (15+), Malawi (1+), Mauritius (7+), Mozambique (3), Namibia (3), Seychelles (3), Swaziland (5+), Tanzania (7+), Uganda (3), and Zimbabwe (6) (ESAAMLG region).

28. South Africa is the only FATF member of this region and has over 40 legal casinos operating, making it by far the biggest casino sector in Africa. Casinos in South Africa are covered by AML/CFT controls There are a number of cases reported in the press of criminals attempting to launder proceeds of crime through one or a number of South Africa's casinos.

Middle East

29. Online commercial directories[4] list casinos operating in Iraq and Lebanon (1), both jurisdictions members of MENAFATF, but the nature and extent of casino gambling in these countries is unknown. Israel operates licensed cruise-ship casinos as well as land-based casinos.

Asia/Pacific

30. The Asia/Pacific region has the world's fastest growing economies, the world's strongest growth in tourism, and a vast array of cultures, languages, religions, political structures and consumer preferences. The region is also characterised by significant differences in wealth distribution ranging from well developed economies with strong governance and AML/CFT controls to some geographic areas characterised by poor governance, political instability or bordering regions with significant crime or terrorist problems. Some legal casino sectors are located in jurisdictions that have predominant cash-based economies and weak regulatory controls and/or no controls for AML/CFT. These factors present a significant challenge for governments and regional bodies committed to ensuring effective AML/CFT controls.

31. Within Asia there are legal casino sectors in: Korea (17); Lao PDR; Macao, China, China (29); Malaysia (1); Nepal (6); Philippines (14); and Vietnam (2). Sri Lanka has nine large casinos which are not regulated and are not subject to AML/CFT controls, but pay a levy to the government to operate pursuant to the Betting and Gaming Levy Act. Casinos in India are only permitted in one state and are not yet subject to AML controls. Press reports from late 2005 noted a draft bill had been prepared to regulate casinos in Nepal but this has not been enacted. Casinos in the Philippines are

[4] Casino City.

regulated, but there is no competent authority for AML/CFT matters, although the Philippine Amusement and Gaming Corporation (PAGCOR) have voluntarily agreed to submit suspicious transaction reports (STRs) to the Anti Money Laundering Council.

32. There is a mix of state and private ownership of casinos across the region. For example, in the Philippines, all casinos are state owned.

33. Some jurisdictions, such as Cambodia (21), Korea, Nepal and Vietnam restrict citizen access to casinos, only permitting foreign tourists to enter the casinos and gamble.

34. Hong Kong, China does not have a legal casino sector; many residents favouring travel to Macao, China due to its proximity and ease of access. Although the operation of casinos is illegal within the jurisdiction, Hong Kong, China is the home port for several cruise ships offering cruises into international waters principally to provide casino operations (see Chapter 3 for more information on 'high seas gambling').

35. Singapore is due to open its first casinos in 2009. Jurisdictions considering legalising casino gambling include Indonesia, Japan, Palau, Chinese Taipei, Thailand and Timor Leste (see box 2 below).

36. Casinos are illegal in Bangladesh, Brunei Darussalam, China, Chinese Taipei, Indonesia, Mongolia, Myanmar, and Pakistan.

Box 1. A Closer Look at Macao, China

Macao, China is a Special Administrative Region of China. Macao, China's population is just 0.5 million. The majority of the economy is linked to the tourism and casino industries. The casino industry now outstrips Las Vegas with casino revenue. Tax collected in 2008 made up over 70% of government total revenue. Macao, China holds the monopoly over casino-style gaming in the region with 31 casinos in operation.[5] There are approximately 30 million total visitor arrivals in 2008. Over half are from mainland China, the remaining predominantly from Hong Kong, Chinese Taipei and South East Asia. In 2002 Macao, China ended the gaming monopoly which had been dominated by Mr Stanley Ho's *Sociedade de Turismo e Diversões de Macao, China* (STDM) for 40 years. It liberalised the gaming industry by granting three casino gaming concessionaires and 3 sub-concessionaires.

The competent authorities responsible for the regulation of the casino sector are the Gaming Inspection and Coordination Bureau (DICJ) and the Judiciary Police. Criminal investigation of money laundering activities is undertaken by the Judiciary Police, whilst the preventative measures against money laundering are the responsibility of the DICJ. For currency exchange activities inside the casinos, they are under the supervision of the Monetary Authority of Macao.

Macao, China has introduced a licensing system to regulate junket operators. All licensed junket operators are obliged to file their information with the government, with their names published in the Official Gazette. Their licence will be reviewed periodically to see whether they are properly complying with the legislation and see whether they still fit the requirements of a junket operator. All casinos, junket operators and currency exchange counters inside the casinos have the duty to report Suspicious Transaction Reports to the Financial Intelligence Office of Macao, China. At the same time, casinos and junket operators have to submit large transaction reports to the Gaming Inspection and Coordination Bureau.

37. There are seven jurisdictions with legal casino sectors in the Pacific. These include Australia (13), New Caledonia, New Zealand (6), Northern Mariana Islands, La Réunion (France), Solomon Islands, and Vanuatu (1). Papua New Guinea passed legislation in 2007 for 23 land-based and online

5 As at September 2008, reported by The Gaming Inspection and Coordination Bureau.

casinos and Palau and Timor Leste are considering legalising casinos. All of the jurisdictions with casino sectors or considering legalising casinos are APG members, except for New Caledonia, Northern Mariana Islands, and, La Réunion (France). Casinos are not operating in Niue, the Cook Islands, Fiji, Tonga or Samoa.

38. Cruise ships operating in the Pacific include offshore gaming, but do not operate while in harbour on pacific islands. Pacific jurisdictions indicate that they lack clear information on the operation and regulation of these gaming cruise ships.

39. Australia is the largest casino sector in this region with 13 legally operated casinos, the first opening in Tasmania in 1973, and each state and territory having a least one. The casinos vary in size from 18 tables and 250 gaming machines to 350 tables and 2 500 gaming machines. Total gaming revenues from Australian casinos was recorded as AUD 2.8 billion in 2005/06.[6] Gaming revenue, the largest component of casino revenue, has experienced a 4.1% cumulative annual growth and average annual growth rate since 2002/03. Each state and territory has its own regulatory and licensing control over casinos, which includes investigation and enforcement. In addition, all casinos are classified as "regulated entities" under law and supervised by the FIU (AUSTRAC) for compliance to AML/CFT laws. Casinos are commercially owned and operated in Australia and open to both citizens and tourists.

40. New Zealand has six legally operated casinos, the first opening in 1994. Gambling revenue in casinos was reported at NZ469 million in 2007.[7] They are all commercially owned and operated and open to both citizens and tourists. New Zealand, however, does not have AML/CFT supervision of casinos, but has draft legislation underway to rectify this. Current laws provide financial reporting responsibilities to the FIU. General casino supervision is the responsibility of the Department of Internal Affairs, but casino licensing is the responsibility of a separate Gambling Commission. In 1997 the New Zealand Government passed a moratorium on new casinos, capping the number of legal casinos allowed to operate at six.

Central Asia

41. The Eurasian Group (EAG) report casinos operating in Kazakhstan and Kyrgyzstan (18). In Kazakhstan laws passed in April 2007 limit casinos to two provincial cities – Kapchagai and Shchuchinsk, but it is unknown if any regulation of AML controls are in place. The 18 casinos reported in Kyrgyzstan are regulated, including for AML/CFT, however a recent ME noted the casinos are showing some resistance to these laws.

42. Tajikistan, Turkmenistan, and Uzbekistan report no casinos operating, although it is uncertain if this is because of legal restrictions or market limitations.

Europe

43. Europe has long-established casino and gaming sectors and has experienced large-scale growth in recent years. Within Europe European Union (EU) members have responsibility to implement AML/CFT measures on casinos following the relevant EU directives. There are

---

6 "Australian Casino Economic Report 2005/06", July 2007, *Australian Casino Association*, http://www.auscasinos.com/documents/publicationsSubmissions/ACAFinalReport200506v3.pdf

7 Department of Internal Affairs. *Gambling Expenditure Statistics 1983 – 2007*, http://www.dia.govt.nz/Pubforms.nsf/URL/Expendstats07.pdf/$file/Expendstats07.pdf

39 jurisdictions in the Europe with reported legal casino sectors in operation. These include: Austria (12), Belgium (9), Cyprus (20+), Czech Republic (158), Denmark (6), France (161), Finland (1+), Georgia (2), Germany (62), Greece (9), Hungary (6), Italy (4), Latvia (14), Luxembourg (1), Malta (4), Poland (27), Portugal, Romania, Russia (348), Slovakia (4), Slovenia (14), Spain (39), Sweden (4), Switzerland (19), and the United Kingdom (165 licensed 140 operating). See Annex A for full details.

44. Casino ownership across Europe varies between state and private ownership, but some jurisdictions, such as Germany, Slovenia and Sweden have a mix of both. There is no citizenship prohibition reported. Most casino sectors are regulated and all are subject to AML/CFT controls. Casino jurisdictions rely less on junket or casino tourism operations and few European jurisdictions report commercial arrangements between casinos and junket promoters to support casino tourism.

45. In most European countries there exists alongside traditional casinos a low stakes gaming machine market. These machines can be found in many places, including sports betting shops and poker clubs.[8] With regards to the size of each sector, Russia has the largest sector with 348 operating casinos. After 1 July 2009, all gaming in Russia will be prohibited except within four newly created special gaming zones in Kalingrad, Rostov-na-Donu, Altai and Primorie Krai (Vladivostok), France, the Czech Republic, and the United Kingdom follow closely with 160, 158 and 140 respectively.

46. Austria has 12 casinos which generated approximately Euro 190 million in revenue in 2007 from 2.44 million visitors. Finland has just one casino which recorded annual turnover of EUR 30.9 million in 2007. Germany has 62 casinos which generated 944 million revenue in 2005 from 7.7 million visitors. Germany's casino sector employees approximately 5 000 staff. Slot machines account for 75% of gross earnings in German casinos. Malta has three casinos which employ over 600 people. Spain has 39 casinos which attracted 3.3 million visitors in 2006.

47. Ireland has a number of private gaming clubs operating casino-like facilities that create an AML/CFT risk, but which fall outside the scope of their AML laws. Casinos are reported to be illegal in Iceland, Norway and Turkey.

South America

48. Many Central and South American jurisdictions have well established gaming sectors (lotteries, sports betting, etc) but fewer have well established casino sectors. GAFISUD and online directories report casino sectors operating in Argentina (70+), Chile (17+), Uruguay (18), Peru (7), and Venezuela (5), however it is unknown the extent of regulation and/or AML controls over these sectors. Uruguay and Venezuela also report casino sectors, but no further information is available. It is unclear the extent to which South American casinos rely on introduced junket operations.

49. Argentina has a well established gaming market with further expansion taking place in the casino sector. Casinos do not operate in Bolivia, and it is unknown if Colombia, Ecuador and Paraguay have casino sectors.

50. Bolivia and Brazil prohibit casinos.

---

8 Rich Geller. "Saturation or Malaise?" *Global Gaming Business*, June 2008, p. 40.

The Caribbean and Central America

51. The Caribbean has more than 120 casinos on 15 islands. The CFATF reports casinos operating in the Bahamas (4), Belize (2), Costa Rica (35), Dominican Republic (44), Jamaica (10), Panama (14), and Suriname (9), but the level of regulation and AML controls is not clear.

52. Trinidad and Tobago have no legal casinos but have 72 registered Private Members Clubs that operate like casinos, but are not supervised by the government.

53. Open source material reports that Panama has 14 full-scale casinos with three additional licences being recently granted, and 29 gaming machines halls. Combined with non-casino gaming revenues, Panama has the second-largest gaming market in Latin America behind Argentina. AML/CFT controls appear to be lacking in Costa Rica, El Salvador, and Nicaragua despite recent attempts by their respective governments to better control and regulate the industries. The Dominican Republic does not extend AML controls to the sector.

54. In Bermuda, the Cayman Islands, Guatemala and Guyana casinos are illegal.

North America

55. Canada and the United States account for almost 50% of the global casino market.

56. Casinos in Canada are relatively recent with most opening in the early 1990s (except for Yukon where a charity casino was legalised in 1973). Canada now has 63 casinos operating in seven provinces and one territory (Yukon). 29 of these are commercial casinos which are usually state-owned or operated through service contracts with private corporations. There are 24 charity casinos licensed in Alberta, and one in Yukon, which are all privately owned. In Alberta, only religious or charitable groups may hold a casino licence. Also in Canada there are nine First Nations[9] casinos operating in Ontario, Manitoba and Saskatchewan. The provincial and territorial authorities are responsible for regulating all casinos, as well as municipal, provincial and federal law enforcement agencies. The Canadian FIU (FINTRAC) is responsible for ensuring that casinos are compliant with their responsibilities under AML/CFT laws.

57. Cruise ships operate out of Canadian waters and do offer casino facilities (except within five nautical miles of a Canadian port). As with many FATF/APG jurisdictions AML/CFT measures do not apply to cruise ship gambling.

58. The 2005 revenues and profits for commercial and charity casinos in Canada are shown in Table 2 below:

Table 1

	Revenues 2005	Profits 2005
Commercial Casinos	CAD 3.7 billion	CAD 1 billion
Charity Casinos in Alberta	CAD 1.2 billion	CAD 147 million

9. TBD.

59. The United States has approximately 845 casinos and card clubs operating in at least 30 jurisdictions (including Puerto Rico, the U.S. Virgin Islands and Tinian). Casino ownership in the United States is a mix of commercial and tribal ownership. In 2003, more than USD 800 billion was wagered at casinos and card clubs in the United States. In particular, there has been a rapid growth in riverboat and tribal casino gaming as well as card room gaming over the last ten years (see Box 5 for more on Indian Gaming in the United States). Collectively, tribal casinos took in USD 25.7 billion in revenue in 2006, compared with Nevada's revenues of USD 12.06 billion for the same year.

60. Gambling is primarily a matter of state/territory law and responsibility for regulating casinos falls on state gaming commissions and the National Indian Gaming Commission. All legally licensed casino and card clubs with gross annual revenues greater than USD 1 million are subject to Federal AML requirements in the BSA. Covered gaming establishments (state licensed land based, riverboat, tribal casinos and card clubs) are subject to AML requirements. The US FIU (FINCEN) administers the BSA but does not directly examine casino for compliance with the law. That is delegated to the Internal Revenue Service (IRS). For floating casinos, i.e. gambling "cruises to nowhere" which operate out of certain states along the East Coast of the US to conduct gambling beyond the 3 nautical miles limit, customers are subject to reporting currency and monetary instruments of $10,000 or more when sailing both in and out of US territorial waters ships. Moreover, the operators of the "cruises to nowhere" are required to file tax notices for jackpot wins of USD 1200 or more.

Box 2. Indian Gaming in the United States

Tribal government-sponsored gaming is an evolution dating back to the late 1970's. After the Supreme Court confirmed (in 1987) the right of the tribal governments to establish gaming operations, Congress passed in 1988 the Indian Gaming Regulatory Act (IGRA) (25 USC 2701) which recognized, but limited, the right of tribes "to conduct gaming operations" and embodies a compromise between state and tribal interest. According to the IGRA, the states are given a voice in determining the scope and extent of tribal gaming by requiring tribal-state compacts for all forms of casinos style gambling and other gaming activities. Most recently tribal casinos have moved rapidly from relative obscurity within the casinos industry to prominent position with ample potential for money laundering and other types of financial crimes. There are 567 federally recognised Indian Tribes, half of which are in Alaska, and 225 of them operate 411 gaming facilities in 28 states.[10] Of these 307 are considered casino operations, while the remainder are basically bingo halls. Collectively, the tribal casinos took in USD 25.7 billion in revenue in 2006, more than twice the amount generated by Nevada casinos.[11] If the tribal gaming industry were a single company, rather than 307 casinos, it would rank near the top 100 corporations in America. Tribal gaming interests have what is currently the largest casino in the United States, Foxwoods Resort and Casino, located in Mashantucket, Connecticut and owned by the Mashantucket Pequot Tribe. The west coast, primarily California, represents the fastest growing region for the Indian gaming industry.

61. Mexico reports a growing gaming industry; however, the only casino-style of gambling authorised is in betting game halls exclusive to regional fairs with cards, dice and roulette. These are Temporary permits for large-scale "salones de Apuestas ", regulated by the Secretaría de Gobernación (Ministry of Interior), but not subject to AML controls. The Mexican government do not foresee any permanent casinos being located or permitted to operate within national territory.

10 "An Analysis of the Economic Impact of Indian Gaming in 2006", *National Indian Gaming Association,* http://www.indiangaming.org/info/pr/press-releases-2007/NIGA_econ_impact_2006.pdf

11 "Tribal casino revenue up 5 percent nationwide", *Associated Press*. June 19 2008, http://blog.mlive.com/kzgazette/2008/06/tribal_casino_revenue_up_5_per.html

Emerging Markets

62. Given the scope of potential revenue and the interest in foreign direct investment, a number of regions have significant emerging markets in the casino and gaming sectors. This is particularly the case in the Asia/Pacific region and in Africa.

63. A number of developing countries with predominantly cash-based economies and weak or limited AML/CFT capacity are giving active consideration to establishing casino sectors. Some of the smaller less developed countries considering legalising casinos include Palau and Timor Leste.

64. Singapore has passed legislation which provides for granting two licences for large-scale casinos. The licensing remains subject to confirmation of suitability of the two casino operators.

65. Papua New Guinea passed legislation in 2007 for approximately 20 land-based and online casinos.

66. Japan has indicated has organised crime groups running casino-like operations for online gaming, but is giving consideration to establishing luxury casino resorts by 2012 if liberalisation of the gaming market goes ahead.

67. Chinese Taipei is considering proposals to open up the island nation's gambling business by revising legislation that may allow casinos on the offshore islands of Chinese Taipei.[12]

68. Thailand is also considering legalising gambling after the findings of a detailed study on the prevalence of illegal casinos at the border between Thailand and Myanmar and related flows of funds to neighbouring casino jurisdictions. Thailand estimates USD 4-17 billion in illegal gambling turnover annually and 100 000 people arrested per annum for illegal gaming.

Box 3. Drivers for Change in Asia

Market analysts consider that the Asia region has an undersupply of quality legal casino venues. Such analysts view Asia as having the greatest potential for growth in casino revenue and venue development. The key drivers for regulatory change in the Asia region include:

1. Economic growth resulting in increased disposable income.
2. Changing social attitudes.
3. Increased media and government attention on existing illegal gambling industries.
4. Need for increased taxation revenues.
5. Need for tourism infrastructure development.
6. Availability of private sector capital for foreign direct investment.

However, issues that drive resistance to regulatory change include:

1. Social conservatism.
2. Religion.
3. Corruption in government.
4. Incumbent illegal and legal operators.
5. Government inefficiency or insufficient capability to affect change.
6. Voter/communities lack of faith in government to effectively regulate and control the industry.

12 Global Gaming Business, "Asia Update", June 2008, p. 30.

Conclusion

69. What is shown in this chapter and in detailed tables at Annex A is the extent of casino gambling around the world and the diversity of each region's sector. Demand for casino gambling services is high and increasing and is associated with high revenues for government. This is leading some jurisdictions to legalise gambling particularly in developing countries.

70. There are established casino sectors in jurisdictions with government oversight, but are unregulated for AML/CFT.

71. The next two chapters set out a number of vulnerabilities of casinos to money laundering by describing the methods and indicators of money laundering from past cases and the casino sector vulnerabilities and emerging AML-related issues.

CASINO SECTOR RISK ASSESSMENTS FOR MONEY LAUNDERING & TERRORIST FINANCING

The need for casino sector-specific risk assessments

72. The casinos project group considered the need to conduct periodic assessments of ML/TF risks in the casino and gaming sector. The project group discussed the benefits of understanding the nature of the ML/TF environment to allow regulatory and enforcement agencies to better allocate resources to address priority risks in the casino sector.

73. ML/TF is one aspect of criminal risk. Risk assessments of the casino sector may look at broader risks including organised crime, loan sharking, prostitution, drug dealing, human trafficking etc.

Guidance on Typologies Risk Assessments

74. The FATF WGTYP June 2008 paper on Risk Assessments identifies factors that may influence the ML/TF risk in a county and suggests information to access when conducting a risk assessment. The WGTYP paper highlights a wide range of factor to be covered in a risk assessment. For the casino and gaming sector, these may include:

- Legal and regulatory environment.
- Characteristics of the economy as well as the casino/gaming sector.
- Ownership structure, integrity, internal controls and corporate governance of casino/gaming institutions.
- Ownership structure, integrity internal controls and corporate governance of intermediaries and associated businesses (junket promoters, agents, gaming equipment, financial service providers).
- Types of products and services offered and clients served.
- Criminal activities and proceeds of crime generated domestically as well as generated abroad but laundered domestically.
- Financial services offered by casino/gaming institutions and by casino intermediaries (junket promoters, agents etc).

Sources of information

75. Responses received from FATF/APG questionnaires indicate that many jurisdictions are receiving suspicious activity reports from casinos or that relate to casino activity. Casino regulators, law enforcement, bank regulators and FIUs hold useful information to assess risk areas.

76. The project group noted that a number of commercial companies provide baseline information on national and regional casino and gaming trends, including size, scope and nature of markets; trends in investment and regulation and criminal exploitation, including money laundering. This information can assist competent authorities understand the nature of their sector as well as offshore sectors.

Risks for jurisdictions without a casino sector

77. The casinos project group discussed why and how a jurisdiction without a casino sector may undertake an ML/TF risk assessment. These may be undertaken in response to illegal gaming as well as the movement of persons and funds to another gaming jurisdiction to launder the proceeds of crime.

Models for casino sector risk assessments

78. A number of countries have recently undertaken casino sector risks assessments. The models of assessment have varied, depending on the agency undertaking the assessment and the purpose (*e.g.* policy settings, law enforcement responses, regulatory compliance).

Police-led assessment - e.g. Canada

79. Canada's RCMP has recently undertaken a police-led assessment of ML risks in the casino sector. This involved working with a very wide range of stakeholders to identify national sector-specific risks. As with other risk assessments, the RCMP drew on a wide range of information sources to understand risks in the sector. These included typologies trends derived from the FIU; interviews with operators in the sector, including staff of casinos (pit bosses, owners, security etc); and information collected from intelligence databases on related crime trends.

80. The assessment aimed to understand:

- The scope of the casino sector: number, type, location, ownership, risk profile etc of casinos.
- How Casinos are used as financial intermediaries.
- Law enforcement cases / intelligence of how casinos are used for ML or are associated with predicate offences (fraud, loan sharking etc).
- Criminal trends linked to casinos.

Academic Sectors – e.g. Thailand

81. Thailand is a jurisdiction where casinos and gaming are illegal. Thai authorities have long recognised a very significant illegal gaming problem and the large scale movement of Thai nationals to foreign casino jurisdictions.

82. In order to better understand background issues, Thailand sought the assistance of the academic sector to undertake a scoping study of the impact of illegal gaming on Thailand, including ML and TF risks to the country. Thai authorities have given some consideration to regulatory reform and the possible licensing of some forms of gaming, including casinos.

83. The scope of the Thai assessment included the value of gaming sector (illegal and offshore gaming); scope of illegal gaming; movement of Thai people to foreign jurisdictions for gaming; risks for ML/TF and other predicate offences (smuggling, drugs, human trafficking etc); and impact on the community from illegal gaming.

- Over 100 000 people are arrested each year for illegal gambling offences.
- It is estimated that there are 200 to 300 illegal gambling houses in Bangkok.
- Annual turnover for illegal gambling houses in Bangkok is estimated at between USD 4 to 17 billion and for those outside Bangkok is USD 2 to 4 billion.
- There are 27 legal or semi-legal casinos operating in neighbouring countries within very close proximity of the Thai border servicing Thai gamblers.
- Thai junket operators offer casino tourism services in major Thai cities to move people and funds to these 'offshore' casinos.
- Movement of Thai citizens to border casinos increases risks associated with currency smuggling and cross-border crime risks including smuggling, human trafficking and drug trafficking.

Regulator-led assessments – e.g. Australia

84. In Australia, AUSTRAC, as the AML/CFT regulator, and various state-based casino regulators have worked together to conduct a preliminary assessment of key typologies and regulatory risk related to money laundering and terrorist financing. This has involved considering a range of law enforcement information, regulatory information and sector information to identify areas of specific risk and to supporting preparation of AML guidelines and AML/CFT supervision and monitoring.

CHAPTER 2: MONEY LAUNDERING METHODOLOGIES AND INDICATORS

85. This chapter will identify and examine money laundering methods from known cases and draw out related indicators to support the detection of money laundering activity.

Broad risks in casinos

86. Casinos are by definition non-financial institutions. As part of their operation casinos offer gambling for entertainment, but also undertake various financial activities that are similar to financial institutions, which put them at risk of money laundering. Most, if not all, casinos conduct financial activities akin to financial institutions including: accepting funds on account; conducting money exchange; conducting money transfers; foreign currency exchange; stored value services; debit card cashing facilities, cheque cashing; safety deposit boxes; etc. In many cases these financial services are available 24 hours a day.

87. It is the variety, frequency and volume of transactions that makes the casino sector particularly vulnerable to money laundering. Casinos are by nature a cash intensive business and the majority of transactions are cash based. During a single visit to a casino a customer may undertake one or many cash or electronic transactions, at either the 'buy in' stage, during play, or at the 'cash out' stage.[13] It is this routine exchange of cash for casino chips or plaques[14], TITO tickets[15], and certified cheques, as well as the provision of electronic transactions to and from casino deposit accounts, casinos in other jurisdictions and the movement of funds in and out of the financial sector, which makes casinos an attractive target for those attempting to launder money.

88. As this research is solely focused on casinos, the data collected is not wide enough to carry out statistical trend analysis. Chapter 3, however, does provide specific sector vulnerabilities and emerging issues as a start to this broader study. It is also recognised that methods and indicators are immediately useful to private sector organisations seeking to develop effective AML/CFT processes.

---

13 The 'buy in' stage is when a customer enters a casino and purchases casino chips, tickets, or gaming machine credits in order to commence gambling. The 'cash out' stage is when a customer converts casino chips, tickets or gaming machine credits for cash, casino cheque, credits an account or transfers funds to another casino.

14 The term 'casino chip' also refers to plaques and other wagering instruments provided by the casino.

15 Ticket In/Ticket Out (TITO) is a gaming machine system that allows a gaming machine to accept either banknotes or tickets with a credit value printed on them (Ticket In) to commence play. TITO also prints tickets with a credit value when a player wishes to 'cash out' of the gaming machine (Ticket Out). The player can them redeem his/her ticket for cash at a cashier's desk, ticket redemption kiosk, or insert the ticket into another TITO machine and continue playing. A ticket redemption kiosk machine is a multifunctional device, connected to a gateway or kiosk server, that can perform a variety of financial transactions for customers, such as redeeming slot machine/video lottery tickets for currency, exchanging currency for currency (*i.e.*, breaking bills or paper money), redeeming player slot club points, purchasing slot machine vouchers (*i.e.*, tickets), and initiating electronic transfers of money to or from a wagering account including currency withdrawals from a casino ATM.

89. The importance of studying money laundering methods – the "how to" – cannot be overstated. Such studies provide government decision-makers and operational experts with the material to target policies and strategies for combating financial crime. The sharing of these methods, together with indicators to detect money laundering activity, with responsible financial and non-financial organisations is equally important. They are a necessary tool for financial institutions, other financial intermediaries and gatekeepers who are on the front line in confronting activities that may or may not be suspicious (and thus may or may not be related in some way to money laundering, terrorist financing or some other financial crime).

90. For the private sector, and in this case casino owners and operators, valid money laundering indicators are therefore essential in establishing and "calibrating" mechanisms that help to identify suspicious or unusual transactions which must then be reported to a financial intelligence unit.

91. For the purposes of this chapter the following definitions apply:[16]

- *Method:* a particular procedure for carrying out money laundering activity. There are further distinctions in the concept of a money laundering method:
    - *Technique:* a particular action or way that the activity is carried out, for example, purchasing a cashier's cheque.
    - *Mechanism:* a system or thing that carries out part of the process. An example of a money laundering mechanism is a casino.
    - *Instrument:* an object of value (or representing value) that is somehow used in the money laundering process, for example, a casino cheque or casino chips.

92. For example, the action of depositing funds into a casino account relates to all three concepts: *i)* depositing the funds is a *technique*, *ii)* the casino managing the account is a *mechanism* and *iii)* the funds deposited are an *instrument*. It should be noted as well that, for the most part, the examples provided for each of these concepts may not in and of themselves represent illegal activities. Indeed it is only when these *techniques*, *mechanisms* and *instruments* are put together to form a money laundering activity that they become illegal.

93. With regards to indicators, there is sometimes confusion between a money laundering indicator and a money laundering method. While it is sometimes true that the methods defined below could indicate money laundering activity, they are not synonymous. For example, exchanging chips for cash is not by itself an indicator of money laundering. By the same token, indicators are not all necessarily money laundering methods.

Criminal interest in casinos – players and infiltration of casinos

94. Casinos are attractive venues for criminals. Casinos are consistently targeted by criminals for criminal influence and criminal exploitation. Organised crime groups seek to control or own casinos or aspects of casino operations. Criminals attempt to infiltrate or influence casinos to facilitate theft, fraud, money laundering and other crimes.

95. A core function of all casino regulators is making certain that gaming is conducted honestly by approving the rules of the games and requiring the operator to provide a high standard of

16 Financial Action Task Force. *Money Laundering & Terrorist Financing Trends and Indicators Initial Perspectives.*

surveillance and security systems. This ensures public confidence in the gaming product, minimises opportunities for criminal activity and provides certainty of government revenue streams.

96. Criminal influence and exploitation of casinos appears to be both for possible money laundering, but also for recreation and in some cases enhancing their criminal endeavours outside the casino. Casinos have been noted as a place where criminals and organised crime figures like to socialise and particularly like to spend and launder their criminal proceeds.

97. Feedback from police also indicates that large casinos with sophisticated security and surveillance systems may be viewed by criminals as providing a safe haven to meet and associate in without fear for their personal safety.

98. Gaming venues attract ancillary criminal activities including loan sharking, vice and other crimes.

Box 4. Loan Sharking

Loan Sharking (also known as usury) is prevalent in casinos in a number of jurisdictions. Loan sharking is a crime that involves loaning money to individuals at an interest rate that is above a maximum legal rate, sometimes collected under blackmail or threats of violence. Loan sharks may be financed and supported by organised crime networks who are also involved in money laundering activities. A loan shark usually preys on individuals who are problem gamblers, struggling financially or, for some reason, are unwilling to seek credit from legal sources.

Persons in debt to loan sharks may be coerced into assisting with money laundering schemes in the casino.

Box 5. Credit card scam using the casino

A jurisdiction reported a credit card point scam where casino chips are purchased using credit cards. The chips are then cashed out and instead of crediting the credit card, casinos usually issue cash or a casino cheque. The balance on the credit card is eligible for consumer points. The balance on the credit card is paid back using the cash or cheque received from the casino. This method enabled large amounts of credit card points to be accumulated in a short period of time and can be used for merchandise purchases.

Money laundering methods and techniques in Casinos

99. The money laundering methods outlined in this chapter are:

- Use of Casino Value Instruments (cash / casino chips / TITO / gaming machine credits / cashier's orders / casino cheques / gift certificates / chip purchase vouchers / casino reward cards).
- Structuring / Refining.
- Use of Casino Accounts (credit accounts, markers[17], foreign holding accounts) / facilities.
- Intentional losses.
- Winnings / intentional losses.

17 Casino markers act as a credit line through a personal checking account, no transaction occurs, but are issued once a patron submits their checking account number and a cheque to the casino. The casino has the right to deposit the marker at any time but usually waits a few months to allow for customers to pay back the credit if the losses are high. Money launderers will pay back the debt with the proceeds of crime.

- Currency Exchange.
- Employee Complicity.
- Credit Cards / Debit Cards.
- False Documents.

100. Each method is illustrated by representative cases[18] and followed up with related indicators that can be used to detect suspicious or unusual transactions by casino owners and operators. The methods, cases and indicators have been generated from the following research material:[19]

- Sanitised case material from regulatory, law enforcement and security organisations.
- International case study and typology reports including FATF, APG and the Egmont Group.
- Open source research.

Casino value instruments

Cash / Casino Chips / TITO / Gaming Machine Credits / Cashier's Orders / Casino Cheques / Gift Certificates / Chip Purchase Vouchers / Casino Reward Cards

101. Casinos utilise various value instruments to facilitate gambling by their customers. The type and use of the value instruments listed above differs between casinos and is influenced by local regulation and casino operating structures. Casino value instruments are most often used for money laundering by converting illicit funds from one form to another.

102. Casino chips are the most common casino value instruments. Casino chips are issued by casinos and used in lieu of cash in gaming transactions between the house and players. Chips are round and marked with the denomination and name of the casino and are negotiable within the casino, or, in some cases, within casinos in the same group. Casinos may issue 'credit chips' which are different in colour and only used by patrons playing on credit. Casinos may issue 'dead chips' which are only used by *junket* patrons (*see section below on junkets*).

103. ***Buying chips for cash or on account, then redeeming value by way of a casino cheque, bank draft of money transfer.*** Launderers typically buy chips with cash or through their casino account. Chips bought on account may use a Chip Purchase Voucher (CPV) or similar value instrument. Repayment is then requested by a cheque, draft or transfer drawn on the casino's account. This method can be made more opaque by using a chain of casinos where the chips that were purchased with illicit cash are converted to credit, and transferred to another jurisdiction in which the casino chain has an establishment; the credit is then converted into in the form of a casino cheque at the second casino.

---

[18] The cases outlined are provided from jurisdictions contributing to the project research, and while some countries may appear to be over/under-represented in the cases, this is not an indicator of high or low levels of money laundering within that country, but merely a reflection of that government's willingness to share money laundering information to support global AML awareness.

[19] It is important to note that this chapter does not provide a description of all methods used to facilitate money laundering. It is limited to those methods that have been reported to FATF or APG and from cases that have been approved for use in the public forum.

104. Money launderers may hold the chips for a period of time, either using the chips to gamble in hopes of generating certifiable winnings or later redeeming the chips for cash/ cheque / transfer.

105. ***Purchase of chips from 'clean' players at a higher price*** – Money launderers may purchase chips from other money launderers or un-associated casino patrons with 'clean' backgrounds. This is done at a price greater than the chips' face value. This is referred to as *value tampering*.

106. ***Casino cheques payable to cash*** – in some jurisdictions, casinos allow winning cheques to be made payable to 'cash'. High-value casino cheques payable to cash have been observed in secondary circulation as bearer negotiable instruments and used as payment for goods or for reinvestment in criminal ventures, such as purchasing drugs. High-value casino cheques may originate from VIP rooms, which may provide alternative remittance services between player's home jurisdictions and the casino VIP room.

107. ***Combining winnings and cash into casino cheques*** – although few jurisdictions allow this, money launderers seek to add cash to casino winnings and then exchange the combined cash and winnings for a single cheque.

108. ***Use of chips as currency in illegal transactions –*** money launderers may retain casino chips to be used as currency to purchase drugs or other illegal goods. Carrying chips from a drug transaction may also contribute to an alibi for the predicate offence. The recipient of the chips will later cash them at the casino.

109. Casino chips to be used as currency may be taken across borders and exchanged for payment of an illegal enterprise then returned by the third parties and cashed at the issuing or honouring casino in amounts below a reporting threshold. Most jurisdictions do not list casino chips as money value instruments and therefore do not require Customs declaration.

110. In some jurisdictions, casino chips from one casino can be utilised in another associated casino. Cases showed that the money launderers will take advantage of this arrangement to avoid attracting attention to their activities at the one casino. This may take in another jurisdiction. To prevent this some jurisdictions require casinos to have casino-specific chips and do not allow inter-casino chip cashing.

111. ***Purchase of large numbers of 'casino gift certificates' –*** Cases have been detected of money launderers purchasing high value or numerous low value casino gift certificates which can be redeemed by 3rd parties. The certificates are then sold or given to other persons distancing the money launderer from the illicit funds.

112. ***Purchase of casino reward cards –*** Money launderers use illicit funds to purchase casino reward cards from legitimate customers paying them a premium above the value of the reward.

Case 1. Casino used as preferred method to launder millions

Offence:	Money Laundering
Jurisdiction:	Australia
Technique:	Chip purchase and cash out, claiming credits as jackpot wins, playing games with low return and high win.
Mechanism:	Casino
Instrument:	Casino chips, casino cheques

Information identified alleged money launderers using the casino as a preferred method of laundering millions of dollars accumulated from criminal activities. The methods used to launder the money included purchasing and cashing out chips without playing, putting funds through slot machines and claiming credits as a jackpot win and playing games with low returns but higher chances of winning. The same group were also utilising bank

accounts and businesses to launder funds.

Case 2. Purchase of chips and gambling without clear intention to win

Offence:	Money Laundering
Jurisdiction:	Belgium
Technique:	Chip purchase and cash out, claiming credits as jackpot wins, playing games with low return and high win.
Mechanism:	Casino
Instrument:	Casino chips, casino cheques

Two Asian males residing in Belgium went to a Belgian casino twice to purchase chips for a total amount of almost 25 000 EUR. When visiting they did not play at the tables and immediately collected funds through a third person, also an Asian national.

Investigations indicated that the three persons were students and lived at a common address with other Asian students. It appeared that the transactions were likely to be linked to human trafficking. By not playing at the casino and collecting the money through a third person they wanted to leave a paper trail in order to justify the origin of the funds.

Case 3. Proceeds of drugs used to purchase chips and claim funds as winnings

Offence:	Drug importation
Jurisdiction:	Australia
Technique:	Chip purchase and cash out
Mechanism:	Casino
Instrument:	Casino chips, chip to cash transfer, casino cheques

A cargo consignment addressed to a person contained approximately 3.4 kilograms of black opium resin, concealed within the contents. The person was arrested when attempting to collect the consignment. Further investigation revealed the person to be a regular customer of a casino, having conducted approximately 50 betting transactions, predominantly chip cash outs totalling AUD 890 000. Very little casino gaming play was recorded for the person and it was assumed that he used the proceeds from previous importations to purchase chips and claim the funds as winnings.

Case 4. Proceeds from stolen cheques used to purchase casino chips

Offence:	Money Laundering
Jurisdiction:	United Kingdom, India
Technique:	Purchase casino chips
Mechanism:	Casino
Instrument:	Casino chips

In November 2007 two men were convicted for their part in a GBP 25 000 cheque scam. The victim was robbed at New Delhi Railway Station in India in March 2006 and among the items stolen were two Barclays cheque books. The money laundering trail led authorities to a casino in London where cash withdrawn from the defendants account was used to purchase gambling chips. Both men claimed gambling addictions. STRs were not submitted by the casino in this case.

Case 5. Cash laundered through casino used to bribe officials

Offence:	Money Laundering
Jurisdiction:	Korea
Technique:	Cash to chip to cash/cheque transfers
Mechanism:	Casino
Instrument:	Casino chips, casino cheques

Early 2006 a bribery case involving money laundering at a casino was investigated by the Public Prosecutor's Office. A legal broker bought casino chips with cheques to a total of KRW 20 billion (approx USD 20 million) from 2003 to 2005 and then changed the chips with cash and cheques issued by the casino. He then used the money to bribe politicians and senior government officials.

Case 6. Casino reward cards traded for gold coins

Offence:	Money Laundering
Jurisdiction:	United States
Technique:	Purchase casino reward cards from legitimate customers
Mechanism:	Casino
Instrument:	Casino reward cards, gold coins

A suspect purchased casino reward cards from legitimate customers at a US casino. The cards increase in value with each casino visit and with each gambling session. The cards were purchased with illicit funds and were then traded for gold coins at the casino's store. An employee at the store was an accomplice in the laundering scheme.

Case 7. Embezzled money laundered through casino

Offence:	Money Laundering
Jurisdiction:	United States
Technique:	Purchase and cash out with little or no gaming activity
Mechanism:	Casino
Instrument:	Casino chips

A lawyer was sentenced in New Jersey for embezzling more than USD 500 000 and laundering USD 250 000 of it through an Atlantic City casino. The defendant wire transferred USD 250 000 to the casino and arrived at the casino later the same day to launder the funds. He purchased casino chips and gambled for an hour on a roulette table losing USD 10 000. He then cashed out the remaining USD 240 000 into currency and left the casino.

Case 8. Embezzled money laundered through casino

Offence:	Money Laundering
Jurisdiction:	Spain
Technique:	Purchase and cash out with little or no gaming activity, casino cheques in the name of 3rd parties
Mechanism:	Casino
Instrument:	Casino chips

Different people entered separately in a casino and bought chips. After playing minor amounts of chips they tried to change chips and requested a cheque paid to the name of a third person. They tried to do the same operation with different people and lower amounts one day later, which raised suspicion of casino operators.

Indicators of ML using casino value instruments

- Inserting funds into gaming machines and immediately claiming those funds as credits.
- Customers claiming gaming machine credits/payouts with no jackpot.
- Customers claiming a high level of gaming machine payouts.
- Noticeable spending/betting pattern changes.
- Customers frequently inserting substantial amounts of banknotes in gaming machines that have high payout percentages and do not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play.
- Frequent even-money wagering when conducted by a pair of betters covering both sides of an even bet (e.g., in roulette, baccarat/mini-baccarat, or craps).
- Customer's intention to win is absent or secondary.

- Two or more customers frequently wagering against one another on even-money games.
- Customer in possession of large amounts of coinage or bills.
- Customer befriending/attempting to befriend casino employees.
- Purchasing and cashing out casino chips with little or no gaming activity.
- Customer requests to add cash to casino winnings and then exchanging the combined cash and winnings for a single cheque.
- Multiple cheques being requested or drawn on account.
- High volume of transactions within a short period.
- Multiple chip cash outs on the same day.
- Structuring of chip/cheque transactions.
- Chip cash out is same/similar to chip purchase.
- Requests for credit transfers to other casinos.
- Use of multiple names to conduct similar activity.
- Use of third parties to purchase casino chips.
- Use of credit cards to purchase casino chips.
- Use of personal cheques, bank cheques and traveller's cheques to purchase casino chips.
- Customer due diligence challenges, e.g. refusals, false documents, one-offs, tourists passing trade.
- Customer purchases chips and leaves casino shortly after.
- CPV, TITO, ticket or voucher dated prior to date of redemption.
- Large chip purchases.
- Frequent purchase of casino gift certificates.
- Unexplained income inconsistent with financial situation/customer profile.
- Supposed winnings do not correspond with recorded winnings.
- Dramatic or rapid increase in size and frequency of transactions for regular account holder.
- Detection of chips brought into the casino.

Structuring

113. Structuring or 'smurfing' involves the distribution of a large amount of cash into a number of smaller transactions in order to minimise suspicion and evade threshold reporting requirements. Common methods of structuring include:

- Regularly depositing or transacting similar amounts of cash, which are below a country's reporting disclosure limit.
- The use of third parties to undertake transactions using single or multiple accounts.
- Using cheques from multiple financial institutions or branches of a financial institution to 'buy in' while the amount of each cheque is below the reporting threshold.
- Utilising shift changes to systematically 'cash in' chips or other value instruments to avoid threshold reporting.
- Regularly switching gaming tables, gaming rooms, junkets or casinos within a chain when the wagering amounts are approaching the reporting threshold.
- Requesting the division of winnings or prize money, which exceeds the reporting threshold, to be broken down into cash and chips below the reporting threshold in order to exchange it at the cashier's desk.

114. While money launderers will often structure their transactions to avoid financial institutions filing reports to authorities, it has been found that some money launderers using casinos have the opposite strategy and seek to trigger a cash transaction report to further authenticate a transaction.

Case 9. Using reporting thresholds to legitimise suspicious transactions

Offence:	Money laundering
Jurisdiction:	United States
Technique:	Use of third parties, triggering transaction reports to legitimise suspicious transactions
Mechanism:	Casino
Instrument:	Casino chips, casino cheque

A number of persons purchased chips with illicit cash in amounts below the CTR threshold, but then passed the chips to one individual who cashed out, receiving a casino cheque and triggering the filing or a CTRC that gave the appearance of further authenticating the transaction. Over a twelve-month period, one individual was named in casino CTRCs reporting UDS1.1million paid out, but was not named in a single CTRC for cash taken in.

Refining

Exchanging low denomination for high denomination currency

115. Individual launderers or organised groups use casino services to refine large amounts of low denomination bank notes into more manageable high denomination notes. Some countries note this as being associated with drug dealers who accumulate large amounts of small denomination bills from drug sales. In cases of groups, they may seek to refine money by dividing it amongst the group before entering the casino. The group enter the casino, individually refine their portion of the money and meet again outside the casino to assemble the total amount. The refining techniques most commonly identified are listed below:

116. ***Refining using the cashier's desk*** – money launders exchange coins or small denomination bills for larger denomination bills at the cashier's desk.

117. ***Refining using 'note acceptors' or gaming machines that accept cash*** – Most casinos with gaming machines have 'note acceptors'. Money launderers will feed currency notes into the machine to accumulate credit with little or no play before redeeming the credits. As the amount can be quite large, it requires a 'ticket' or similar document provided by the slot attendant as proof to enable the exchange for cash or cheque at the casino cashier's desk. Gaming machines, Video Lottery Terminals (VLTs) and Ticket In/ Ticket Out (TITO) machines are used to refine currency. Gaming machines, TITO machines and VLTs are fed large sums of low denomination cash. Launderers redeem credits with minimal play. The ticket is then cashed at the cashier's desk, ticket redemption kiosk, for high denomination bills.

118. ***Use of casino account for refining*** – launderers pay low denomination cash into their casino accounts and withdrawn funds with cash of higher denominations.

Case 10. Refining low denomination notes

Jurisdiction:	Spain
Technique:	Refining, Use of third parties
Mechanism:	Casino
Instrument:	Cash, casino chips, remittance arrangement

A group of three foreign people entered separately in a casino and bought chips, paying with low denomination notes. They didn't play any game, and after they changed the chips that they had bought trying to obtain high denomination notes.

Case 11. Drug proceeds converted into casino chips by third parties

Offence:	Drug importation
Jurisdiction:	Australia, Vietnam
Technique:	Use of third parties
Mechanism:	Casino, remittance agent
Instrument:	Casino chips, remittance arrangement

A person was involved in the importation and distribution of heroin into Australia from Vietnam. The person gambled a large proportion of the proceeds at casinos and used third parties to purchase gaming chips on his behalf. Reports from the casino noted multiple chip cash outs on the same day, with some of these transactions being structured to avoid the AUD 10 000 reporting threshold.

Further investigations noted that he would send large cash payments to various entities in Vietnam through a remittance dealer. The remittance dealer was a trusted associate of the person and had been non-compliant with his reporting obligations.

Indicators of ML using structuring/refining methods

- Activity was inconsistent with the customer's profile.
- Associations with multiple accounts under multiple names.
- Use of multiple names to conduct similar activity.
- Depositing multiple amounts of cash and receiving multiple cheques drawn on that account.
- Multiple individuals sending funds to the one beneficiary.
- Cheque issued to a family member of the person.

- Third party presents for all transactions but does not participate in the actual transaction.
- Transferring funds into third party accounts.
- Transactions on casino accounts conducted by persons other than the account holder.
- Use of third parties to undertake structuring of deposits and wire transfers.
- Use of a remittance dealer / junket operators to deposit or withdraw cash.
- Use of third parties to purchase gaming chips.
- Use of third party to conduct wagering.
- Cash handed to third party after cash out.
- High volume of transactions within a short period.
- Purchasing and cashing out casino chips with no gaming activity.
- Exchanging large quantities of quarters from non-gaming proceeds for paper currency.
- Frequent betting transactions just under thresholds.
- Frequent 'buy in' and 'cash out' transactions just under thresholds.
- Cash deposits / withdrawals just under thresholds.
- Wire transfers / currency exchanges just under thresholds.
- Requests for winnings in separate cash or chip amounts under reporting threshold.
- Cashing in winnings in a multiple combination of chips, cheque and cash.
- Customer conducts several transactions under reporting thresholds over several shift changes.
- Customer moving from table to table or room to room before the wagering amounts reach the reporting threshold.
- Opening a casino account or purchasing casino chips with small denominations bills.
- Customer gambling with large amounts of small denomination bills.
- Currency exchange from small denomination bills to larger denomination bills.
- Frequent 'cash out' transactions without corresponding 'buy in' transactions or vice versa.
- Customer due diligence challenges, e.g. refusal, false documents, one-off/tourist or passing trade.
- Dramatic or rapid increase in frequency of currency transactions for regular account holders.
- Noticeable spending/betting pattern changes.

- Insert banknotes in electronic gaming devices with no gaming activity, press the "cash out" button which generates a TITO ticket, and redeem ticket at cashier's desk or ticket redemption kiosk machine.

Casino accounts & facilities

Credit accounts / Markers / Foreign holding accounts / safe deposit boxes

119. Casino accounts provide criminals further opportunities to attempt to laundering crime proceeds. Many casinos offer deposit accounts and lines of credit with less scrutiny and CDD requirements than financial institutions. The frequent movement of funds between financial institutions and casinos, or between casino accounts held in different casinos may be vulnerable for money laundering. Many casinos offer private safe deposit boxes, particularly to VIP/'high roller' customers.

120. ***Cashing cheques into casino accounts*** – Some casinos allow customers to cash various types of cheques and use the proceeds for gambling. Cheques could be signed over to the bearer by the cheque recipient. In the cases studied, proceeds from illegal activity were initially used to draw these cheques with the aim of avoiding the casino's suspicion.

121. ***Deposits into casino accounts by wire transfers or bank cashier's cheque*** – funds are deposited by wire transfer of bank cheque, then cashed out or moved to other accounts with minimal or no gambling activity.

122. Cashed out funds are stored in casino safety deposit boxes or held in the form of safekeeping markers and then cashed out.

123. ***Foreign Holding Accounts (FHAs)*** – Accounts that are held in one jurisdiction by the casino, but the funds can be used to gamble in another jurisdiction under the same casino group. For example, funds held in a FHA account in Macao, China can be used to gamble at a casino in Las Vegas. The money held in the account does not physically leave the country and is not subject to cash declarations. Large casinos may operate marketing offices in jurisdictions other than where the casino is located. Patrons are able to pay in funds to their casino account to be played when they travel to the casino without sending a cross-border wire transfer. *See the Junkets section for further details*.

124. ***Wire transfers from Casas de Cambio to casino accounts*** – Casas de Cambio in another jurisdiction may wire transfer funds to casinos. As an example, in the United States Casas de Cambio businesses are concentrated along the southwest border, with over 1 000 located along the border from California to Texas. These businesses are generally unregistered and do not comply with AML reporting requirements, and are suspected of being a significant money laundering risk. These *Casas de Cambio* have corresponding bank accounts which allow them wire transfer of large amounts of cash to casinos and other institutions throughout the world.

125. ***Safety deposit boxes*** – A number of casinos offer safety deposit boxes to patrons, in particular to 'high roller' patrons in VIP rooms. These present a risk due to the lack of transparency with the use of such boxes and the possibility for 3rd parties to be given access to safety deposit boxes via a password or key, to facilitate financial transactions. Very few jurisdictions regulate the safety deposit boxes in casinos.

Case 11. Large money laundering conspiracy

Offence:	Money laundering, VAT fraud, counterfeiting, credit card fraud, drug trafficking
Jurisdiction:	United Kingdom, Dubai
Technique:	Use of casino accounts, placement via gambling
Mechanism:	Bank, casino
Instrument:	Cash

The money laundering conspiracy involved millions of UK pounds from organised criminal gangs being laundered by a group of men from West Midlands. The money laundered included the profits from a number of activities including drug trafficking, multi-million pound VAT conspiracies in the mobile phone industry, counterfeiting and credit card fraud. The monies were a mixture of Scottish and English notes. The defendants would transfer large amounts of money to a back account in Dubai, which would then be accessed by their associates. The defendants received the proceeds of crime in the UK and made equivalent amounts of criminal monies available in Dubai. They then utilised the gambling industry to launder the money. Money was placed on a deposit at a casino and withdrawn a day or so later. Other sums would be gambled. Thousands of pounds would be passed over the tables in order to disguise the original source of the banknotes. Monies gambled or exchanged at the casino provided the defendants with an apparently legitimate explanation as to their source.

Case 12. Bank employee gambles millions from clients' accounts

Offence:	Fraud, money laundering
Jurisdiction:	Australia
Technique:	Use of casino accounts, structuring
Mechanism:	Bank, casino
Instrument:	Bank cheques

An investigation into a bank employee who gambled millions of dollars from clients' accounts was initiated as a direct result of information submitted by the casino. The suspect used his knowledge of the bank's internal procedures to discreetly transfer funds from customer accounts to his own personal account. Over a period of time, these funds were deposited into his casino account in the form of bank cheques made out in his name. The casino reported the regular deposit of bank cheques. The same casino had also previously reported bets placed by the suspect of AUD 9 000 to avoid the AUD 10 000 reporting threshold. As a result of the investigation the suspect was charged with three counts of money laundering and 37 counts of fraud.

Case 13. Avoiding liquidation action

Offence:	Money laundering
Jurisdiction:	Australia
Technique:	Placement via gambling
Mechanism:	Casino
Instrument:	Cash

A person was a director of a company that was subject to liquidation. Contrary to liquidator's instructions, the person began transferring large amounts of cash between company accounts and depositing the money into a casino account. The funds were used to gamble at the casino and subsequent "winnings" taken as cash.

Case 14. Cigarette Fraud

Offence:	Money laundering, bank fraud, wire fraud, conspiracy
Jurisdiction:	United States
Technique:	Use of third parties and casino accounts to facilitate fraud
Mechanism:	Casino
Instrument:	Cash, Casino Cheques

A suspect in New York lured foreign buyers into ordering large quantities of cigarettes. Suspect did not have cigarettes and had no intention of providing them to the buyers. The casino was used to launder the funds from the fraud as below:

- Buyer 1 paid USD 100 000 up front in a casino cashier's cheque. Suspect had accomplice deposit the cheque at the casino. Accomplice was permitted to gamble with USD 10 000 and cash out remainder and give to suspect.
- Buyer 2 provided a USD 60 000 certified cheque up front. Accomplice deposited the cheque at the same casino and was permitted to gamble, but lost USD 50 000 and gave remaining USD 10 000 in cash to

defendant. Buyer 2 sent another USD 100 000 certified cheque.

- Buyer 3 deposited USD 600 000 cheque into an account against which a cheque in the amount of USD 180 000 was made payable to the same casino. Accomplice then tried to withdraw all of the money, but the casino refused and permitted only a USD 50 000 withdraw. Accomplice then gambled with some funds and won USD 15 000. Casino then permitted withdrawal of funds and allowed accomplice to cash out.

Case 15. Loan-sharking profits laundered at casino

Offence:	Money laundering
Jurisdiction:	Japan, United States
Technique:	Purchase and cash out with little or no gaming activity
Mechanism:	Casino
Instrument:	Cash, casino chips, casino credit

A boss of a loan-shark business ordered his associates to convert the profits from Yen into US currency using false names. These funds were then distributed to numerous bank accounts around the world. Some of the money was also invested with a foreign agent of a Las Vegas casino, who kept the money in a safety deposit box in the head office of a major Tokyo bank. Against the security of this money, the boss played frequently at Las Vegas casinos as a VIP player. Although he gambled in the VIP room, he would never place big bets and, after minimal play, would frequently cash in his chips for US currency. His associated were also circulated through a number of Las Vegas casinos cashing in chips worth USD 2 000 or less.

Indicators of ML using casino accounts:

- Frequent deposits of cash, cheques, bank cheques, wire transfers into casino account.
- Funds withdrawn from account shortly after being deposited.
- Significant account activity within a short period of time.
- Account activity with little or no gambling activity.
- Casino account transactions conducted by persons other than the account holder.
- Funds credited into account from country of concern.
- Large amounts of cash deposited from unexplained sources.
- Associations with multiple accounts under multiple names.
- Transfer of funds from/to a foreign casino/bank account.
- Transfer of funds into third party accounts.
- Funds transferred from casino account to a charity fund.
- Multiple individuals transferring funds to a single beneficiary.
- Structuring of deposits / withdrawals or wire transfers.
- Using third parties to undertake wire transfers and structuring of deposits.
- Use of an intermediary to make large cash deposits.

- Use of gatekeepers, e.g. accountants and lawyers to undertake transactions.
- Use of multiple names to conduct similar activity.
- Use of casino account as a savings account.
- Activity is inconsistent with the customer's profile.
- Unexplained income inconsistent with financial situation.
- Transfers with no apparent business or lawful purpose.
- Transfer of company accounts to casino accounts.
- Use of false and stolen identities to open and operate casino accounts.
- Customer name and name of account do not match.
- U-turn transactions occurring with funds being transferred out of country and then portions of those funds being returned.
- Customer due diligence challenges, *e.g.* refusal, false documents, one-off/tourist or passing trade.
- Requests for casino accounts from Politically Exposed Persons (PEPs).

Winnings

126. ***Use of illicit funds to gamble*** – this is the simplest method of gambling illicit funds in the home hopes of generating certifiable winnings. One way to do this is to play gaming machines or other games with low payout higher win/loss ratios. The money launderer will then receive a casino cheque for the total amount of credits remaining on the machine plus the jackpot.

127. Some jurisdictions require casinos to endorse the casino cheques from jackpots as 'winnings' in order to differentiate it from a cheque generated as a result of cashing out large amounts of machine credits.

128. ***Buying winnings from legitimate customers*** - is another method used across the gaming sector. Money launderers will approach customers and offer them cash at a premium above their winnings. This was evident with customers who had won gaming machine jackpots, or accumulated a large amount in casino chips from winnings on table games, or customers that had won in other forms of betting offered by some casinos, such as electronic lotteries, horse racing and sports betting.

129. ***Parallel Even money betting*** – In cases where gambling is undertaken to launder funds, it is usually on low odds, low risk games such as the even money options on roulette. This would involve two or more persons placing opposite equivalent bets on even money wagers in the same game. As an example Person A places USD 1 400 on red, while Person B places USD 1 400 on black in a game of roulette. The bet is 'double or nothing'. In this case the winning party would win just under USD 3 000 which could be paid out with a 'winnings' cheque and the size of the win would not trigger CDD requirements at the roulette table.

130. ***Betting against associates / intentional losses*** – This is also the case in games where which provide money launderers the option to bet against an associate so that in most cases one party will win. These 'intentional losses' where money launderers are intentionally losing to one of the party, who is able to receive a casino issued cheque or wire transfer of 'legitimate' winnings.

Case 16. Overseas nationals purchase winning jackpots with illegal proceeds

Offence:	Drug trafficking & money laundering
Jurisdiction:	Spain
Technique:	Buying winning lottery tickets
Mechanism:	Lotteries
Instrument:	Winning jackpots, cash

Investigations in Spain related, mainly with drug trafficking, corruption and tax fraud identified the use of gaming to launder funds. The technique consisted of buying winning lottery tickets from legitimate gamblers.

Case 17. Overseas nationals purchase winning jackpots with illegal proceeds

Offence:	Money Laundering
Jurisdiction:	Australia
Technique:	Buying winning jackpots
Mechanism:	Gambling clubs
Instrument:	Winning jackpots, casino cheques

A group of overseas nationals were identified buying winning jackpots from other persons at various clubs in Sydney, Australia. The suspects deposited approximately AUD 1.7 million in winning cheques within a year, immediately withdrawing money in cash afterwards. The source of the funds used to buy winning jackpots was suspected to be from illegal means.

Indicators of ML using winnings:

- Frequent claims for winning jackpots.
- Frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash.
- Customers watching/hanging around jackpots sites but not participating in gambling.
- Multiple chip cash outs on the same day.
- Customers claiming gaming machine credits/payouts with no jackpot.
- Customers claiming a high level of gaming machine payouts.
- Purchasing and cashing out casino chips with no gaming activity.
- Requests for winnings in separate cash or chip amounts under reporting threshold.
- Frequent 'cash out' transactions without corresponding 'buy in' transactions.
- Cashing in winnings in a multiple combination of chips, cheque and cash.

Currency exchange

131. Given the popularity of casino-based tourism and the willingness of customers to travel to legal casino sectors, most casinos offer currency exchange services.

132. ***Conversion of large sums of foreign currency*** – launderers may use large, one-off, or frequent foreign currency exchanges or deposits of a foreign currency. This may not appear suspicious in jurisdictions with high numbers of foreign players.

133. Reported cases indicate that criminals involved in the distribution and supply illegal drugs are using casino currency exchange services to convert their criminal proceeds from one currency to another, in order to alter its original form.

134. Individuals and groups will also employ structuring methods to undertake currency exchanges without triggering threshold reports. They will use multiple casino locations and once the currencies are exchanged, will meet again to assemble the total amount.

135. ***Casino play is undertaken in foreign currency*** – in some poorly regulated jurisdiction, customers are able to purchase chips directly in a foreign currency (for example in Nepal with USD and Indian Rupees).

Case 18. Overseas nationals purchase winning jackpots with illegal proceeds

Offence:	Money Laundering
Jurisdiction:	Spain
Technique:	Currency conversion
Mechanism:	Casino
Instrument:	Cash – various currencies

A group of foreign people entered separately in a casino to buy casino chips using Swiss Francs (CHF). The purpose of the syndicate was not to play in the casino, but to redeem the chips in Euros. The casino detected the operations, stopped the transactions and filed an STR.

Indicators of ML using currency exchange:

- Bank drafts/cheques cashed in for foreign currency, *e.g.* Euros, USD.
- Multiple currency exchanges.
- Dramatic or rapid increases in size and frequency of currency exchange transactions for regular account holders.
- Currency exchange for no reasonable purpose.
- Currency exchanges with low denomination bills for high denomination bills.
- Currency exchanges carried out by third parties.
- Large, one-off, or frequent currency exchanges for customers not known to the casino.
- Requests for casino cheques from foreign currency.
- Currency exchanges with little or no gambling activity.

- Structured currency exchanges.

Employee complicity

136. Employee complicity is another method in which third parties are used to facilitate money laundering. Individual employees or organised groups comprising of staff from different departments conspire with customers to enable money laundering transactions to go undetected. Methods include:

- Failing to file suspicious transaction reports or threshold transaction reports.
- Destroying documents/transactions reports related to due diligence or reporting processes.
- Falsifying player ratings and other gambling records to justify the accumulation of casino chips/gaming machine credits.

137. Some jurisdictions have raised vulnerabilities from providers of gaming equipment and machines as well as contractors that supply goods with a potential to impact on the integrity of the operation. Major contracts can be an avenue for criminal exploitation of the operation (*e.g.* through corrupt purchasing and under supply of contract goods). Criminals will try to exploit gaming equipment and associated computer systems to achieve theft and money laundering in the casino.

Case 19. Suspected falsified player ratings

Offence:	Money laundering
Jurisdiction:	Australia
Technique:	Falsifying player ratings to legitimise criminal proceeds
Mechanism:	Casino
Instrument:	Cash

An ex-employee of one casino was investigated by Australian authorities after he was able to purchase a house for cash. The family of this person is alleged to be involved in illegal drug activity and it was suspected that the funds used to purchase the house were provided by his family. The person, however, was able to show 'player ratings' from a second casino to show how he had turned NZD 20 000 into over NZD 400 000 in two weeks. It is suspected that an accomplice at the second casino falsified these 'player ratings', but this was not able to be proven.

Case 20. Back door corruption

Offence:	Money laundering
Jurisdiction:	United States (Indian casino)
Technique:	Casino staff bribed to facilitate money laundering
Mechanism:	Casino
Instrument:	Cash, jackpots

In Florida drug proceeds were laundered through gaming machines. Some gaming machines are controlled by software that have certain override features, or 'back doors' that give key casino staff the ability to force jackpot payouts. In Florida drug dealers bribed casino staff who accessed the override features and rigged a number of machines for the drug dealers to play and win jackpots from their drug proceeds.

Indicators of employee complicity:

- Contact between patrons and casino staff outside of the casino.
- Supposed winnings do not correspond with recorded winnings.

- Dramatic or rapid increases in size and frequency of currency transactions for regular account holders.
- Large sums of cash from unexplained sources.
- Large sums credited into accounts from other jurisdictions or countries of concern.[20]
- Associations with multiple accounts under multiple names.
- Transactions on casino accounts conducted by persons other than the account holder.
- Deposits into casino account using multiple methods.
- Cheques issued to a family member of the person.
- Multiple individuals sending funds to a single beneficiary.
- Third party presents for all transactions but does not participate in the actual transaction.
- Transferring funds into third party accounts.
- Use or third parties to undertake wire transfers.
- Use of an intermediary to make large cash deposits.
- Use of gatekeepers, *e.g.* accountants and lawyers to undertake transactions
- U-turn transactions occurring with funds being transferred out of a country and then portions of those funds being returned.
- Use of remittance agents to move funds across borders.
- Use of third parties to purchase gaming chips.
- Use of third party to conduct wagering.
- Wire transfers from third parties in tax haven countries.
- Junket tours where funds can be concealed amongst the pool for the group.
- Cash handed to third party after cash out.

Credit cards / debit cards

138. ***Laundering proceeds from stolen credit cards*** – Casinos in some jurisdictions allow customers to purchase casino chips using credit cards. In cases where the cards are not stolen or fraudulently obtained, the outstanding credit card balances are paid by the card holder at the bank using the illicit funds.

20. TBD.

139. ***Credit cards*** – criminals use of credit cards provides an opportunity for authorities to follow the money trail more readily.

Case 21. Debit card scheme

Offence:	Fraud, money laundering
Jurisdiction:	Belgium
Technique:	Use of credit cards to conduct money laundering transactions
Mechanism:	Casino
Instrument:	Credit cards, casino chips.

A person residing in Belgium, originally from Eastern Europe, visited a casino on the Belgian coast on two occasions and bought gaming chips for a total value of EUR 400 000 paid for in cash and with credit cards. The casino reported these transactions to the FIU.

Based on the history of gambler's purchases using credit cards it was determined that his account had been extremely active: it had been inundated with various transfers from companies and, in particular, with many cash deposits. The spouse of the party concerned ran a business in Belgium and maintained underworld links with organised crime from Central and Eastern Europe. The party concerned received citizens from those countries at his personal address and that financial transactions were carried out in cash. The gambler was in frequent contact with a person who was being investigated for the laundering of money deriving from organised crime.

140. ***Debit cards*** – are another value instrument used to conduct fraud and money laundering crimes. In the case below, criminals would join a casino and use their debit card to draw up to the casino's maximum standard daily limit and purchase casino chips. The subjects either do not put any funds at risk or there would be minimal play. The subjects would then typically cash out. In similar cases, plaques would be passed to an associate for play. Sometimes all the funds would be put at risk. The major operators quickly identified this trend and put risk control mechanisms in place to limit the initial debit card transaction to a much lower limit for first time transactions in high risk situations.

Case 22. Debit card scheme

Offence:	Fraud, money laundering
Jurisdiction:	United Kingdom
Technique:	Use of debit cards to conduct money laundering transactions
Mechanism:	Casino
Instrument:	Casino plaques

An existing member of a casino introduced a number of people over a period of time. Suspicious was raised as the new members were completing debit card transactions to the maximum limit and receiving gaming plaques in exchange, which in turn were passed to the existing member. Most of the new members never returned to the casino after the initial visit. The nationalities of the new members varied widely, but all are believed to have recently arrived from foreign jurisdictions. The transactions varied from GBP 1 000 to 7 000. Some money was put at risk and lost by the existing main member.

Indicators of ML using credit/debit cards:

- Purchasing casino chips using credit card.
- Purchasing casino chips using debit card.
- Purchasing and cashing out casino chips/plaques with no gaming activity.
- Customer purchases chips and leaves casino shortly after.
- Use of stolen or fraudulently obtained credit card.

- Use of multiple credit/debit cards to purchase casino chips.
- Use of third parties to purchase chips using credit/debit card.
- Structuring of credit card transactions.
- Conducting debit card transactions up to the maximum limit.
- Chip cash out is same/similar to chip purchase.
- Customer due diligence challenges, *e.g.* refusals, false documents, one-offs, tourists passing trade.

False documents

141. As with financial institutions, money launderers use false documentation to disguise the origin of criminal proceeds and to protect the identity of those laundering the proceeds.

142. ***False identification documents*** – often used to conduct financial transactions at the casino, open casino accounts, undertake gambling transactions and redeem winnings.

Case 23. Money launderer uses third parties and false identities to launder drug proceeds

Offence:	Money laundering, identity fraud
Jurisdiction:	United States
Technique:	Use of 3rd parties and false identities to structure gambling transactions
Mechanism:	Casino
Instrument:	Cash, casino chips

A Person of Interest (POI) of a drug trafficking organisation, utilising both the money he was paid for his services and the large sums of money put into his possession to be laundered, elevated his previously modest gambling practices to that of a high-roller. The person would recruit third parties at the casino to purchase, or cash in, chips for him, paying them a nominal fee to do so. After gambling, he would cash some of these third-party purchased chips back out again, claiming they were his gambling winnings. According to the CTRs a USD 313 000 discrepancy was found to exist between chip purchases and cash out. Twenty-four of the CTRCs recording his activities revealed the use of aliases and multiple social security numbers. On numerous other CTRCs he had refused to provide a social security number.

Indicators of ML using false documents and counterfeit currency:

- Associations with multiple accounts under multiple names.
- Purchasing chips or undertaking cash transaction and immediately leaves casino.
- Transferring funds into third party accounts.
- Use of multiple names to conduct similar activity.
- Use of altered/fraudulent or stolen identification to conceal identity.
- Customer due diligence challenges, *e.g.* refusal, false documents, one-off/tourist or passing trade.

- Inconsistent identity information presented.
- Refusal to provide identification / false identification or Social Security numbers.
- Using false or multiple Social Security numbers.
- Refusing to provide required identification.

CHAPTER 3 – SECTOR VULNERABILITIES AND EMERGING ISSUES

Introduction

143. This chapter identifies some of the sector vulnerabilities and emerging issues within the global casino sector, as reported by members of the FATF, APG and other FATF-style regional bodies (FSRBs).

Casino-based Tourism – "Junkets"

144. Casino junkets or casino-based gaming tours are derived from casino marketing programs. A junket is an organised gaming tour for people who travel to the casino primarily to gamble. The junket may include transport, accommodation, incentives to play at the casino and the movement of funds to and from the casino.

145. Casino junkets may be part of the casino's in-house marketing operation or may be run by independent operators who have a contract with the casino. In jurisdictions where the role of junkets is limited, they may still operate in travel agent roles with an added service of moving funds to the jurisdiction. In such cases, junkets may have no direct connection to the casino, but just bring the players and their funds to the front door of the casino. Junket agents are persons or companies who have a role to sign up casino patrons to take part in junkets. Junket representatives work to organise the junket.

146. In house marketing by casinos may include representative offices of the casino being located in foreign jurisdictions in order to organise junket gaming tours to the casino jurisdiction.

147. Junkets appear to be common in casino jurisdictions in the Americas, Caribbean and Asia, but are less common in European casinos. The extent of junket operations in casinos in Africa, the Middle East and Central Asia is unclear.

Regional junket patterns

148. A number of casino sectors in the Asia/Pacific region have a sizable junket industry to attract gambling tourists to their sector. As at 28 January 2009 Macao, China has 153 licensed junket operators, made up of 107 companies and 46 individuals. The patterns of casino-based tourism in the Asia Pacific region vary but source jurisdictions include China, India, Hong Kong, Japan, Chinese Taipei, Thailand, Australia, New Zealand and the United States.

149. Junkets do not operate in Canada and it is reported that junkets do not operate in much of Europe, although Malta reported EUR 28 million in revenues from junkets operations in 2006 and Austria reports that there is only small-scale activity in the sector, due to tight regulations applicable to casino customers. While casino-linked junkets are not a feature of some casino sectors in Europe, it is likely that junkets are a relatively recent development for this region and authorities may not yet recognise junket-type operations or the level of risk they present.

Features of Junkets

150. Junket operators provide incentives for patrons to play at a particular casino. As part of this, the junket provider may organise all aspects of a player's tour to the casino, including the movement of funds to be played in the casino. Junkets generally target the high net worth clients. In some jurisdictions, junket operators and their agents have a role in conducting CDD on junket patrons.

151. In house marketing by casinos may include representative offices of the casino being located in foreign jurisdictions in order to organise gaming tours to the casino jurisdiction. In such cases, players can organise all aspects of their visit to the casino, including depositing funds into their casino account. An example is Wynn Resorts, which has casinos in Las Vegas and Macau and has marketing executives located in local offices in, Tokyo, Hong Kong, Singapore, Taipei and Vancouver. Other large-scale casinos operate similar networks of offices.

152. Junket representatives / agents serve as an agent between casino marketing departments and proven premium players. VIP junkets do not tend to be advertised. Region specific junkets often do not deal with the general public, but rely on introductions from intermediaries. Junket representatives / agents rely on commissions or fees to support their business. These commissions vary, but may include:

- A percentage of front money.
- A commission on 'dead chips'.
- A commission on 'live chips'.
- A commission on players' losses.
- A percentage of the casino's theoretical win.

Vulnerabilities

Movement of people and money to casinos

153. A vulnerability of junket programmes is that they involve the movement of large amounts of money across borders and through multiple casinos by third parties. Junket participants generally rely on the junket operators to move their funds to and from the casino. This creates layers of obscurity around the source and ownership of the money and the identities of the players. This is made more difficult if the junket operator is complicit in any money laundering activity by the players, or is solicited by criminals to blend illicit funds with the pool of legitimate funds.

154. Foreign marketing offices/branches of casinos may accept deposits to a patron's casino account before they travel to the casino. The study of casino vulnerabilities could not identify cases where the foreign marketing offices of a casino were subject to local AML/CFT controls, despite their role in taking deposits to player accounts. In such cases there is, in effect, no cross border wire transfer to move the funds to the casino.

Case 24. Criminal control of junket operations

Offence:	money laundering
Jurisdiction:	Australia
Technique:	Use of a junket agent to move funds and purchase chips
Mechanism:	Casino agent

A gambler used gambling contacts and knowledge of high-stakes gambling to become a registered and successful junket operator, bringing millions of dollars of revenue to a casino. All of the money gambled by the junket went through the operator's accounts in order to calculate commission from the group's turnover. This way the casino bypassed the necessity for identifying the source and beneficial owner of the funds. It was not until the junket operator began stealing from her customer's winnings that this situation came to the attention of the authorities.

155. Junket operators may use wire transfers to move funds on behalf of clients. The identity of the junket patrons may be unknown to the sending and receiving financial institution or the receiving casino.

Regulation of Junkets

156. Relatively few casino jurisdictions regulate junkets. While the US has a long history of regulating junkets, as an example Macao, China has only recently taken steps towards clear regulation of junkets and their representatives.

157. In the US, a number of states require registration of junket representatives. As an example, the State Gaming Control Board of Nevada requires a fingerprint check and detailed information including military record and criminal arrests. Macao, China requires licensing and registration as well as fit and proper tests of junket operators, as does Australia. Very few gaming jurisdictions have controls on whether or not junket operators are permitted to extended credit to the players taking part in the junket.

158. In cases where junket operators are strongly regulated, jurisdictions require junket operators to be vetted, licensed and operate according to regulations; some with specific AML/CFT controls that compel junket operators to report suspicious transactions by its players. In addition some legal frameworks place the responsibility for junket activities on the casino operator, with their license at risk if players' funds are found to be unlawful. Strong regimes oblige the casino operators to report any suspicion that a junket promoter may be involved in illegal activity.

159. Some casinos and junket providers operate in a number of jurisdictions and offer services from the same casino group in a number of jurisdictions. It is not clear what obligations are placed on junket operators or casinos when they operate in a number of jurisdictions. In relation to junkets offered by independent operators and by casinos, there are a number of issues with foreign branches or subsidiaries of casinos operating in another jurisdiction to the one where the casino is located.

160. Such issues vary from jurisdiction to jurisdiction, but include the following:

- Over-reliance on junket operators, especially in markets with resident populations that are too small to normally support casinos can pose a heightened money laundering risk. In these instances, casinos can become overly dependent on junket operators for business, a potential misuse of these services.
- In some jurisdictions, a casino may enter into a contractual agreement with a junket operator to rent a private room within a casino and in some situations, it is the junket operator, not the casino, which monitors player activity and issues and collects credit.

- Junket operators that provide premium players may exert commercial pressures on casinos, which may result in reducing scrutiny of individual spending patterns, or unduly influence or exercise control over licensed casino operations.
- Junket operators may engage in lending or the facilitation of lending to players outside casinos' knowledge.
- In some jurisdictions, junket operators are allowed to 'pool' and therefore obscure the spending of individual customers, thus preventing casinos from making any assessment of customers' spending patterns.
- In certain jurisdictions, licensed junket operators act as fronts for junket operators in another country. The front operators supply players to a casino through a casino's licensed junket companies which may not qualify for licensure in the country where the players will be gambling. Such unlicensed sub-junket operators can act as unlicensed collectors of credit and may have ties to organized crime networks.

161. All the above issues pose serious risks, and can lead a casino to engage in informal arrangements with junket operators that are inconsistent with risk-based AML/CFT policies, procedures and internal controls as well as hinder authorities' ability to recognize the level of risk that certain operators pose.

Junkets use of alternative remittance

162. In some jurisdictions junket operators may use formal or informal systems to remit money. The nature of junket business assists them to facilitate informal alternative remittance. The Junket operators may have agents in a number of jurisdictions. Junkets / casino agents may utilise their branch offices in foreign jurisdictions to organise movement of funds to the casino jurisdiction. It is not clear if these agents are responsible to their home jurisdiction for reporting STRs on junket patrons.

Case 25. Cash smuggling and underground remittance

Offence:	Cash smuggling, money laundering
Jurisdiction:	Macao, China
Technique:	Use of an casino agent to move funds and purchase chips, structuring
Mechanism:	Casino, casino agent, remittance arrangements
Instrument:	Cash, cashier's order

A casino agent received large amounts of cash in PR China from a mainland customer who wanted to gamble at a Macao, China casino. The agent took the cash to a shop at Zhuhai, which is adjacent to Macao, China. The shop divided the sum into small lots, which would be carried to Macao, China by many 'professional commuters'. Another agent collected these lots and handed them to the casino agent by depositing the monies into his account in the form of cash, cheque, bank transfer and remittance. When the full sum was received, the casino agent converted it into a cashier's order for receipt by the VIP room of the casino. The VIP room then issued non-negotiable chips to the mainland customer who could start gambling. When the customer won from the table, the gain in cash is given to the casino agent who would remit the funds back to China via underground banks.

Case 26. Use of junket promoter and casino VIP room to move cash between countries

Offence:	Money laundering
Jurisdiction:	Macao, China
Technique:	Use of third parties to move illicit funds
Mechanism:	Casino, junket operators
Instrument:	Cash

A merchant in country A could not perform a large remittance to country B due to its foreign exchange control. With the help of a junket promoter, he transferred the monies to the VIP room of a local casino, which informed

an underground remitter in country B about the amount and beneficiary of the funds. The remitter would then arrange payment of the fund to the beneficiary. For country B citizens who wished to gamble in this casino of country A, but had difficulty in bringing in the cash, they would arrange alternative remittance through this remitter who would then inform details of these customers to the VIP room. When these citizens arrived at the VIP room they could immediately obtain the amount required for gambling. Both the VIP room and the remitter would perform reconciliation for net settlement, and basically no transfer of monies between two sides was required.

Case 27. Junket promoter use of underground banking

Jurisdiction:	South Korea
Technique:	Alternative remittance
Mechanism:	trade-based settlement mechanism

A casino in Las Vegas, 'A' operated a marketing team entirely responsible for Korean customers. This team lent gambling money to Koreans in form of card (coupon) not cash so that the loan would be spent only for the purpose of gambling at 'A'. The members of this team visited Korea to collect debts or made their relatives in Korea do so on behalf of them.

The collected money was paid to trading companies in Korea for the goods that these companies sold to importing companies in the United States. And the importing companies paid the amount to 'A'.

Junket incentives – 'Dead chips'

163. Casinos in some regions offer junket agents a commission on non-negotiable, or "dead", chips. The use of dead chips requires the junket operator to account for their use. These 'dead chips' cannot be redeemed for cash from the casino, but are only negotiable with the junket promoter. In general, dead chips can be wagered only in the game of baccarat.

164. Players purchase large amounts of these chips from the junket operator at a discounted price based on an operator's terms. They cannot redeem the chips for cash or for live chips but must play the chips until they lose them or win replacement live chips. The live chips can be redeemed for cash with the casino. At the conclusion of gambling, 'dead chips' can be redeemed with the junket operator. A junket operator requires players periodically to roll their "live chips" into "non-negotiable" dead chips so that an operator can receive a commission from a casino based on the total value of the dead chips. Because 'dead chips' are offered at a premium to junket patrons, there is an incentive for players to purchase additional 'dead' chips and players receive live chips in exchange as well rebates equal to the product of the agreed-upon rebate percentage and total dead chips purchased.

165. ***'Dead chips' being used by criminals as currency*** – jurisdictions report 'dead chips' being used in drug deals and to settle other criminal transactions.

166. ***'Dead chips' being smuggled out of a jurisdiction*** – such chips are a safe way for criminals to move value as they are difficult for customs agencies to detect in cross border movements.

Case 28. 'Dead chips' associated with loan sharks

Offence:	money laundering, criminal coercion
Jurisdiction:	Hong Kong; China; Macao, China
Technique:	Use of 'dead chips'
Mechanism:	Junket 'dead' chips

Dealing in junket chips (colloquially known as 'mud-chips') is closely connected to other forms of criminality, and it is particularly ripe for exploitation by loan sharks often with a triad element, who are attracted by lucrative profits and the ease of finding potential borrowers amongst gamblers, with loans being offered in the form of 'mud-chips'.

In Hong Kong, China for example, stooge or nominee corporate accounts are often used for settlement purposes

by loan shark syndicates operating offshore. A common scenario involves victims being induced to gamble more than they can afford in the VIP rooms at offshore casinos by mud-chip (*dead chip*) syndicates, which often work with loan sharks. The victims are then escorted back to Hong Kong, China and held pending settlement. Family members are induced to make settlement by bank transfers, which are structured through a series of stooge accounts.

Case 29. Diversion of illicit funds to casino agents and junket operators

Offence:	Fraud, money laundering
Jurisdiction:	Hong Kong, China, China, United States
Technique:	Use of third parties to move illicit funds
Mechanism:	Casino agents, junket operators
Instrument:	Cash

In 2006, three provincial managers of a bank in another jurisdiction were indicted for embezzling in excess of USD 3.5 billion that was subsequently channelled through shell companies and personal and investment accounts in Hong Kong, China with the help of associates and intermediaries. Approximately HKD500 million was deposited with the representative agents and junket promoters of various South East Asian and North American casinos for the groups' personal use.

167. Indicators of money laundering through junket operations include:

- Players refusing to provide identification.
- Use of representatives/third parties to conduct cash buy-in.
- Junket chips redeemed without any gambling activity.
- Source of funds for buy-in not disclosed.
- Source of funds for buy-in from companies.
- Buy-in of junket chips by a person whose occupation is not commensurate with the buy-in value.
- Junket issuing cheques to rival casinos.
- Junket transferring funds to players with no verifiable proof of winnings.
- Player frequently requesting cheques from junket operator below threshold amounts.

Emerging Issue – Cruise Ship junkets

168. A growing number of independent casino junket representatives now offer junkets to cruise ships. These escorted cruise casino junkets tend to be on ships of the same lines and the packages offered by independent operators range from cruises that are entirely complimentary (with the exception of port charges and taxes) to packages offering reduced player rates. In most cases, players deposit a significant amount of money up front with the independent junket operator. Once aboard, the player can then draw this money for gambling in the cruise ship casino. Very few jurisdictions regulate junket operations linked to cruise ship gaming.

VIP Rooms and 'High-Roller' Customers

169. VIP customers or 'high rollers' are highly valued casino customers who gamble in private and exclusive rooms within the casino complex and are afforded special treatment by the casino. VIP rooms are closely tied to the junket business, and, like junkets, the vulnerability is with identifying the high rollers, and being able to know where their money is coming from and going to. A concern shared by many jurisdictions is that casino staff view very high cash use or large deposits and withdrawals by VIPs, and especially within VIP rooms, as 'normal'. In addition casinos offer VIP customers financial facilities akin to any banking institution, yet many jurisdictions do not have the level of AML controls over casinos as they do their banking industry. If there are no requirements to conduct CDD on VIPs, particularly those associated to junkets, and/or regulators and law enforcement cannot access membership information on operations and if required the money trail associated with their gambling, it poses a serious risk.

170. VIP customers represent high revenue streams for most casinos. A Canadian study in 2007 showed VIP customers are responsible for 80% of casino turnover in Canada, but only represented 1% of casino patrons. Macao, China also reports 50-70% of all casino revenue comes from VIP rooms.

171. In the past, under Macao, China's old monopoly system the VIP rooms catered to clients seeking anonymity and were shielded from official scrutiny. With the changes to the gaming industry in 2002 and passing of new AML/CFT laws in 2006, the casino industry has been placed under the AML/CFT regime with casinos (including gaming intermediaries and junket operators) having obligations to report STRs to the FIU in the main areas and VIP rooms – and with respect to all customers. Macao, China reports that supervisors and casinos are aware of the risk that VIP rooms could be associated with crimes, and have been tightening the control of junket activities. At the same time, all casinos do not cede control of their VIP gaming facilities to outside organisations, which impedes organised crime's ability to operate in the casino sector.

172. The following two cases illustrate the risks presented by VIP players:

- In Australia a high profile Asian organised crime figure became a member of the high rollers club at an Australian casino. The person was running a heroin trafficking network from suites in the casino's hotel and using his gambling activities to mask the illicit profits. He was a VIP player with an extremely high turnover. Over a two-year period he was given gambling incentives by the casino of more than AUD 2.5 million dollars and spent two years as a non-paying guest of the casino's hotel. It was not until he was investigated by law enforcement agency that the casino looked more closely at his gambling transactions.

- In the United States a foreign national travelled frequently to Las Vegas to gamble. He was well-known to a Las Vegas casino and had a gambling loss of approximately USD 1 million over a four year period. Over a subsequent three year period his losses increased to more than USD 125 million. On his behalf the casino conducted wire transfers and direct bank to bank transfers from corporate accounts. The casino on occasion would extend him USD 10 million line of credit and frequently offered him extravagant perks including use of hotel suites, cars, and the casino jet. There were no SARs filed by the casino and no verification of his source of funds was undertaken. Yet open source documents show the company owned by the person could not have generated income sufficient to sustain his gambling losses.

Corrupt or Inadequately Trained Staff

173. Effective AML/CFT controls require casinos (and support industries) to be free from corruption and influence and casino employees to be adequately trained to prevent and detect money laundering activity. However, high staff turnover is characteristic of many casino sectors, particularly in the regions that are poorly regulated for AML/CFT, AML training and experience being lost from the sector as a result. And the potential for corruption in a cash intensive industry, characterised by high employee turnover, is ever-present. Reported cases demonstrate that casino employees, either individually or acting in concert with others, intentionally do not file suspicious/threshold reports, destroy records and falsify documents to disguise money laundering activities. However, inadequate systems and poor employee training also account for large-scale money laundering in the casino sectors.

- In 2007 a number of casino employees were charged for their role in running an illegal gambling ring out of a casino, taking in USD 22 million in sports betting. The casino employees included poker room supervisors, dealers, and a bartender and their roles mostly involved not filing suspicious reports on transactions.

- A Las Vegas compliance officer was charged with failure to file approximately 15 000 CTRCs between 2001 and 2003. He stated that he did not file the reports because he was having personal problems, was behind in his work, and the importance of filing CTRCs was never explained to him.

- In 2006 a drug dealer admitted to distributing approximately 100 pounds of crystal methamphetamine between Las Vegas and Hawaii. In court, he admitted to gambling millions of dollars in cash through Las Vegas Casinos, mostly carried in to the casino in duffle bags. Law enforcement authorities were never notified of this activity.

- USD 207 million in cash was found in a home in Mexico. It is believed to be the proceeds of a drug kingpin who reportedly lost between USD80 – 120 million at Las Vegas Casinos. However, law enforcement authorities were unaware of this person until the cash seizure.

174. Most well-regulated jurisdictions require casino operators to certify an employee's competence to perform the functions authorised by their employment license. This can include reporting of suspicious and significant transactions to the FIU and reporting of illegal and undesirable activity by patrons. Some jurisdictions require regulators to approve the content of training courses run by the casino operator. Yet inadequate employee training, as demonstrated by the cases above, is a significant vulnerability within the casino sector, regardless it seems of the level of regulation imposed.

New Casino Markets

175. As discussed in Chapter 1, new and emerging casino markets are vulnerable to money laundering activities, particularly in the Asia/Pacific and African regions where casino sectors are being rapidly established in developing countries. Many of these jurisdictions have predominantly cash-based economies, poor governance and weak or limited AML/CFT capability. Often the growth of the casino industry will outpace the country's ability to put in place sufficient AML controls, as well as regulatory and enforcement capacity, leaving the sector vulnerable to corruption and money laundering by organised crime groups.

176. Macao, China is another area of vulnerability due to rapid market growth. Revenues in Macao, China started to surge in 2004 when new casinos opened after the 2002 decision to end the 40 year monopoly by the STDM. Now the majority of Macao, China's economy is linked to the casino industry. In less than 6 years, Macao, China has become the biggest casino market in the world. Prior to regulatory reforms in 2002, Macao, China's casino industry was under-regulated, despite the presence of high cash transactions and lucrative junket and VIP room contracts. Since 2002, Macao, China has sought to reform its legal regulatory framework for AML/CFT in the casino sector, however, like many jurisdictions, effective implementation of FATF standards remains a challenge.

177. Like all jurisdictions, Macao, China continues to face threats from organised crime. Whilst AML/CFT implementation in the casino sector is occurring, the scale and speed of growth experienced in the market may result in even greater vulnerabilities for ML.

178. The United States has noted that the rapid growth of new casino markets can provide money laundering opportunities. A US threat assessment in 2005 considered the most notable development in this field is the striking growth of Native American casinos, which have enjoyed double-digit revenue growth for the last ten years, collectively taking in USD 25.7 billion in revenue in 2006, more than twice the amount generated by Nevada casinos.[21]

179. A challenge to establishing effective AML/CFT controls for tribal casinos is coordinating the various regulatory bodies. Tribal gaming is regulated on three levels:

a) Indian Nations (Tribal Government – Gaming Regulatory Commissions).

b) State Gaming Agencies.

c) The National Indian Gaming Commission and federal government agencies, including the U.S. Justice Department, the U.S. Treasury Department and the Department of the Interior.

180. The growth of the Indian gaming market, coupled with overlapping regulatory jurisdictions and limited enforcement resources, has generated concern over the potential for large-scale criminal activity in the Indian gaming industry.

High Seas Gambling

181. High seas gambling (also called boat gambling or floating casinos) involves gaming vessels that travel to international waters to conduct gaming/casino activities. These may be long-distance cruises that have gaming/casinos as side entertainment, or short distance trips that are directed solely at gaming.

182. The phenomenon of gambling in international waters is an issue for all countries with cruise ships registered or operating within their jurisdiction. While many countries prohibit casinos on ships from operating in territorial waters, cruise ship gambling in international waters is not well regulated.

183. Few jurisdictions have regulatory oversight over cruise ship casinos registered to their jurisdiction and fewer have AML/CFT controls over cruise ship casinos. Since cruise ship casinos, with only minor exceptions, are allowed to operate only when in international waters the casinos are largely unregulated. Some steps have been taken within the cruise line sector to self regulate (see

---

21 Associated Press., "Tribal casino revenue up 5 percent nationwide", June 19 2008, http://blog.mlive.com/kzgazette/2008/06/tribal_casino_revenue_up_5_per.html

guidelines published in 1999 by the International Council of Cruise Lines (ICCL).)[22] It is unknown what general record-keeping or due diligence processes, if any, are carried out by cruise lines or if they report suspicious activities to appropriate authorities.

184. Little is known about the level of risk presented by gambling that is undertaken in international waters. For example, it is unknown what methods are used to transfer funds to and from the cruise ship and any associated money laundering risks.

185. Regulatory control over 'High seas gambling' raises complex questions of international law. If AML/CFT laws were to apply, which jurisdictions would have oversight; the jurisdiction from which the ship is operating from, or the jurisdiction where the vessel is registered?

186. Some jurisdictions impose tax and AML regulations on cruise ship lines, such as the United States. Ships registered in the US are subject to income tax and money laundering legislations, meaning that US citizens and permanent residents must declare any income from cruise-ship gambling with Customs on returning to the US and through yearly tax returns. The cruise line is also required to file tax notices for jackpots of over USD 1200However, there is some question as to whether all US registered ships comply with these requirements, and it is unknown the nature or level of oversight by US authorities.

187. High seas gambling is an issue for many jurisdictions, for example Hong Kong, China, where a number of cruise ships or large luxury vessels, operate from their harbours, with the sole or primary purpose of providing casino gaming in international waters. These vessels sail under foreign flags, so port jurisdictions have difficulty in imposing AML/CFT controls on these "foreign" vessels due to the limitation of extra-territorial jurisdiction.

Case 30. High Seas casinos used to launder proceeds of fraud

Offence:	Money laundering
Jurisdiction:	Hong Kong, China; Australia
Mechanism:	High-seas casino; bank accounts,
Instrument:	Casino

In 2005 five Australian citizens defrauded a superannuation scheme of AUD 150 million. Two of the five men flew to Hong Kong, China and boarded a cruise ship, drawing on the illicit funds while gambling at the ship's casino. After losing approximately AUD 3 million, they cashed in their casino chips and had the remaining funds sent to their personal accounts in Hong Kong, China.

188. The case above highlights how 'high seas gambling' poses a money laundering risk to port jurisdictions. The lack of supervision of casinos operating in international waters leaves port jurisdictions exposed to casino-related money laundering risks.

189. It should be noted that the FATF and a number of FSRBs, including the APG, consider AML/CFT controls on cruise ship casinos in the context of a country's ME evaluation if this activity presents a risk of money laundering.

190. Jurisdictions have raised the challenges faced by the issue of extra-territorial jurisdiction over gambling activities beyond flag-flying vessels, as per the current status of international law. There appears to be a need for further consideration of the issue and possible multilateral solutions.

22 Further information can be found at http://www.cruising.org/industry/tech-intro.cfm

Terrorist Financing

191. Throughout this report, the term money laundering has also referred to terrorist financing. It should be pointed out that the research undertaken failed to find any reported cases of terrorist financing in the casino sector. This may be due to the characteristics of terrorist financing that make it difficult to detect, characteristics such as the relatively low value of transactions involved in terrorist financing, or the fact that funds can be derived from legitimate as well as illicit sources.

192. It would be a mistake, however, to assume that terrorist financing has not and could not occur in the casino sector. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing and includes the methods and indicators described in Chapter 2, though these indicators would only support suspicious activity, and may not be identified as or connected to terrorist financing once further investigation is undertaken.

193. It should be noted that transactions associated with the financing of terrorism may be conducted in very small amounts, which may not be the type of transactions that are reflected in the indicators for money laundering. Where funds are from legal sources, it is even more difficult to determine if they could be used for terrorist purposes. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimate sources, transactions related to terrorist financing may not exhibit the same traits as conventional money laundering.

194. The ability of casinos to detect and identify potential terrorist financing transactions without guidance on terrorist financing typologies or unless acting on specific intelligence provided by the authorities is significantly more challenging than is the case for potential money laundering and other suspicious activity.

195. Detection efforts, absent specific national guidance and typologies, are likely to be based on monitoring that focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available (many of which are indicative of the same techniques as are used for money laundering). Particular individuals, organisations or countries may be the subject of terrorist financing sanctions, in a particular country. In such cases a listing of individuals, organisations or countries to which sanctions apply and the obligations on casinos to comply with those sanctions are decided by individual countries.

CHAPTER 4 - POLICY IMPLICATIONS

196. A number of issues and policy implications have been identified by the APG/FATF casinos project. Many of these relate to implementation issues with the current FATF standards.

Online gaming / online casinos

197. While this study has not included online gaming / online casinos in its scope of enquiry, it is clear that there are a number of related risks and vulnerabilities from online casinos. A number of jurisdictions license physical casinos and online casinos under a similar process. This report notes a significant gap with understanding regional money laundering risks and vulnerabilities from online casinos and online gaming. There is a need for further study in this area and for sharing case studies and regulatory models.

Lack of AML/CFT coverage for casino sectors

198. A number of jurisdictions clearly lack awareness of money laundering and terrorist financing risks in the casino and gaming sectors.

199. A significant number of jurisdictions have limited regulatory controls, including 'fit and proper' tests for casino owners, managers and staff, internal controls, etc. A greater number of casinos sectors are not yet subject to any AML/CFT controls, in particular in developing countries. Very few jurisdictions regulate junket operators.

200. ***Vetting, licensing and training relevant employees*** – jurisdictions raised the need to ensure that staff with a potential to impact on the integrity of the casino operation should be vetted and appropriately trained in AML/CFT. There are significant gaps in coverage of staff in some gaming jurisdictions.

201. ***Internal controls*** – Most jurisdictions require casinos to have a documented set of internal controls over almost all aspects of casino operations. Some require the regulator to approve these whilst others require the documented controls to meet a set of specified standards.

Lack of regulatory tools

202. Law enforcement agencies and regulators report the need for and implementation of suitable tools that carry effective, proportionate and dissuasive sanctions to use in the regulation of casinos, which are wilfully negligent in AML. Results of Mutual Evaluations indicate a lack of effective regulatory tools for casinos across members of the FATF and FSRBs.

203. There is a need for further guidance and sharing of best practice models for AML/CFT regulation, supervision and monitoring of the casino and gaming sectors.

Implementation of CDD measures

204. Many jurisdictions have struggled to implement CDD measures in casinos in keeping with the international standards. A number of jurisdictions have not followed the thresholds outlined in the FATF standards (for example opting for a USD 10 000 threshold for CDD).

205. A number of jurisdictions are relying on customers being issued with a casino membership cards for which CDD information is collected at the start of the relationship. Customers are then only required to present the card to identify themselves when transacting over the threshold of USD/EUR 3 000.

206. A number of jurisdictions have noted challenges with determining a suitable timeframe for determining whether transactions are linked for the purposes of determining whether the USD 3 000 is met. Cases have illustrated criminals' awareness of change of shifts with casino staff to seek to avoid reporting requirements.

207. A key issue is that in general casinos are not doing enough to establish source of funds and failing to recognise suspicious activity by their customers. Casino security and marketing systems tend to pay particular attention to customer's financial transactions and gambling behaviours, but mostly in terms of patterns of winning and opportunities to encourage greater participation. There is a need for greater vigilance of patterns of transactions and play, unusual transactions and possible indicators of suspicious transactions.

208. There is a need for jurisdictions to share more case examples of money laundering cases and experience of ways in which effective AML/CFT preventative measures have contributed to detecting and prosecuting cases of money laundering.

Application of AML/CFT controls to casino foreign branches, offices or subsidiaries

209. A number of casino operations are owned or controlled in a jurisdiction other than the one in which the casino is established. It is not clear what AML/CFT obligations are placed on junket when they operate in another jurisdiction. There is an issue in a number of jurisdictions of equivalent AML/CFT controls not being implemented by branch or subsidiary casinos. There is a need for further international guidance and best practice experience with regulating branches and subsidiaries.

Application of AML/CFT controls to casino foreign holding accounts

210. It is not clear what AML/CFT controls are in place over accounts operated in a jurisdiction foreign to the location of the casino. Large casinos may operate marketing offices in jurisdictions other than where the casino is located. Patrons are able to pay in funds to their casino account to be played when they travel to the casino without sending a cross-border wire transfer.

Control of junket operators and their agents

211. A number of jurisdictions that allow junket play do not require registration/licensing and regulation of junket organisers and their agents. The vulnerabilities identified in the previous section raises concerns about the need to ensure that junkets and their agents are not under criminal control/influence and to ensure that financial transactions are transparent and subject to relevant AML/CFT measures.

212. The international standards do not clearly address junket operations, but their role as intermediaries or third parties is a significant concern in many jurisdictions.

213. ***Issues with foreign branches or subsidiaries of junkets*** – as outlined above, a number of junket providers operating in a number of jurisdictions and offer services from the same casino group in a number of jurisdictions. It is not clear what obligations are placed on junket operators when they operate in another jurisdiction.

Regulatory controls over VIP rooms and related facilities

214. There are significant issues with implementation of CDD controls over VIP rooms. In some jurisdictions there are not clear powers for the regulator, FIU or law enforcement to have access and to share information regarding members of casino VIP programs.

215. In some cases VIP gaming rooms are leased to junket operators, who provide the gaming equipment, staff and funds to play in the room. This may be done outside of the CDD and other internal controls of the casino.

216. VIP rooms may offer safety deposit boxes and other facilities that are not subject to AML/CFT controls, but which might represent a vulnerability for AML/CFT.

Regulatory coverage of 'foreigners only' casino models

217. As indicated above, a number of jurisdictions have sought to establish casino sectors, but to ban nationals from entering or playing in the casino. This is viewed as a risk management and harm reduction strategy. In some cases this leads to weakened oversight by authorities as there is a perception that risks from money laundering are less under this model. In some cases of very weak supervision, only basic licensing criteria and foreign exchange obligations are enforced on such casinos.

Regulatory control over high-seas gaming

218. As outlined in the previous section, there is a large-scale high seas or cruise ship casino and gaming market, but few jurisdictions regulate or impose AML/CFT controls over the sector. There are significant issues of legal jurisdiction. In very few cases do the 'flag' jurisdictions of cruise ships offering gaming services extend their regulation to gaming conducted aboard the vessels in international waters.

Controls over significant contractors, systems and equipment

219. Jurisdictions raised concerns about contractors that supply goods with a potential to impact on the integrity of the casino operation (*e.g.* gaming equipment and computer systems) should be required to be subject to probity assessment.

Lack of AML/CFT capacity / experience by casino regulators

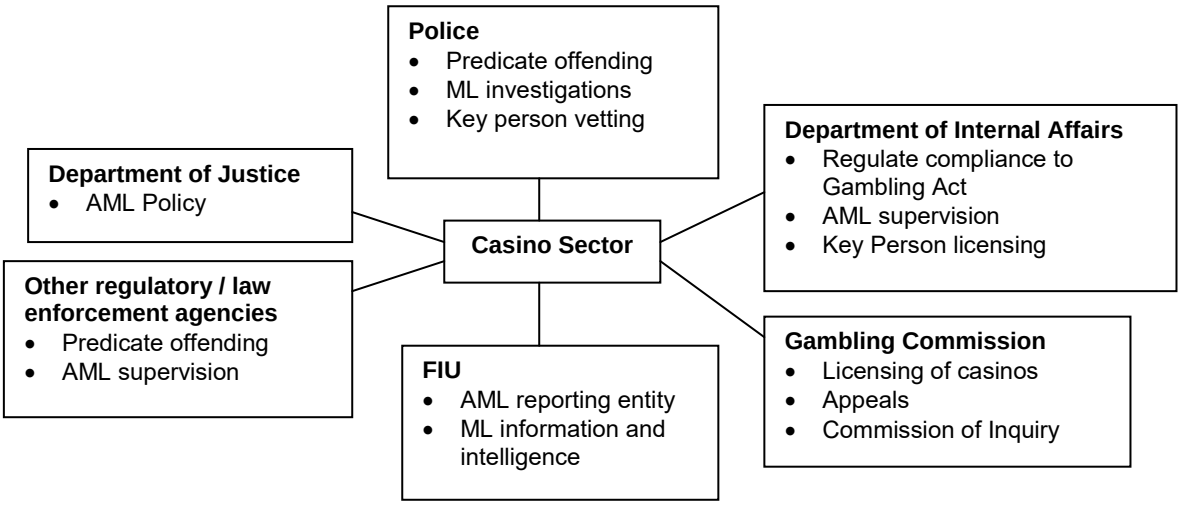
220. In some jurisdictions where casinos have recently been brought under AML/CFT controls, the AML supervisor lacks technical expertise of the casino sector to effectively supervise. There are a number of technical issues specific to casinos and gaming that require sector-specific technical knowledge and experience to support effective regulation and supervision.

Coordination between AML/CFT and casino-sector supervisors

221. Many jurisdictions lack effective coordination between AML/CFT authorities and casino regulatory authorities for setting policies, implementing preventative measures and investigating ML and TF in the sector.

222. In some jurisdictions, a gambling supervisor audits gambling operations in casinos for compliance to gambling laws, but may have a limited role in assessing the casino's level of AML compliance, despite their day to day role. Given the number of financial and non-financial sectors to be supervised, as well as other agencies involved, AML supervision of casinos without the direct involvement of casino regulators may present problems. Joint supervision depends on a high level of inter-agency collaboration to be effective.

223. As shown in the diagram below, New Zealand is an example of a jurisdiction in AML-related policy and operations are invested across a number of agencies.



224. A number of federal systems report state/provincial-level casino regulation, but national level AML/CFT regulation. Effective inter-agency coordination and cooperation is needed to achieve consistent national coverage of casino and gaming sectors for AML/CFT.

Building compliance culture in casino sectors

225. Precluding criminal involvement in casinos and gambling involves addressing both criminal influence and criminal exploitation. Successfully minimising criminal influence of casino operations is dependent upon a licensing and regulatory regime to preclude criminal involvement in the management and operation of casinos and effective preventative measures to detect ML and TF. A number of jurisdictions have struggled to establish an appropriate casino management compliance culture, including for AML/CFT.

226. Persons with large amounts of disposable cash are attractive customers casinos and this makes it imperative that the operator has not only integrity but a commitment to preserving a crime-free environment. Importantly commercial reward systems often provide bonuses or remuneration for "middle management" based on revenue-based performance criteria. These may not take into account the protection of the primary asset (the casino licence) and unless an appropriate management culture is in place within the operator these may work against maintaining a crime-free environment.

227. There is a need for greater cooperation between AML/CFT regulators and enforcement agencies and the front line compliance staff within casinos who are responsible for AML/CFT regulation within casinos.

Law enforcement / FIU / Regulator access to information and investigation of ML/TF

228. ***Legislative system for gathering information for law enforcement:*** Many jurisdictions provide a legislated system for the regulator to receive requests for casino information (such as patron records) and then direct the casino operator to supply that information to the regulator. The regulator then provides the information to the law enforcement agency without the casino being made aware of which law enforcement agency requested the information.

229. In some jurisdictions this provision is regularly used to obtain lists of the casinos' major players for a set time period.

230. There is a reported need for regulations to oblige casinos to adopt AML- systems, particularly when current arrangements hinder the detection and investigation of money laundering. As an example, most casinos operate player tracking systems (or player loyalty schemes) that record customer's levels of gambling, and can include data such as, capital introduced, wagering amounts, win and loss totals, and turnover. This type of information is critical to identifying and prosecuting money laundering; however, these systems are not calibrated to provide the calculations necessary for investigations or to the evidential standard required of prosecutions. Some jurisdictions report casinos showing very little interest in supporting AML efforts by addressing this issue.

231. ***Dedicated police squads or intelligence units:*** – In jurisdictions with large urban casinos it is common for there to be a dedicated police squad (sometimes located on site) or a specific police casino intelligence/investigation unit.

232. An important intelligence function for this type of body is being a gathering point of all available criminal intelligence related to casino operations (including from the casino operator and regulator). It is important that such specialist functions should work closely with AML investigations units.

233. ***Police barring of undesirable patrons***: – A number of jurisdictions have provided the head of the Police with the power to require casinos to bar specified patrons where there are grounds to believe the person might attempt to criminally exploit the casino if allowed to attend. This is generally on the basis of criminal history or in some cases intelligence information. In some jurisdictions this has been made non-appealable and non-reviewable.

234. ***Regulator barring of undesirable patrons***: – A number of jurisdictions have provided the casino regulator with the power to bar or require – casinos to bar specified patrons. This is generally a power reserved for patrons who have not given the casino or police adequate reason to bar the person but owing to information available to the regulator, the regulator is of the opinion that the person is an unacceptable risk to the integrity of the operation of the casino. In some jurisdictions this has been made non-appealable and non-reviewable.

235. ***Casino regulator assistance to FIU***: – In many jurisdictions the casino regulator proactively assists the flow of AML/CTF information to the FIU by conducting inspection programs or audits which seek to identify suspicious activity which the casino operator or regulator then reports to the FIU and/or law enforcement. There needs to be close cooperation between the FIU and gaming regulators.

International Cooperation

236. Effective international cooperation remains a challenge for AML and casino regulatory authorities on AML issues in many jurisdictions. Jurisdictions responses indicated relatively low levels of international cooperation between casino regulatory authorities on issues relevant to AML. In addition, several Asian jurisdictions report the difference in legal frameworks between jurisdictions as a factor, as well as their inexperience in AML/CTF supervision and international information exchange.

237. Effective mechanisms are not always in place, in particular to share information related to junket operators and patrons of junket businesses. There is a need for both casino jurisdictions and those jurisdictions whose citizens regularly travel to casino jurisdictions to ensure clear channels for information sharing and cooperation. This is a challenge when a number of the large casino sectors, such as that in the US, are characterised by a large number of state/provincial/city based regulators.

238. The issues described above in no way represent all of the problems encountered by jurisdictions.

Conclusion

239. While it is estimated that 100 countries participate in casino and card room gambling,[23] this research was able to confirm 77 jurisdictions with legalised casino sectors and 8 jurisdictions who have recently legalised or are giving consideration to legalising casinos. This represents a significant global activity that is cash intensive, competitive in its growth and vulnerable to criminal exploitation. What is encouraging is that all 77 jurisdictions are members of FATF or other related FSRBs, requiring those jurisdictions to meet an international standard in their AML programmes.

240. Mutual Evaluations have shown that globally, that while low, the casino sector has shown relatively higher levels of compliance with FATF standards than other DNFPBs. This is largely because of historical concerns many government have over the perceived levels of criminality and social consequence inherent in casino operations. Governments also tend to impose more stringent supervision and record keeping on casino operations in order to track and secure government revenues. For these reasons, it is often less politically difficult to apply AML/CFT measures to casino sectors, compared to other DNFPBs. Despite this there are many jurisdictions that are yet to fully extend AML controls to the casino sector, and as demonstrated by this research, not all jurisdictions have effective controls over the casino sectors even if they are included in AML frameworks.

241. There are significant regional and global sector vulnerabilities and emerging issues that have weakened AML controls and provide opportunity for money laundering and other financial crimes to flourish.

242. A key issue is casinos not doing enough to establish source of funds and failing to recognise suspicious activity by their customers. Casinos have to pay particular attention to customer's financial transactions and gambling behaviours, particularly if it does not correspond to that of a normal gambler or the intention to play to win is apparently absent or secondary. The methods and indicators in Chapter 2, the sector vulnerabilities and emerging issues in Chapter 3, and the policy implications in Chapter 4 are written to provide government decision-makers and supervisors with the base material from which they can properly target policies and interventions based on the pervasiveness of these methods and issues in their country. But more importantly the material in these chapters, specifically

[23] Casino City.

the methods, case studies and indicators, can and should be shared with casino operators and their staff who are on the front line in confronting these activities, so they may put effect to the AML controls imposed on their operation.

243. Indicators are not of themselves evidence of money laundering and it is not the casino's responsibility to determine that money laundering activity is taking place, rather it is the casino's role is to identify and report the suspicious activity. It is then up to the FIU and law enforcement authorities to examine the matter further and determine if there is a link to money laundering or terrorist financing.

BIBLIOGRAPHY

"An Analysis of the Economic Impact of Indian Gaming in 2006", *National Indian Gaming Association*, http://www.indiangaming.org/info/pr/press-releases-2007/NIGA_econ_impact_2006.pdf. Accessed at 13 July 2008.

Aninat, E. Hardy, D. & Johnston, Barry R. "Combating Money Laundering and the Financing of Terrorism", Finance & Development, Vol. 39, No. 3, September 2002.

"A guide for cruisers who enjoy casino VIP privileges." *Cruise-Casinos*, 2004, http://www.cruise-casinos.com/jackpots.htm.

Australian Casino Economic Report 2005/06", July 2007, *Australian Casino Association*, http://www.auscasinos.com/documents/publicationsSubmissions/ACAFinalReport200506v3.pdf

Casino City, http://www.casinocity.com/casinos, Accessed 16 July 2008.

Corcoran, B. "Betting on (non-) compliance in South Africa", *Money Laundering Bulletin*, Informa UK Ltd.

Department of Internal Affairs. *Gambling Expenditure Statistics 1983 – 2007*, http://www.dia.govt.nz/Pubforms.nsf/URL/Expendstats07.pdf/$file/Expendstats07.pdf
Global Gaming Business., "Asia Update", June 2008.

Ernst & Young, Reviewing the Market: The 2008 Global Gaming Bulletin, 2008

Ernst & Young, Global Gaming Bulletin 25th Anniversary Edition, 2007

European Commission - "Study of gambling services in the internal market of the European Union - Final Report" 14 June 2006, Swiss Institute of Comparative Law, www.isdc.ch , accessed September 2008

French National Institute of Demographic Studies, http://www.ined.fr/fichier/t_telechargement/15700/telechargement_fichier_en_publi_pdf2_pesa436.pdf, Accessed 3 August 2008.

Geller, R. "Saturation or Malaise?" *Global Gaming Business*, June 2008.

Global Gaming Business., "Casinos, Mon!", June 2008.

Guilano , D. "Meet in the Middle: An Update on Gaming in Central America", *Global Gaming Business*, June 2008.

Monaghan,S. "Presentation on Understanding Gaming in the Far East", *13th International Conference on Gambling and Risk Taking*, May 2006.

"Overview of Gaming Worldwide", *Casino City, Global Gaming Almanac*, 2007, http://www.casinocitypress.com/GamingAlmanac/globalgamingalmanac, Accessed 5 July 2008.

PricewaterhouseCoopers., "Economic Crime: People, Culture and Controls", 2007, http://www.pwc.com/extweb/home.nsf/docid/29CAE5B1F1D40EE38525736A007123FD, Accessed 29 July 2008.

Ricardo. C. S. Siu., "Formal Rules, Informal Constraints and Industrial Evolution - The Case of the Junket Operator Regulation and The Transition of Macao's Casino Business", UNLV Gaming Research and Review Journal, Vol. 11, Issues 2, 5 February 2007.

ACRONYMS AND ABBREVIATIONS & GLOSSARY

AML/CFT	Anti Money Laundering and Countering the Financing of Terrorism
APG	Asia Pacific Group on Money Laundering
AUSTRAC	Australian Transactions Reports and Analysis Centre
BSA	Bank Secrecy Act (United States)
CFTAF	Caribbean Financial Action Task Force
CDD	Customer Due Diligence
CPV	Chip Purchase Voucher
CTRC	Currency Transaction Report - Casino
DICJ	Gaming Inspection and Coordination Bureau (Macao, China)
DNFPB	Designated Non-Financial Businesses and Professions
ESAAMLG	The Eastern and South African Money Laundering Group
EAG	The Eurasian Group
EU	European Union
FATF	Financial Actions Task Force
FBI	Federal Bureau of Investigations (United States)
FINCEN	The Financial Crimes Enforcement Network (United States)
FHA	Foreign Holding Account
FINTRAC	The Financial Transactions Report Analysis Centre of Canada
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Body
GIABA	Intergovernmental Anti Money Laundering Group in Africa
IGRA	Indian Gaming Regulation Act (United States)
IMF	International Monetary Fund
IRS	Internal Revenue Service (United States)
ME	Mutual Evaluation
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Europe)
MENAFATF	Middle East and North African Financial Action Task Force
PACGOR	Philippine Amusement and Gaming Corporation
PEP	Politically Exposed Person
POI	Person of Interest
RCMP	Royal Canadian Mounted Police
SAR	Suspicious Activity Report
STDM	Sociedade de Turismo e Diversões de Macao, China
TITO	Ticket In/Ticket Out
VLT	Video Lottery Terminal
VIP	Very Important Player

GLOSSARY OF COMMON CASINO TERMS

The bank	The casino
Barred / banned	A person who is not permitted to enter a casino (may be banned by the casino itself or the regulator)
Betting Limit	For table games, the minimum and maximum amount of money that a player is allowed to wager in a single bet
Bill changer	A machine which accepts coins or currency notes and exchanges them for currency notes or coins
Blackjack	A casino card game. Players bet against the dealer
The Cage (cashier's cage / casino cage)	A secure area within the casino which has custody of funds and provides banking services to casino patrons
Chips	Casino value instruments. Issued by casinos and used in lieu of cash in gaming transactions between the house and player. Chips are round and marked with the denomination and name of the casino and are negotiable within the casino
Dead chips	Promotional or junket associated casino chips that cannot be exchanged for cash. See *Mud Chips* and *non-negotiable chips*
Even money bet	A wager what pays back the same amount that was originally wagered, plus the original wager.
Even money exchange	Exchanging two items of equivalent value in the casino, such as purchasing USD 100 in chips for USD 100 cash
Float	The amount of value (chips + cash) on a table game
High rollers	Premium players who consistently gamble high stakes and large sums of money – see also *VIPs* and *whales*
House	The casino
Junket	A group of people who travel to the casino primarily to gamble. The junket may include transport, accommodation, incentives to play at the casino and the transportation of funds to and from the casino
Junket agent	A person or company who signs up casino patrons to take part in junkets
Junket representative	The person who organises the junket
Mud chips	Promotional or junket associated casino chips that cannot be exchanged for cash. See *Dead Chips* and *Non-negotiable chips*...
Non-negotiable chips	Promotional or junket associated casino chips that cannot be exchanged for cash. See *Dead Chips* and *Mud Chips*
Pit	An area in the casino where gaming tables operate
Pit boss	A casino supervisor responsible for gaming on the casino floor
Plaques	Casino value instruments. Issued by casinos and used in lieu of cash in gaming transactions between the house and player. Rectangular, square-shaped or oval cheque primarily used in European casinos
Slot machines	Gaming machines that accept coins or vouchers and pay out winnings either in coins or via cashier's cheque
Ticket-in-ticket-out	A cashless slot machine that uses vouchers instead of chips or coins
VIP	Premium players who consistently gamble high stakes and large sums of money – see also *Highrollers* and *whales*
Wager	A bet of value
Whale	A high-stakes player

APPENDIX 1. REGIONAL DATA ON CASINO SECTORS

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Africa						
Benin	Yes	1		No		
Botswana	Yes	10			None	Only two casinos operate gaming tables with the reminder operating only slot machines. Both the casinos with gaming tables are subsidiaries of South African casinos. A bill to include casinos under AML/CFT regime is being drafted.
Cameroon	Yes	3				
Central African Republic	Yes	2				
Comoros	Yes	3		Unclear		
Cote d'Ivoire	Yes	1		Unknown		Abidjan Hotel Ivoire Inter-Continental & Casino
Democratic Republic of the Congo	Yes	1		No		

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Djibouti	Yes	1		Unknown		
Egypt	Yes	25				
Gambia	Yes					Kololi Casino, African Gaming Co. Ltd. – Royal 7's
Ghana	Yes	3				Run by KaiRo International.
Kenya	Yes	15				Controlled by the Betting Control & Licensing Board, Mombasa
Liberia	Yes	1				
Madagascar	Yes	2		No		
Malawi	Yes	1+		No		
Mali	Yes	1		No		Run by KaiRo International.
Mauritius	Yes	7+		No		
Morocco	Yes	8?		Yes		
Mozambique	Yes	3		No		
Namibia	Yes			No		
Nigeria	Yes	2				
Reunion	Yes	4				
Senegal	Yes	4				

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Seychelles	Yes	3				
Sierra Leone	Yes	1		No		Licensed, but no supervision by government.
South Africa	Yes	45		Yes		**More details**
Swaziland	Yes	3			Yes	licensed online operators
Tanzania	Yes	3				
Tunisia	Yes	3		No		Only open to foreigners.
Uganda	Yes	3				
Zambia	Yes	3				
Zimbabwe	Yes	6			Yes	Lotteries and Gaming Act, 2000 -Ministry of Home Affairs is the regulator. Limited CDD obligations
Middle East						
Israel	Yes	4				NB – two of these casinos are cruise-ship based casinos
Lebanon	Yes	1				
Central Asia						
Kazakhstan	Yes	28				Since April 2007 laws passed to limit casinos to two provincial cities — Kapchagai (near Almaty) and Shchuchinsk.
Kyrgyzstan	Yes	18		Yes	Yes	MER noted that casinos are showing some resistance to AML/CFT implementation.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Turkmenistan	Yes	2				
Asia/Pacific						
Cambodia	Yes	21		No	No	Cambodian nationals are prohibited from entering casinos
Chinese Taipei	No		Yes			Press reports indicate that in late 2007 the Chinese Taipei legislature was considering a draft gambling bill which, if passed, would legalise casinos and gaming in Chinese Taipei
Hong Kong, China	No				No	Foreign registered vessels operate casinos in international waters.
India	Yes	6		No		Offshore – limited to the state of Goa
Japan	No		Possibly		No	
Korea, South	Yes	17		Yes	No	
Korea, North	Yes	1		No		
Lao PDR						
Macao, China	Yes	31		Yes	No	3 concessionaires and 3 sub-concessionaries operate all the casinos in Macao, China. Annual revenue is over USD 13.8 billion per annum
Malaysia	Yes	1		Yes	No	
Myanmar	Yes	4		No		The established casinos are not clearly legal.
Nepal	Yes	6	No	No	Yes	Nepal nationals are prohibited from entering. No 'fit and proper' tests for licensees

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Palau	No		Yes		No	Proposals for legalising casino sector have not been supported.
Philippines	Yes	14		No	Yes	All 14 casinos are government owned and operated by PAGCOR. PAGCOR operates an internet casino run in conjunction and cooperation with PhilWeb Corp Approximately 20% of patrons are foreign nationals - Chinese Taipei, Japan and Hong Kong, China.
Singapore	No		Yes	Yes	No	
Sri Lanka	Yes	9		No		Nationals are not allowed into Sri Lankan casinos. Casinos are not clearly regulated by the government, although tax is paid. There is no 'fit and proper' test for casino licensees.
Thailand	No		Possibly			Initial risk assessment from illegal gaming sector undertaken
Vietnam	Yes	2		Yes	No	
Australia	Yes	13	No	Yes	Yes	State-based casino regulation, with FIU national AML/CFT regulator.
New Caledonia	3					
New Zealand	Yes	6	No	Yes	No	Regulator is
Northern Mariana Islands	1					
Papua New Guinea			Yes	No	Yes	Newly passed legislation, May 2007
Solomon Islands	2					
Vanuatu	Yes	2	Yes	Yes	No	No 'fit and proper' tests for casino licensees. Vanuatu licensed an online casino, but it no longer in

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
						operation since 2002.
Europe						
Albania	Yes	1				
Austria	Yes	12		Yes		
Belarus	Yes	Approx 25		Yes		
Belgium	Yes	9		Yes		
Bosnia & Herzegovina	Yes	1				
Bulgaria	Yes	7				
Croatia	Yes	15				
Northern Cyprus (Area of)		Approx. 20				
Czech Republic	Yes	158		No		2004 -27 licenses for 158 casinos across the country. 15 licensed for foreign exchange
Denmark	Yes	6		Yes		
Estonia	Yes	75				
Finland	Yes	1 + some in Åland		Yes Unclear if Åland is covered.	Some in Åland.	Casinos also operating on ships.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
France	Yes	161		Yes		Widespread casino and gaming industry
Georgia	Yes	10		Yes		
Germany	Yes	62				Widespread casino and gaming industry. Casino regulators at state level. AML/CFT is a federal role
Gibraltar	Yes	1			Yes	19 online casino licensees offering 166 sites.
Greece	Yes	9		No		
Hungary	Yes	6		Yes		
Ireland	No				No	A number of private gaming clubs operate casino-like facilities that create an AML/CFT risk, but which fall outside the scope of the CJA (1994).
Italy	Yes	5		Yes		Although legislation has been adopted bringing casinos within the scope of the AML Law, further regulations are required to implement it.
Latvia	Yes	14		Yes	Yes	
Lithuania	Yes	18		Yes		
Luxembourg	Yes	1				
Malta	Yes	3		Yes	Yes	Regulated by the Lotteries and Gaming Authority 266 online gaming sites are operating. Malta regulates junket providers
Moldova	Yes					

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Monaco	Yes	4				
Netherlands	Yes	167		Yes		
Poland	Yes	27		Yes		FIU is the casino regulator for AML/CFT purposes ***The Ministry of Finance gives licenses, approves rules of the games in casinos, issues certificates of profession and registers gambling devices***.
Portugal	Yes			Yes	No	
Romania	Yes	20		Yes		The number of tourists who come especially to gamble in the Romanian casinos is very little, even insignificant (approximately 40-50 persons/month).
Russia	Yes	169		Yes – the FIU	Yes	After 1 July 2009, all gaming will be prohibited in Russia, except within 4 newly created special gaming zones in Kaliningrad, Rostov-na-Donu, Altai and Primorie Krai (Vladivostok).
Serbia & Montenegro	Yes	7				
Slovakia	Yes	4			1	
Slovenia	Yes	23 + 36 gaming saloons		Yes		Office for Gaming Supervision is the regulator. The 23 licenses for Casinos are mainly owned
Spain	Yes	39 + 2 branches		Yes	No	Approx 3.5 million visitors per annum to Spain's casinos. Regulator is the Ministry of Interior through the National Police.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Sweden	Yes	4	No. Casinos Act allows for a maximum of 6 casinos	AML only	No	Sweden does not permit internet casinos. MER noted Swedish businesses marketing Malta-based internet casinos in Sweden. Swedish National Gaming Board is the regulator - www.lotteriinspektionen.se
Switzerland	Yes	19	No	Yes	No	
Ukraine	Yes	45		Yes		Over 50 000 patrons visit Ukrainian casinos daily. Ministry of Finance is the licensing body.
United Kingdom	Yes	140 operating casinos		Yes	Yes	Regulations have permitted operators to apply for an online casinos license only since 2007. Regulator: The Gambling Commission - http://www.gamblingcommission.gov.uk
The Americas & Caribbean						
Antigua & Barbuda	Yes	6			yes	
Argentina	Yes	80				Regulated at the provincial level
Aruba	Yes	10				
Bahamas	Yes	4		Yes	No	Tourism Board is the general and AML regulator
Barbados	Yes	2				
Belize	Yes	2			Yes	
Canada	Yes	63		Yes	No	*Cruise ship casinos*. Cruise ships can offer casino facilities under strict conditions in Canadian waters, but are not covered by the AML/CFT legislation.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Chile	Yes	17				In 2005 a new Casino Law was passed for a maximum of 24 casinos
Colombia	Yes	20				ETESA regulates all gambling
Costa Rica	Yes	35		No	Yes	more than 250 sports betting companies operate as online casinos
Dominican Republic	Yes	32		No		There is no monitoring of the financial behaviour of casinos or supervision of their AML compliance.
Ecuador	Yes	13				
El Salvador	Yes	2				
Guyana	No					
Haiti	Yes	2				
Honduras	Yes	3				
Jamaica	Yes	10		No		
Martinique	Yes	2				
Mexico	Yes	Up to 5		No		Temporary permits for large-scale “salones de Apuestas“. Regulator is the Secretaría de Gobernación (Ministry of Interior)
Netherlands Antilles	Yes	26				
Nicaragua	Yes	10				
Panama	Yes	36		Yes	1 not yet functioning	

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Paraguay	Yes	3				
Peru	Yes	7				
Puerto Rico	Yes	18				
Saint Vincent & the Grenadines	Yes	2				
St Kitts and Nevis	Yes	2				
Suriname	Yes	9		No		
Trinidad & Tobago	No			No		No legal casinos but the 72 Private Members Clubs (registered) seem to operate like Casinos, but are not supervised.
USA	Yes	845		Yes	No	Various US gaming jurisdictions regulate junket operators and their agents.
Uruguay	Yes	18				
Venezuela	Yes	5				

Appendix P:

FATF, *Money Laundering & Terrorist Financing Through the Real Estate Sector* (Paris: FATF, 2007)

Financial Action Task Force

Groupe d'action financière

MONEY LAUNDERING & TERRORIST FINANCING THROUGH THE REAL ESTATE SECTOR

29 June 2007

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. Various reports produced by the FATF over the last few years have made reference to the fact that the real-estate sector may be one of the many vehicles used by criminal organisations to launder their illicitly obtained money.[1] The general objective of this report is to develop more information on this issue and present a clearer picture of the way that real estate activity can be used for money laundering or terrorist financing.

2. The study aims to accomplish two primary goals: First, it explores the means by which illicit money is channelled through the real-estate sector to be integrated into the legal economy. Second, it identifies some of the control points that could assist in combating this phenomenon. One of the most effective ways to understand how the sector is abused is to examine concrete case studies; therefore, the report is based primarily on information provided by participating FATF and non-FATF members.

3. Several characteristics of the real estate sector make it attractive for potential misuse by money launderers or terrorist financiers. The report outlines the reasons for this. From the case examples provided during the research for this project, several basic techniques were identified, such as the use of complex loans or credit finance, the use of non-financial professionals, the use of corporate vehicles and so on. The report briefly describes these techniques, followed by one or more most striking case examples. To reach out to the private sector, part of the research has been to develop a basic list of risk indicators from the case examples. These indicators may assist financial institutions and others involved in certain types of real estate activities in customer due diligence and in performing a risk analyses on new and existing clients.

4. The project identified three areas that seem especially vulnerable for misuse in money laundering schemes involving real estate and thus suitable for further consideration. In almost all case examples provided, wire transfers to channel the money have been involved at some stage. Also emerging markets seem to be more vulnerable to misuse of the real estate sector. Due to the worldwide market growth of real estate-backed securities and the development of property investment funds, the range of options for real estate investments has also grown. This effect has not gone without notice in emerging markets. Money laundering transactions can be easily camouflaged in genuine commercial transactions among the huge number of real estate transactions taking place. Complicating matter is the fact that often these less developed economies do not have an average market price for real estate, but rather prices varying across sectors and districts. To complete real estate transactions in some stage of the process involvement of legal expert is inevitable. The case examples have shown this category, when not covered by AML/CFT obligations, often becomes the weakest link in the process.

[1] This report is the product of research carried out by a project team operating under the umbrella of the FATF typologies initiative. The FATF project team was led by Spain and the Netherlands with the participation of Australia, Belgium, Canada, Japan, Lebanon, Luxembourg, Mexico, Myanmar, Norway, Pakistan, Portugal, South Africa, South Korea, Sweden, Ukraine, the United Kingdom, the United States, Interpol, the European Central Bank, and the OECD.

INTRODUCTION: NATURE OF THE REAL-ESTATE SECTOR

5. The real estate sector merits closer consideration given the large scope of monetary transactions, its significant social impact, and because of the number of cases in which money laundering, and in limited circumstances terrorist financing and tax fraud schemes, have been detected.[2] Abuse in this sector also has the undesirable effect of political, institutional and economic destabilisation. Moreover, due to the international nature of the real-estate market, it is often extremely difficult to identify real estate transactions associated with money laundering or terrorist financing.

6. Given that the purchase or sale of a property is one of the largest financial transactions a family or individual may undertake, changes in property prices have a substantial impact on the considerations taken into account by potential buyers and sellers of properties. Fluctuations in property prices have an impact on decisions about where to live and work in addition to affecting an owner's net worth. Moreover, to the extent that property values influence rents, the effect is manifested in the distribution of wealth between landlords and tenants. Finally, property prices significantly influence the building industry. Taken together, these factors all suggest that fluctuations in property prices may influence economic activity and price stability by affecting aggregate supply and demand, the distribution of income, and the debt decisions undertaken by households.[3]

7. Nevertheless, it is difficult to monitor and explain variations in property prices due to a lack of reliable and uniform information. Property markets are geographically segmented and numerous factors shape the local price of real-estate. Understanding the factors that underlie pricing in the property market is therefore essential.

8. Historically there exists a commercial and residential real-estate market, and the property in both types of market may be bought and sold, managed and/or developed. More recently, new investment vehicles have emerged, including *property investment funds* (PIF) and *real estate investment trusts* (REIT). Such instruments allow average citizens to invest in markets – historically only available to the very wealthy – in order to create a diversified portfolio.

9. Investment in the real-estate sector offers advantages both for law-abiding citizens and for those who would misuse the sector for criminal purposes. Real property has historically appreciated in value, and many countries offer incentives to buyers, including government subsidies and tax reduction. Most importantly for misuse by criminals, however, is the facility the sector may provide for obscuring the true source of the funds and the identity of the (ultimate) beneficial owner of the real asset, which are two key elements of the money laundering process.

10. The real-estate sector is therefore of extraordinary importance to the economy in general and the financial system in particular. The widespread use of mechanisms allowing households to access the property market, the elimination of personal limitations on property ownership, the economic development and growth of tourism in many regions have all led to exponential growth in the number

---

[2] It is important to note as is mention by the OECD (Sub-group on Tax Crimes and Money Laundering) in its real estate report that in many countries, their tax authorities investigate these cases in partnership with other law enforcement agencies. In some instances, parallel investigations for tax fraud and money laundering may be pursued. The OECD examined tax fraud and money laundering involving the real estate sector, along with identity theft and identity fraud. It also developed a training manual to assist tax auditors in detecting and reporting cases of suspected money laundering and/or terrorist financing. The confidential report contains: the scope and nature of the issue, how cases are successfully detected and investigated, a list of red flag indicators (catalogue), the benefits of multi-agency co-operation (including effective exchange of information), compliance results and risk prevention strategies and an inventory of relevant case studies.

[3] European Central Bank (2006).

of financial transactions linked to real-estate. The extraordinary range of possibilities for misusing these processes also allows suspected criminals to integrate and enjoy illegally obtained funds.

11. Through the implementation of international standards in recent years, countries have put various measures into place within their formal financial sector – which includes, among others, banks and credit unions – in order to prevent money laundering and terrorist financing. Because of the tendency for illegal activity to move to other financial / economic areas that may have less formal oversight or where there is relatively less potential for detection, countries must consider extending AML/CFT measures to other parts of their economies, if they want to respond successfully to this threat. For the real-estate sector, this would necessarily include such key players as real-estate agents, legal advisors and notaries.

BASIC TECHNIQUES

12. In order to misuse the real-estate sector, a number of methods, techniques, mechanisms, and instruments[4] are available. Many of these methods are in and of themselves illegal acts; however, certain of them might be considered perfectly legal if they were not associated with a money laundering or terrorist financing scheme (or if this association could not be detected. Through examination of case examples from past money laundering and terrorist financing cases, this study has identified a series of the more common or basic methods and then grouped them according to type or "typology".

- Use of complex loans or credit finance.
- Use of non-financial professionals.
- Use of corporate vehicles.
- Manipulation of the appraisal or valuation of a property.
- Use of monetary instruments.
- Use of mortgage schemes.
- Use of investment schemes and financial institutions.
- Use of properties to conceal money generated by illegal activities.

Typology 1: Complex Loans and Credit Finance

13. Intercompany loans have become a frequent instrument used as a means for raising funds. The ease with which such loans can be arranged makes them popular with the general public. These loans are also used in the real estate sector. Where an instrument is frequently used, misuse of the instrument becomes a possibility as well. Depending on the way in which the loan is structured, two different schemes have been detected.

Loan-Back Schemes

14. Intelligence and law enforcement reports indicate "loan-back" transactions are used by suspected criminals to buy properties – either directly or indirectly – through the purchase of shares in property investment funds. Essentially, suspected criminals lend themselves money, creating the appearance that the funds are legitimate and thus are derived from a real business activity. The purpose of the loan is to give the source of the money an appearance of legitimacy and to hide the true identity of the parties in the transaction or the real nature of the financial transactions associated with it.[5]

---

[4] This report uses the terminology commonly used by the FATF in its various projects. See Annex A to this report and FATF (2005) for more on this terminology.

[5] The lack of information caused by the internationalisation of these structures and their specific morphology make it difficult to understand the true relationship between the various corporate vehicles involved in the loan structure and to be sure of the real origin of the funds, and thus determine whether they are linked to criminal activities or not. In several cases, offshore company loans were used. See FATF (2006) for more on the use of legal persons for money laundering.

Case study 1.1: Proceeds of drug trafficking laundered into real estate

(Predicate offence: money laundering forged loan agreement)

An individual set up three companies. For one of the companies he held bearer shares. To hide his involvement in the companies he used a front-man and a trust and company service provider[6] as legal representatives. For each of the companies, the legal representatives opened bank accounts with three different banks in different jurisdictions. The individual used the three companies to set up a loan-back scheme in order to transfer, layer and integrate his criminal money. He then co-mingled the criminal funds with the funds that originated from the legal activities of one of his companies.

Next the front man then bought real estate. To finance that transaction he arranged for a loan between the two companies.

A more detailed version of this scheme (describing all steps in the process) is included in Annex C.

Indicators and methods identified in the scheme:

- **The source of the funds used to finance the real estate transaction was from abroad, in particular from offshore jurisdictions and jurisdictions with strict bank secrecy.**
- **The lender of the money, an offshore company, had no direct relation with the borrower of the money**
- **A financial institution was not involved in the loan structure.**
- **There was no loan agreement between the lender and borrower.**
- **The loan agreement was legally invalid.**
- **The information in the loan agreement was inconsistent or incorrect.**
- **The conditions in the loan agreement were unusual (for example, no collateral was required).**
- **No payment of interest or repayment of the principal.**
- **Transaction monitoring by financial institutions showed payable-through accounts, by which incoming payments from abroad were immediately transferred abroad without a logical reason.**

Source: Netherlands.

Back-to-Back Loan Schemes

15. As with *loan-back* schemes, *back-to-back loans* are also known to be used in real-estate related money laundering schemes. In this case, a financial institution lends money based on the existence of collateral posted by the borrower in the usual way. However, the collateral presented to the financial institution originates from criminal or terrorist activities. Although financial institutions are obligated to disclose the existence of these funds on a risk dossier, there are occasions where this analysis may contain shortcomings. Instances where the collateral posted is not specified in the loan agreement or unreliable information as to the nature, location and value of the collateral make it very difficult to recognise a back-to-back loan.

Case study 1.2: Back-to-back loan used to launder funds

(Predicate offence: forged loan agreement, in particular the failure to mention the security underlying the loan and money laundering)

An individual set up two companies in different jurisdictions. He used a front man and a trust and company service provider as legal representatives to hide his involvement. One of the companies, led by the front-man, owned real estate and generated income through rental activity. He set up a back-to-back loan structure to use his criminal money for his real estate investments. He then arranged a bank guarantee between two banks in case of a default of the loan. The bank was willing to provide the bank guarantee with the pledged deposit of one of his companies as collateral. The money placed as a deposit was generated by the individual's criminal activity.

A more detailed version of this scheme (describing all steps in the process) is included in Annex C.

Indicators and methods identified in the scheme:

- **No reference in the loan agreement to the underlying collateral.**

[6] See Annex A for definitions of this term and others used in this report.

- **The collateral provided was not sufficient**
- **The collateral provider and other parties involved in the loan structure were not known.**
- **The borrower of the money was not willing to provide information on the identity and background of the collateral provider and/or the other parties involved in the loan structure.**
- **The complex nature of the loan scheme could not be justified**
- **There was an unexpected loan default.**

Source: Netherlands.

Typology 2: The Role of Non-Financial Professionals

16. Research has shown that when governments take action against certain methods of money laundering, criminal activities tend to migrate to other methods. In part, this reflects the fact that more aggressive policy actions and enforcement measures increase the risk of detection and therefore raise the economic cost of using these methods.

17. FATF experts have observed in recent years that money launderers are increasingly forced to develop elaborate schemes to work around AML/CFT controls. This has often meant seeking out the experience of professionals such as lawyers, tax advisors, accountants, financial advisors, notaries and registrars in order to create the structures needed to move illicit funds unnoticed. These professionals act as *gatekeepers* by providing access to the international financial system, and knowingly or not, can also facilitate concealment of the true origin of funds.[7]

Obtaining Access to Financial Institutions Through Gatekeepers

18. A number of cases reveal that criminals and terrorists have used non-financial professionals or gatekeepers to access financial institutions. This is especially important during the process of determining eligibility for a mortgage, opening bank accounts, and contracting other financial products, to give the deal greater credibility. It has also been documented that bank accounts are opened in the name of non-financial professionals in order to carry out various financial transactions on their behalf. Examples include depositing cash, issuing and cashing cheques, sending and receiving international fund transfers, etc., directly through traditional saving accounts or indirectly through correspondent accounts.[8]

Case study 2.1: Misuse of a real estate agent to gain introduction to a financial institution, possible link to terrorist financing

(Predicate offence: suspected terrorist financing)

A trustee for a trust established in an offshore centre approached a real estate agent to buy a property in Belgium.

The real-estate agent made inquiries with the bank to ask whether a loan could be granted. The bank refused the application, as the use of a trust and a non-financial professional appeared to be deliberately done to disguise the identity of the beneficial owner. The bank submitted a suspicious transaction report.

Following the analysis of the financial intelligence unit, one of the members of the board of the trust was found to be related to a bank with suspected links to a terrorist organisation.

Indicators and methods identified in the scheme:

- **Instrument: real estate, loan.**
- **Mechanisms: bank, trust, real-estate agent.**

[7] FATF (2001), p. 12.

[8] Although it is not the scope of the report, the FATF experts have observed the misuse of the correspondent accounts as a way to hide the origin or destination of money flows and the real participants in the transaction. On several occasions, the misuse of these accounts has been linked to the type of operations reflected in it, especially when cheques or cover payments were used.

- **Techniques: offshore customer, non-account holder customer, physical person intermediary, high risk jurisdiction, loan, purchase of real estate.**
- **Opportunity taken: using a trust and appealing to a non-financial profession was clearly done to disguise the identity of the beneficial owner.**

Source: Belgium, 2003.

Assistance in the Purchase or Sale of Property

19. Non-financial professionals such as notaries, registrars, real-estate agents, etc., are sometimes used by suspected criminals on account of their central role in carrying out real-estate transactions. Their professional roles often involve them in a range of tasks that place them in an ideal position to detect signs of money laundering or terrorist financing.

20. Until relatively recently, however, these professionals have not been obligated under international standards to report suspicious activity to their national financial intelligence units (FIUs). In some countries where non-designated financial professionals fall under the scope of anti-money laundering legislation, these systems are still in the initial stages of implementation[9], so that the level of co-operation and the effectiveness of their suspicious transaction reporting have not yet been extensively tested. Operational problems have also arisen. In some cases, these have resulted from difficulties in centralising information gathered from various domestic authorities, and in others it stems from differences in legal systems between jurisdictions (common law and civil law, for example).

21. Several cases have come to light revealing that the role of non-financial professionals in detecting illegal activity can also be significant in this area. There have been examples of notaries and registrars detecting irregularities in the signing of the property transfer documents (for example, using different names or insisting on paying a substantial part of the cost of the transaction in cash). Other examples include buying land designated as residential through a legal person and then reclassifying it a short time later for commercial development. Professionals working with the real-estate sector are therefore in a position to be key players in the detection of schemes that use the sector to conceal the true source, ownership, location or control of funds generated illegally, as well as the companies involved in such transactions.

Case study 2.2: Use of a notary when buying a real estate

(Predicate offence: suspected money laundering by organised crime)

An East European was acting under a cover name as the director of a company for which he opened an account with a Belgian bank. Transfers were made to this account from abroad, including some on the instructions of "one of our clients".

The funds were then used to issue a cheque to a notary for the purchase of a property. The attention of the notary was drawn to the fact that some time after the purchase, the company went into voluntary liquidation, and the person concerned bought the property back from his company for an amount considerably above the original price. In this way the individual was able to insert money into the financial system for an amount corresponding to the initial sale price plus the capital gain. He was thus able to use a business account, front company customer, purchase of real estate, cross border transaction and wire transfers to launder money that, according to police sources, came from activities related to organised crime.

It appeared that the company acted as a front set up merely for the purpose of carrying out the property transaction.

Indicators and methods identified in the scheme:

- **Instruments: check, wire transfers, real estate.**

[9] In some countries the sector contains a large group of supervised natural and legal persons. That may be the cause for concerns regarding the capacity to provide adequate supervision.

- **Mechanisms: notary, bank.**
- **Techniques: business account, front company customer, purchase of real estate, cross border transaction, incoming wire transfer, reverse/flip real estate, unknown source.**
- **Opportunity taken: use of a notary when buying a real estate. Since the company's bank account was not used for any other transaction, it can be deduced that this company was a front company set up for the mere purpose of carrying out the property transaction.**

Source: Belgium, 2003.

Trust Accounts

22. A *trust account*[10] is a separate bank account, which a third party holds on behalf of the two parties involved in a transaction. Funds are held by the trustee until appropriate instructions are received or until certain obligations have been fulfilled. A trust account can be used during the sale of a house, for example. If there are any conditions related to the sale, such as an inspection, the buyer and seller may agree to use a trust account. In this case, the buyer would deposit the amount due in a trust account managed by, or in the custody of, a third party. This guarantees the seller that the buyer is able to make the payment. Once all the conditions for the sale have been met, the trustee transfers the money to the seller and the title to the property is passed to the buyer.

Case study 2.3: Use of a solicitor to perform financial transactions

(Predicate offence: distribution of narcotics)

An investigation of an individual revealed that a solicitor acting on his behalf was heavily involved in money laundering through property and other transactions.

The solicitor organised conveyancing for the purchase of residential property and carried out structured transactions in an attempt to avoid detection. The solicitor established trust accounts for the individual under investigation and ensured that structured payments were used to purchase properties and pay off mortgages.

Some properties were ostensibly purchased for relatives of the individual even though the solicitor had no dealings with them. The solicitor also advised the individual on shares he should buy and received structured payments into his trust account for payment.

Indicators and methods identified in the scheme:

- **Instruments: cash deposits, real estate.**
- **Mechanisms: solicitor, trust accounts.**
- **Techniques: structured cash transactions, establishment of trust accounts to purchase properties and pay off mortgages, purchase of property in the names of the main target.**
- **Opportunity taken: the solicitor set up trust accounts on behalf of the target and organised for transactions to purchase the property, pay off mortgages, and shares were purchased to avoid detection. In some cases properties were purchased in the names of relatives of the target.**

Source: Australia.

Management or Administration of Companies

23. There have been documented cases of non-financial professionals approached by money launderers and terrorists not just to create legal structures, but also to manage or administer these companies. In this context, these professionals may have been generally aware that they are taking an active role in a money laundering operation. Their access to the companies' financial data and their direct role in performing financial transactions on behalf of their clients make it almost impossible to accept that they were not aware of their involvement.

[10] Also known as an *escrow* account.

Case study 2.4: Abuse of a notary's client account

(Predicate offence: suspected trafficking in narcotics)

A company purchased property by using a notary's client account. Apart from a considerable number of cheques that were regularly cashed or issued, which were at first sight linked to the notary's professional activities, there were also various transfers from the company to his account.

By using the company and the notary's client account, money was laundered by investing in real estate in Belgium, and the links between the individual and the company were concealed in order to avoid suspicions.

Police sources revealed that the sole shareholder of this company was a known drug trafficker.

Indicators and methods identified in the scheme:

- **Instruments: cheque, cash, wire transfers, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: intermediary account, purchase of real estate, incoming wire transfer.**
- **Opportunity taken: by using the company and the notary's client account money was laundered by investing in real estate in Belgium, and the links between the individual and the company were concealed in order to avoid suspicions**

Source: Belgium, 2002.

Typology 3: Corporate Vehicles

24. Corporate vehicles – that is, legal persons of all types and various legal arrangements (trusts, for example)[11] – have often been found to be misused in order to hide the ownership, purpose, activities and financing related to criminal activity. Indeed that practice is so common that it almost appears to be ubiquitous in money laundering cases. The misuse of these entities seem to be most acute in tax havens, free-trade areas and jurisdictions with a strong reputation for banking secrecy; however, it may occur wherever the opacity of corporate vehicles can be exploited.

25. Apart from obscuring the identities of the beneficial owners of an asset or the origin and destination of funds, these corporate vehicles are also sometimes used in criminal schemes as a source of legal income. In addition to shell companies, there are other specialised companies that carry out perfectly legitimate business relating to real estate, which have sometimes been misused for money laundering purposes. This aspect is illustrated by the use, for example, of property management or construction companies. The use of corporate vehicles is further facilitated if the company is entirely controlled or owned by criminals.

Offshore Companies[12]

26. Legal persons formed and incorporated in one jurisdictions, but actually used by persons in another jurisdiction without control or administration of a natural or legal resident person and not subject to supervision, can be easily misused in money laundering transactions. The possibilities for identifying the beneficial owner or the origin and destination of the money are at times limited. In these scenarios actors with wrongful intentions have the distinct advantage of extra protection in the form of bank secrecy.

[11] See Annex A for definitions of some of these terms.

[12] It applies to the situation where a company is incorporated in one jurisdiction for persons who are resident in another jurisdiction. See FATF (2006) for the terminology relating to offshore companies.

Case study 3.1: Use of an offshore company to buy real estate.

(Predicate offence: suspected violations related to the state of bankruptcy)

A bank reported a person whose account had remained inactive for a long period but which suddenly was inundated with various cash deposits and international transfers. These funds were then used to write a cheque to the order of a notary for the purchase of a real estate.

It appeared that the party involved had connections with a company in insolvency and acted in this way to be able to buy the property with a view to evading his creditors.

The final buyer of the real estate was not the natural person involved but an offshore company. The party involved had first bought the property in his own name and subsequently had passed it on to the aforementioned company.

Indicators and methods identified in the scheme:

- **Instrument: cash, wire transfers, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: personal account, purchase of real estate, incoming wire transfer, dormant account, offshore transactions.**
- **Opportunity taken: use of an offshore company to buy real estate. It appeared that the party involved had connections with a company in insolvency and acted in this way to be able to buy the property with a view to getting away from his creditors.**

Source: Belgium, 2002.

Legal Arrangements

27. The use of some legal arrangements such as trusts can play an important role in money laundering. Under certain conditions these legal arrangements can conceal the identity of the true beneficiary in addition to the source and/or destination of the money.

28. The nature and/or structure of certain trusts can result in a lack of transparency and so allow them to be misused:[13]

- Certain trusts may exist without the need for a written document constituting them.
- Although there may be a deed defining the trust, in some cases it does not need to identify the depositary and/or a specific beneficiary.
- There may be no obligation to register decisions regarding the management of a trust, and it may not be possible to disclose them in writing to anyone.
- In some types of trust, such as discretionary trusts, the beneficiary may be named or changed at any time, which makes it possible to safeguard the identity of the beneficiary at all times up until the moment the ownership of the assets is transferred.
- Trusts set up to protect assets may protect the depositary against decisions to freeze, seize or attach those assets.
- Trusts may be set up to manage a company's shares, and they may make it more difficult to determine the identities of the true beneficiaries of the assets managed by the trusts.
- Certain legislation may expressly prohibit the freezing, seizure or attachment of assets held in trust.
- Certain clauses commonly referred to as escape clauses, allow the law to which the trust is subject to be changed automatically if certain events arise. Such clauses make it possible to protect the assets deposited in the trust from legal action.

[13] See FATF (2006) for a short explanation of trusts.

29. These conditions may create a significant obstacle for the authorities charged with applying anti-money laundering and counter terrorist financing laws – especially in relation to international co-operation – thus significantly slowing the process of collecting information and evidence regarding the very existence of the trust and identifying its ultimate beneficiary. Under these circumstances it may be very difficult, if not impossible, for a bank or other financial institution to comply with the "know-your-customer" policies applicable in the country or territory in which it is located.[14]

Case study 3.2: Use of trusts to buy real estate

(Predicate offence: suspected serious tax fraud)

Two trusts were established in an offshore centre by a law firm. The trustee had been requested to accept two payment orders in favour of a bank in order to buy real estate. The communication between these trusts and their trustee always took place through the law firm. It appeared that the trust had been used to conceal the identity of the beneficial owners.

Information obtained by the FIU revealed that the beneficiaries of the trusts were individuals A and B, who were managers of two companies, established in Belgium that were the subject of a judicial investigation regarding serious tax fraud. Part of the funds in these trusts could have originated from criminal activity of the companies.

Indicators and methods identified in the scheme:

- **Instruments: wire transfers, real estate.**
- **Mechanisms: lawyer, trust, bank.**
- **Techniques: trust account, purchase of real estate, legal entity transactor, offshore, and incoming wire transfer.**
- **Opportunity taken: use of trusts to buy real estate. The trusts were used to conceal the identity of the true owners.**

Source: Belgium, 2005.

Shell Companies

30. A shell company is a company that is formed but which has no significant assets or operations, or it is a legal person that has no activity or operations in the jurisdiction where it is registered. Shell companies may be set up in many jurisdictions, including in certain offshore financial centres and tax havens. In addition, their ownership structures may occur in a variety of forms. Shares may be held by a natural person or legal entity, and they may be in nominative or bearer form. Some shell companies may be set up for a single purpose or hold just one asset. Others may be set up for a variety of purposes or manage multiple assets, which facilitates the co-mingling of legal and illicit assets.

31. The potential for anonymity is a critical factor in the use of shell companies. They may be used to hide the identity of the natural persons who are the true owners or who control the company.[15] In particular, permissive practices regarding the form of the shares, whether corporate, nominative or bearer, together with the lack of co-operation on the collection of information, represent a significant challenge when seeking to determine the ultimate beneficial owner.

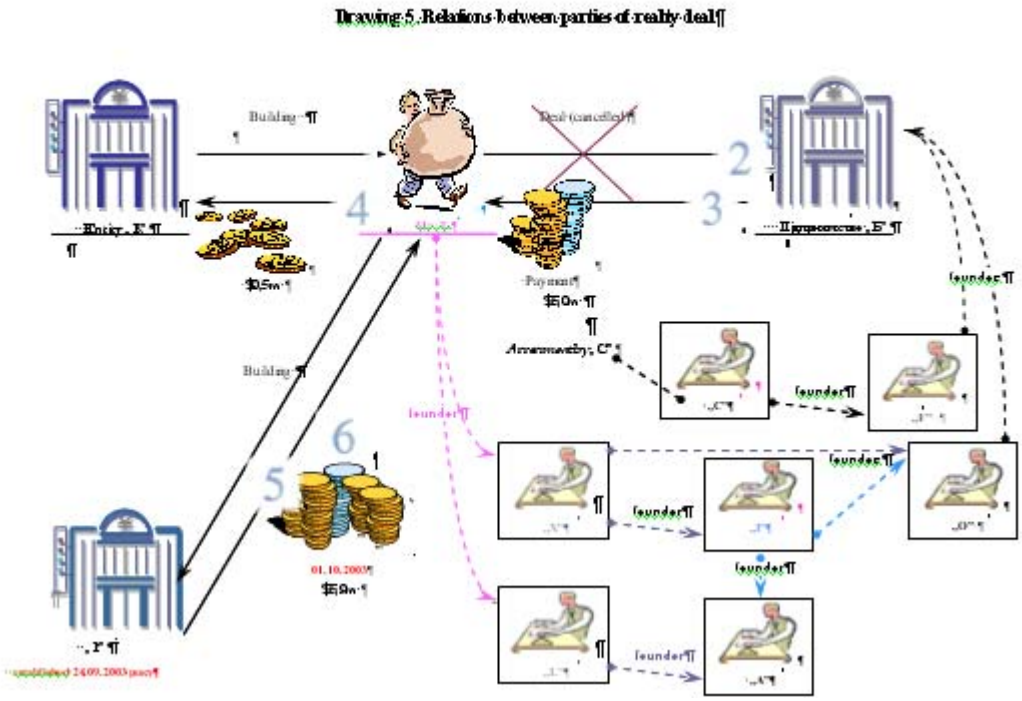
[14] However, it was pointed out in FATF (2006) that, in jurisdictions where trust administrators are licensed and regulated to ensure that they comply with FATF standards on knowing the beneficial owner, these difficulties might be able to be avoided.

[15] Commonly referred to as the *beneficial owner*.

Case study 3.3: Use of a shell company to buy real estate

This scheme involved the purchase of real estate, which was then sold for the higher price to the figureheads. In this case the financial intermediaries informed the financial intelligence unit (FIU) only about the transfer amount. To detect and investigate such cases it was therefore necessary to obtain information from relevant "gatekeepers", especially from registrars of real estate.

The case, investigated by Ukrainian FIU, started from the STR submitted by the auditor of the property buyer. Information was then received from the state registrar of real estate proprietors.



Entity P bought the building in the Ukrainian capital.
Entity K - first owner;
Mr. T - first buyer;
Entity B - next buyer. But the deal was cancelled in 3 months;
Entity P - new buyer.

Suspicion about the transaction was aroused because:

The selling price of building was 10 times higher then purchase price 3 days later.
The purchase price for Mr. T was determined based on the assessment of the state registrar of real estate.
The selling price was based on the assessment of private expert from entity C.
Mr. T did not have his own money. He would have had to work for 200 years to acquire this amount (USD 500 000) through his legal income. Nevertheless, on the day of payment, Mr. T received money from B as an advance for the same building.

In three months the deal with B was cancelled and the building was sold to P for USD 5.9 million. There are close relations between T, B and C, shown at the diagram. There was thus strong probability that the transfers of money to Mr. T were done for the purpose of laundering of USD 5.4 million.

Source: MONEYVAL (Ukraine).

Property Management Companies

32. When using the real-estate sector, the purchase or construction of properties is a commonly used means by which criminals carry out financial transactions. However, a property that is bought or constructed using illegally obtained funds may subsequently be rented out to provide an apparently

legal source of income in order to camouflage movements of funds between various jurisdictions (for example, the tenant and the landlord are located in different jurisdictions).

33. In cases where a company is owned or controlled by a criminal group, a possible way to use the property for money laundering is to mix cash of illegal origin with legitimate rental income. It then appears to be the result of the company's legitimate profits. In other cases, criminals seem to use the company's property management services to create a veil of legitimacy over other transactions they conduct. Those cases showed the active involvement of property management companies in criminal activity. The level of their participation can vary widely both in what kind of property is involved and how the property management company is being misused. The company may be an integral part of the organised criminal group or it may provide a part of the criminal business activity, fundamentally money laundering.[16]

Case study 3.4: Use of property management companies

(Predicate offence: suspected fraud)

The FIU received a suspicious transaction report from notary A on one of his clients, person B, a foreigner without an address in Belgium, who in his office had set up a company for letting real estate. The sole manager and shareholder of this company was a family member of B, who also resided abroad.

Shortly after its creation the company bought a property in Belgium. The formal property transfer was carried out at notary A's office. The property was paid for through the account of notary A by means of several transfers, not from company X, but from another foreign company about which individual B did not provide any details. The establishment of a company managed by a family member with the aim of offering real estate for let and paid by a foreign company disguised the link between the origin and the destination of the money.

Police intelligence revealed that the individual was known for financial fraud. The investment in the property was apparently financed by the proceeds of these funds.

Indicators and methods identified in the scheme:

- **Instruments: cash, wire transfers, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: business account, purchase of real estate, transactor inconsistencies, non-resident customer, unknown source.**
- **Opportunity taken: the establishment of a company managed by a family member with the aim of letting real estate paid by a foreign company disguised the link between the origin and the destination of the money**

Source: Belgium, 2005.

Non-trading real estate investment companies[17]

34. Several characteristics of these companies make them especially vulnerable to abuse by suspected criminals. First, it is often very difficult to identify the real owner or controller. Second, the company can be created very easily with no minimum initial capital and without an authentic deed. Additionally, these entities are only recorded at the trade register. Finally, the shares of such companies can be sold without certification so that the true owner is not easily identified.

16 See Serious Organised Crime Agency (2006).

17 Also known by its French acronym, *SCI* or *société civile immobilière*.

Case Study 3.5: Misuse of *non trading real estate investment companies*

(Predicate offence: suspected organised criminal activities)

Two French non-trading real estate investment companies managed by two residents of a western European country successively bought two high value properties for a significant amount (more than EUR 20 million) with a single payment (not a loan).

The analysis of the FIU revealed that beneficial owner of the two properties was a resident of an Eastern European country. Further analysis showed that offshore Company A had moved the funds used to purchase the properties through SWIFT wire transfers. This offshore company was well known for holding shares of Company B registered in the very same country as the beneficial owner of the properties. Company B itself was known for its links to organised crime. Analysis also showed that the two managers of the real estate investment companies were senior staff of Company B.

Indicators and methods identified in the scheme:

- **Instrument: real estate, single payment.**
- **Mechanisms: bank, *société civile immobilière* (SCI).**
- **Techniques: purchase of real estate, French SCI and foreign/offshore companies as intermediary, high value, physical intermediaries linked to the beneficial owner.**
- **Opportunity taken: the FIU analysis revealed that the 2 managers of the French SCI were linked to the beneficial owner through a company owned by him and in which the two managers had senior responsibilities**

Source: France, 2006.

Typology 4: Manipulation of the Appraisal or Valuation of a Property

35. Manipulation of the real value of properties in relation to real estate involves the overvaluing or undervaluing of a property followed by a succession of sales and purchases. A property's value may be difficult to estimate, especially in the case of properties that might be considered atypical, such as hotel complexes, golf courses, convention centres, shopping centres and holiday homes. This difficulty further facilitates the manipulation when such property is involved.

Over-valuation or Under-valuation

36. This technique consists of buying or selling a property at a price above or below its market value. This process should raise suspicions, as should the successive sale or purchase of properties with unusual profit margins and purchases by apparently related participants.

37. An often-used structure is, for example, the setting up of shell companies to buy real estate. Shortly after acquiring the properties, the companies are voluntarily wound up, and the criminals then repurchase the property at a price considerably above the original purchase price. This enables them to insert a sum of money into the financial system equal to the original purchase price plus the capital gain, thereby allowing them to conceal the origin of their funds.

Successive Sales and Purchases

38. In the case of successive sales and purchases, the property is sold in a series of subsequent transactions, each time at a higher price. Law enforcement cases have shown that these operations also often include, for example, the reclassification of agricultural land as building land. The sale is therefore fictitious, and the parties involved belong to the same criminal organisation or are non-financial professionals in the real-estate sector who implicitly know the true purpose of the transactions or unusual activity.

39. In addition to placing obstacles to discovering the true identity of the owners of the property and the real origin of the funds used in the transaction, these constructs usually also have a significant tax impact, as they generally avoid the liability for capital gains tax.

Case study 4.1: Use of a lawyer when buying a real estate.

(Predicate offence: suspected organised crime activity)

A lawyer created several companies the same day (with ownership through bearer shares, thus hiding the identity of the true owners). One of these companies acquired a property that was an area of undeveloped land. A few weeks later, the area was re-classified by the town hall where it is located so that it could be urbanised.

The lawyer came to the Property Registry and in successive operations, transferred the ownership of the property by means of the transfer of mortgage loans constituted in entities located in offshore jurisdictions.

With each succeeding transfer of the property, the price of the land was increased. The participants in the individual transfers were shell companies controlled by the lawyer. Finally the mortgage was cancelled with a cheque issued by a correspondent account. The cheque was received by a company different from the one that appeared as acquirer on the deed (cheque endorsement). Since the company used a correspondent account exclusively, it can be concluded that this company was a front company set up merely for the purpose of carrying out the property transactions.

After investigation it was learned that the purchaser and the seller were the same person: the leader of a criminal organisation. The money used in the transaction was of illegal origin (drug trafficking). Additionally, in the process of reclassification, administrative anomalies and bribes were detected.

Indicators and methods identified in the scheme:

- **Instruments: cheques and cover payments.**
- **Mechanisms: correspondent bank accounts.**
- **Techniques: business account, front company customer, purchase of real estate, cross border transaction, incoming wire transfer, reverse/flip real estate, unknown source.**
- **Opportunity taken: use of a lawyer when buying real property and performing bank transactions through correspondent bank accounts. Since the correspondent bank account was not used for any other transaction, it can be deduced that the lawyer set up the correspondent account for the purpose of carrying out the property transactions.**

Source: Spain, 2006.

Typology 5: Monetary Instruments

40. The use of monetary instruments in real estate transactions has traditionally dealt primarily with the use of cash. Although methods of payment continue to evolve, cash continues to be one of the main ways of obtaining and handling funds at the early stages of the process in many of the cases that ultimately involve funds of illegal origin.

41. Other monetary instruments used by criminals in their real-estate activities are cheques and wire transfers through conduit or correspondent bank accounts.

Cash

42. The purchase of high-value properties in cash is one way in which large sums of money can be integrated into the legal financial system. Some jurisdictions have observed that there has been a marked increase in demand for high denomination banknotes in their territory, which seems to be inconsistent with the progressive change in public preferences towards other means of payment. Specific geographic and financial concentrations of demand and cross-border movements have also been detected (specific locations, banks, ports, etc.). Although this demand also arises for reasons not strictly considered to be money laundering or terrorist financing activities, such as tax avoidance, evasion or fraud, it does seem to be clear that the real estate sector may be a key contributing factor in the increase in this demand for some jurisdictions, as the black economy tends to grow during a property boom.

43. As well as being used to buy real estate, cash is also used in currency exchange and to structure deposits. It is common to structure cash transactions involving funds from criminal or terrorist sources and then to use these funds to buy, build or renovate a property. When the improved property is finally

sold, the transaction has the advantage that it is difficult, or even impossible, to relate it to a specific individual or a criminal activity.

44. Cash is also used in rental or financial leasing transactions.[18] These processes may be used by money launderers or terrorists to obtain the use of a property without having to fear losing it through its being seized or frozen if their criminal activity is discovered by the authorities. Moreover, it can also be used directly by criminals to settle contracts close to the start of the operation, receiving a reimbursement from the leasing company in the form of a cheque, for example, thus giving the transaction an air of legitimacy. It should be noted that this analysis found that a large share of the market remains in the hands of legal entities which are independent from the banks and financial institutions, thus creating a different channel for funds and making investigation and analysis difficult given the fragmentation of the information.

Case study 5.1: Use of cash to buy real estate

(Predicate offence: drug trafficking)

A criminal organisation operating in the Americas and Europe, laundered resources generated from drug trafficking through the misuse of bureaux de change and exploitation of apparently legitimate real-estate businesses in different countries. The criminal organisation led by Mr. B, sent cocaine from South America to Europe, disguising it in rubber cylinders that were transported by air. The money generated from the trafficking was collected in Europe and forwarded in the same way back across the Atlantic.

In Latin-American Country 1, Mr B acquired an existing bureau de change; he changed its name and became its main shareholder and general director. With the purchase of an already constituted financial institution, the criminal organisation avoided the strict controls implemented by the regulatory authorities as regards to the constitution and operation of financial entities.

In European country 2, the criminal organisation acquired commercialisation companies, created real estate corporations managed by citizens of Latin-American Country 1 and opened bank accounts in various financial institutions, declaring as commercial activity trading in jewels, financial intermediation and real estate activities, among others.

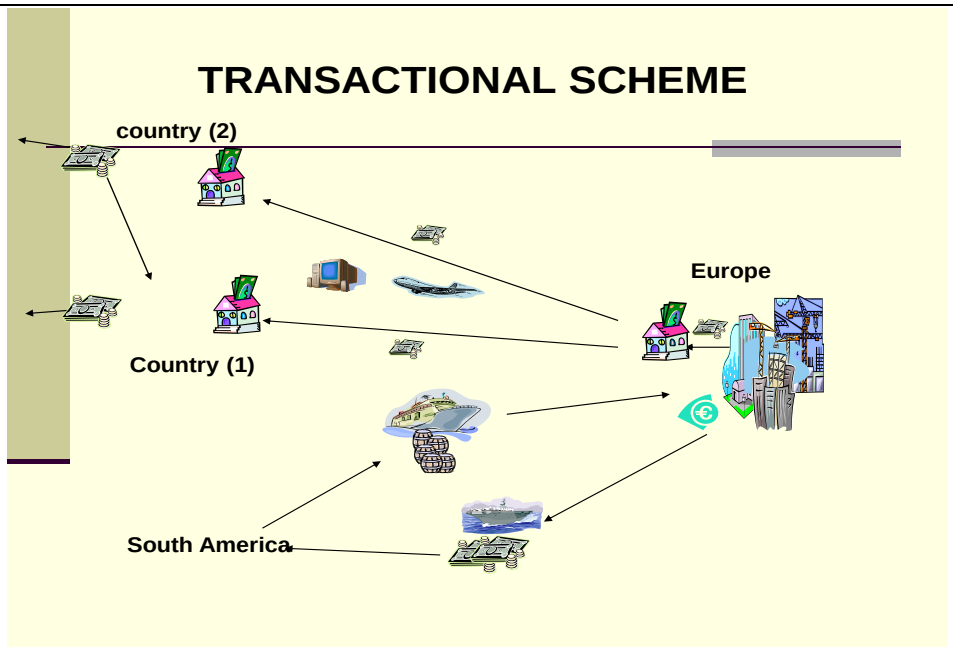
Those companies performed unusual transactions, such as cash deposits in amounts above EUR 500,000 and immediate transfer orders for the same amounts to foreign accounts belonging to Mr. B's bureau de change in Latin-American Country 1 and American Country 2; allegedly for investments in the real-estate sector; money was deposited in low denomination currency and some counterfeit notes were identified as well.

Intelligence information revealed that the account of the bureau de change located in American Country 2, received during a year and a half period, deposits for more than USD 160 million.

Indicators and methods identified in the scheme:

- **Maritime exportation of drugs from America to Europe and cash imports trough the same route.**
- **Incorporation of jewellery and real-estate companies in Europe, managed by citizens of Latin-American Country 1 to launder the money generated from drugs trafficking.**
- **Acquisition of an existing bureau de change in Latin-American Country 1, opening several bank accounts located in Latin-American Country 1, American Country 2 and Latin-American Country 3.**
- **Cash deposits in amounts above EUR 500 000 on behalf of the real state corporations located in Europe and immediate transfer orders for the same amounts to foreign accounts belonging to Mr. B's bureau de changeg in Latin-American Country 1 and American Country 2; allegedly for investments in real state sector.**
- **Intelligence information revealed that the account of the exchange house located in American Country 2, received during a year and a half period, more than USD 160 million.**
- **No continuity in the resources in the accounts.**

[18] Leasing is considered to mean contracts with the sole purpose of granting the use of real property purchased for this purpose in accordance with the specifications of the future user, in exchange for consideration in the form of the periodic payment of instalments to recoup the cost of the asset, excluding the value of the purchase option and financial charges. Leased goods must be used by the user solely for his business purposes. A financial leasing contract must include a purchase option in favour of the user at the end of the lease.



Source: Mexico.

Cheques and Wire Transfers

45. A number of cases revealed that criminals frequently use what might be termed *payable-through accounts* to channel large sums of money, generally through a series of transactions. In many cases sums are initially paid into these accounts in cash, cheques or via international wire transfers. The money never stays in the account for long, the rate of turnover of the funds is high, and the funds are then used to purchase real estate. There would appear to be no commercial or economic justification for using these accounts. The same could apply to correspondent accounts when used as transit account. Suspicion about a legitimate use can be appropriate, when the account has high turnover, it appears to deal exclusively with wire transfer payments (MT 103 plus MT 202 messages) or cheques and the account appears to have no commercial or economic justification for such use.

46. Analysis of the accounts in the cases studied often showed that they were opened for the sole purpose of conducting transactions and operations of this type. The basic purpose of the operation was, as always, to conceal the true origin of the funds and their ownership.

Case study 5.2: Use of a transit account to buy real estate and launder the funds from human being trafficking

(Predicate offence: suspected trafficking in human beings)

A bank's suspicions were raised after a bank cheque was issued to the order of a notary upon request of an Asian national for purchasing real estate. Analysis of the account transactions showed that the account received several transfers from Asians residing abroad and was known through an investigation regarding a network of Asian immigrants.

The analysis showed that the account had been used as a transit account by other Asian nationals for the purchase of real estate.

Indicators and methods identified in the scheme:

- **Instruments: wire transfers, cheques, real estate.**
- **Mechanisms: notary, bank.**
- **Techniques: personal account, purchase of real estate, transit account, incoming wire transfer.**
- **Opportunity taken: use of a transit account by non resident nationals for purchasing real estate.**

Source: Belgium, 2005

Typology 6: Mortgage Schemes

47. Mortgage loans comprise one of the main assets on the balance sheets of banks and other financial institutions. An inherent risk in this activity arises from the fraudulent or criminal use of these products. Through this misuse of the mortgage lending system, criminals or terrorists mislead the financial institution into granting them a new mortgage or increasing the amount already lent. This use constitutes, in the majority of the cases analysed, a part of the financial construction established to carry out criminal activities.

48. It was observed in many instances that financial institutions consider these mortgage products to be low risk. A risk-based approach to monitoring subjects related to money laundering and terrorist financing, similar to those based on customer due diligence or "know your customer" principles, could mitigate some of the risk of this activity.

Illegal Funds in Mortgage Loans and Interest Payments

49. Illicit actors obtain mortgage loans to buy properties. In many cases, illegal funds obtained subsequently are used to pay the interest or repay the principal on the loan, either as a lump sum or in instalments. The tax implications of using these products should also not be overlooked (for example, eligibility for tax rebates, etc.).

50. Front men are also sometimes used to buy properties or to apply for mortgages. The analysed cases seem to indicate that this misuse of mortgages goes hand in hand with a simulated business activity and the related income so as to deceive the bank or other financial institution when applying for the mortgage. On occasion the property is apparently purchased as a home, when in reality it is being used for criminal or terrorist activities (for example, selling or storing drugs, hiding illegal immigrants, people trafficking, providing a safe house for members of the organisation, etc.).

Case study 6.1: Use of illegal funds in mortgage loans and interest payments

(Predicate offence: forgery, deception, fraud, money laundering)

An individual used a front-man to purchase real estate. The value of the real estate was manipulated by using a licensed assessor (realestate agent) to set up a false higher but plausible assessment of the market value of the property after renovation. The bank was willing to grant a mortgage on the basis of this false assessment. After the disbursement of the loan the real estate was paid for. The remaining money was then transferred by the owner to bank accounts in foreign jurisdictions with strict bank secrecy. The renovation took never place. The company finally went into default and the loan could not be reimbursed.

A more detailed version of this scheme (describing all steps in the process) is included in Annex C.

Indicators and methods identified in the scheme:

- **Applying for a loan under false pretences.**
- **Using forged and falsified documents.**
- **The client persisted in representing his financial situation in a way that was unrealistic or that could not be supported by documents.**
- **The loan amount did not relate to the value of the real estate.**
- **Successive buying and selling transactions of the real estate were involved.**
- **The client had several mortgage loans concerning several residences**

Source: Netherlands.

Under-valuation of Real Estate

51. Illicit actors often omit a part of the price from the purchase contract. In other words, the amount listed on the contract of sale is less than the real purchase price paid. The price shown on the contract is paid for with a mortgage loan; whereas the part not appearing on the contract is paid in cash

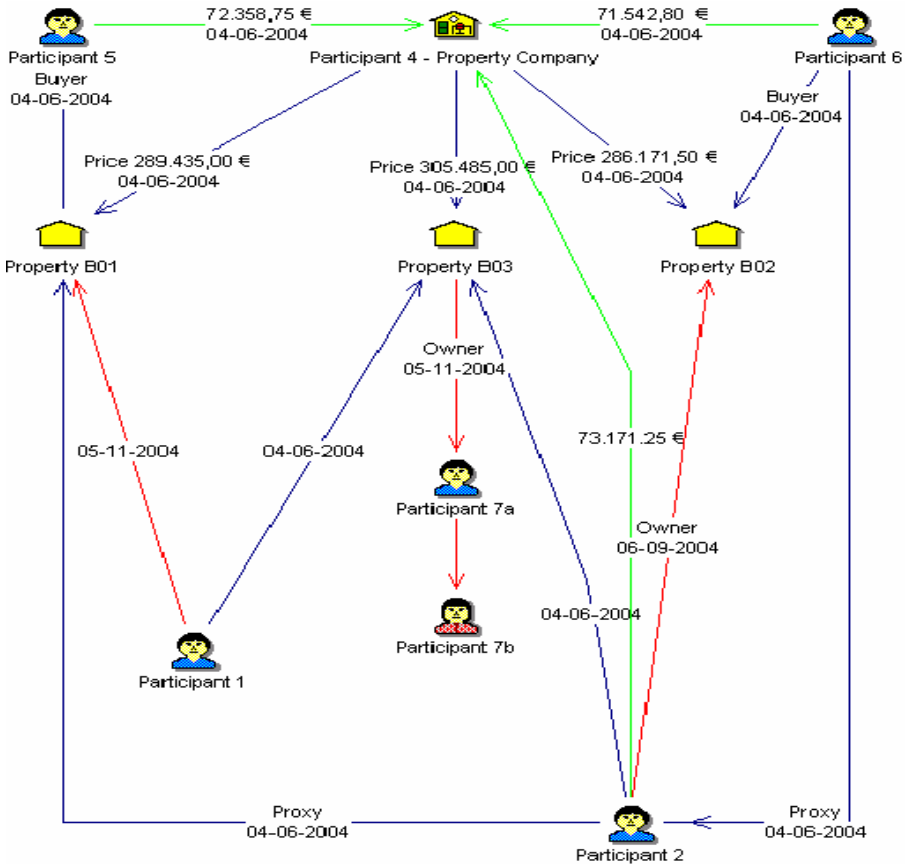
produced by the criminal organisation or terrorist group's criminal activities and is paid to the seller under the table.

52. When the property is sold at fair market price the illicit actor converts illegal income into seemingly legitimate profits. The proceeds might remain available in the bank account of the criminal organisation or terrorist group in the jurisdiction in which the property is located and thus constitute a critical starting point for an investigation.

53. If the criminal organisation or terrorist group is unable to find a seller willing to accept money under the table or is unable to influence the valuation of the property by the independent appraiser, it may still pay for part of the price set in the contract in cash from illegal activities, with a sum of money left over from not using the whole of the mortgage granted to it. In all these scenarios, it should be obvious to the bank or other financial institution that part of the purchase price is being paid via an alternative route, and it should verify whether this is consistent with the known profile of the customer in relation to the customer's pattern of income and expenses.

Case 6.2: Undervaluation of real estate in a terrorist financing scheme

(Predicate offence: money laundering, terrorist financing, manipulation of the appraisal of a property)



The authorities in Country A became aware, during the investigation of the finances of a terrorist organisation in Country B, that the police in Country B had searched the offices of real-estate agents allegedly used by the terrorist group to conceal funds by buying property.

It was found that the owners of the real-estate agents had conducted various real-estate transactions in Country A, either directly or as proxies, using the services of a law firm which had placed its own structure of bank accounts at the disposal of the parties under investigation. Both the law firm and the bank at which it held its accounts were located in Country A.

There was information in Country A regarding the involvement of participants 1 and 2 in the purchase of three properties. On a single day in 2005, Participants 1 and 2 made three deposits of EUR 3 210 each as down-payments to reserve properties in a residential complex in a coastal region of Country A for subsequent purchase. These properties were being built by the property company (Participant 4). Three un-notarised contracts of sale were signed by the property company and Participant 2, acting on his own behalf and as the verbal proxy of the purchasers (Participants 5, 6, 7). On the same day, Participant 1 transferred EUR 210 000 into the current account held by the law firm in Country A (Participant 3).

Three bank drafts were requested, for the sums of EUR 69 000, EUR 68 000, and EUR 73 000, with the funds being drawn from the law firm's current account. These were used to make the first payment against the contract of sale, which named the purchasers and set the final price.

Subsequently, after signing the property transfer documents before a notary in Country A, various assignments were made in the un-notarised contracts of sale that made changes to the final ownership of the properties:

○ Participant 1 ultimately bought property B01, and parking space 01.
○ Participant 2 ultimately bought property B02, and parking space 02.
○ Participants 6 and 7 ultimately bought property B03, and parking space 03.

The law firm (Participant 3) undertook all the legal formalities and attended the signing of the transfer documents and acted as a translator for the purchasers.

To reconstruct the route taken by the funds used to buy the properties and to be reasonably sure of the origin of this money a number of obstacles had to be overcome. The first obstacle was the use of the bank drafts received by the property company in Country A (Participant 4) in each case. Bank drafts were used for the initial payments against the un-notarised contracts and the final payments before signing the deeds[19].

These bank drafts were issued by the main office located near the properties and the relevant funds deducted from current account held by the law firm (Participant 3). Funds transfers were paid into this current account. On some occasions these referred to a person’s name and in others a generic sender.

In the case of the property eventually purchased by Participant 1, at the time of signing the property transfers two certificates issued by a financial institution were submitted, certifying that the funds with which the property was being bought belonged to a non-resident in Country A.

The law firm (Participant 3) stated that at the time of agreeing to act as an advisor to Participant 1 that it knew Participant 1 to be a real-estate agent in Country B and that it was working for third parties who were interested in making investments in Country A, and that for this reason it was unaware of the origin of the funds being paid into its account for the transactions in which it was acting as an intermediary on behalf of Participant 1.

Examining each of the legal and financial transactions described above on their own there does not appear, at first glance, to be any suspicious activity. However, a look at the overall operation provides an argument for the conclusion that the people investigated and the law firm (Participant 3) were facilitating real-estate investments in Country A while hiding the origin of the funds and their true owner.

The purchase of the three properties was designed as a single transaction from the outset:

○ The deposits were paid on the same date, as were the contracts of purchase with the property company (Participant 4) in Country A, and they were all signed by Participant 2.

○ The funds used to make the first payments arrived in a single transfer, against which three bank drafts were requested. These drafts had sequential serial numbers.

○ The three transactions have the same legal structure: payment of the deposit, un-notarised contract of sale, assignment of rights to a second purchaser by means of an un-notarised contract, and deed of sale in the name of a person other than the one who had initially signed the contract with the property company (Participant 4) in Country A.

○ Various legal entities and natural persons acting on behalf of third parties intervened between the property and the final purchaser:

○ The law firm (Participant 3), which had as its client a real estate agent in Country B, carried out legal transactions on behalf of third parties.

[19] In the case of the property bought by Participant 2, it was impossible to obtain evidence of the means of payment used to make the final payment before signing the property transfer documents.

○ From the point of view of the property company, a law firm (Participant 3) and a property company in Country B were buying property on behalf of individuals who paid with bank drafts.

Indicators and methods identified in the scheme:

- **The property which Participants 1 and 2 (who were the managers of the property companies in Country B) were going to buy for themselves was finally assigned to third parties.**
- **The properties that certain third parties were initially going to buy were finally bought by Participants 1 and 2 for themselves.**
- **One of the managers of the property company in Country B, Participant 1, bought an option to buy a property for four times its value even though the property was virtually identical to another which he already had the right to purchase and which he had transferred to a third party at cost. This would imply a profit of >250% if this price was actually paid, although in the contract there is no reference to the form or date of payment.**
- **Participant 1 first bought his property and then one month later applied for a mortgage on it. This may either be for tax reasons or a sign that the funds with which he acquired the property were not his.**
- **In addition to the parties investigated (Participants 1 and 2), there is a thread running throughout the operation as analysed, namely the law firm (Participant 3):**
- **The law firm (Participant 3) placed its current account with a bank in Country A at the disposal of Participants 1 and 2 so that they could send funds, while knowing that as professionals in the property business that they could open non-resident accounts in Country A either in the name of the company for which they worked or in their own names.**
- **The participants also obtained bank drafts for the various payments arising out of the contracts they signed. The combination of the use of bank drafts and the current account of a law firm considerably complicated the task of tracking the funds with which the property was bought, as, starting with the property transfer documentation it is necessary to contact the seller to obtain the bank draft number, and then obtain information about the origin of the funds used to purchase the draft from the bank, to finally arrive at the law firm.**
- **Given the active participation of the law firm in all the legal transactions relating to the properties (from the signing of the first, un-notarised contracts of sale, through to the signing of the property transfer documents, in which the law firm was present to act as a translator for the final buyers) the contract transferring the right of purchase that Participant 1 obtained from the purchaser (Participant 5) for four times its value can only be interpreted as a transaction intended to provide the buyer (Participant 5), or others, with an apparently legitimate origin for at least EUR 200 000.**

Source: Spain 2006.

Over-valuation of Real Estate

54. Cases have also occurred in which illicit actors overvalued properties in order to obtain the largest possible mortgage. This over-valuation was achieved by manipulating the appraisal or by setting up a succession of purchases. Properties that have a more subjective valuation offer more scope for overvaluation, as is the case of hotel complexes, leisure centres, golf courses, restaurants, unique buildings, etc.

55. When applying for a mortgage, illicit actors often submit false documentation regarding the real value of the property underlying the operation. Additionally, they often use front men or corporate vehicles as a party to the mortgage agreement. The list of participants (for example directors, representatives, etc.) also changes frequently. On occasion, it has been noticed that some time after the mortgage was granted by the financial institution, the borrower defaulted on payment. When the bank tried to recover the debt from the front-man, it found that the latter did not know who was really behind the operation or where they might be located, leading to the debtor's being classified as insolvent. The same thing happens if the defaulter is a corporate vehicle.

Case 6.3: Overvaluation of real estate and used of third parties launder funds

(Predicate offence: money laundering, forged loan agreement)

The parents of Mr X (Mr and Mrs Y) purchased a residential property and secured a mortgage with a Canadian bank. In his mortgage application, Mr Y provided false information related to his annual income and his ownership of another property. The property he had listed as an asset belonged to another family member.

Mr and Mrs Y purchased a second residence and acquired another mortgage at the same Canadian bank. A large portion of the down payment came from an unknown source (believed to be Mr X). The monthly mortgage payments were made by Mr X through his father's bank account. This was the primary residence of Mr X. Investigative evidence shows that Mr X made all mortgage payments through a joint bank account held by Mr and Mrs Y and Mr X.

Mr X then purchased a residential property and acquired a mortgage from the same Canadian bank. Mr X listed his income (far higher than the amounts he had reported to Revenue Canada) from Company A and Company B. Mr X made the down payment and monthly payments. Over two years, Mr X paid approximately CAD 130 000 towards the mortgage. During this time his annual legitimate income was calculated to be less than CAD 20 000.

Mr X also used his brother Mr Z as a front man (nominee) on title to purchase an additional property. Investigators discovered that Mr Z had stated an annual income of CAD 72 000 on his mortgage application listing his employer as Mr X although Mr Z had never worked for his brother, and his total income for two years was less than CAD 13 000.

Mr X made the down payment on this property, and his tenants, who were members of Mr X's drug trafficking enterprise, paid all the monthly mortgage payments. A total of CAD 110 000 was paid towards this property until Mr X and his associates were arrested.

Mr X and his father purchased a fifth property. The origin of the down payment, made by Mr Y, was unknown but is believed to be the proceeds of Mr X's drug enterprise. Monthly payments were made by Mr X.

The use of real estate was one of many methods Mr X employed to launder the proceeds from his drug enterprise. Recorded conversations between Mr X and his associates revealed that he felt it was a fool-proof method to launder drug proceeds.

Mr X was convicted in 2006 of drug trafficking, possession of the proceeds of crime and laundering the proceeds of crime in relation to this case.

Indicators and methods identified in the scheme:

- **The use of real estate was one of many methods Mr X employed to launder the proceeds from his drug enterprise. Recorded conversations between Mr X and his associates revealed that he felt it was a fool-proof method to launder drug money.**
- **The only problem he faced was securing a mortgage alone, so he had to use a nominee to secure the mortgage or to co-sign on the mortgage. A problem surfaced in this investigation when various properties were sold prior to a restraint order being served. This resulted in a portion of the funds being secured in a lawyer's trust account, which could not be restrained. It was the investigator's belief that up to CAD 500,000 was being held in this trust account.**

Source: Canada 2006.

Typology 7: Investment Schemes and Financial Institutions

56. Direct or indirect investment in the real estate sector by banks and other financial institutions is significant.[20] However, the volume of investment by insurance companies and pension fund managers is also significant, as these institutions place a large part of their long-term liabilities in the property sector at both national and international levels. Bank and other financial institution investment policies demonstrate that investment in property is gaining ground relative to other direct investments.

[20] In the majority of countries, On the balance sheets of banks and financial institutions in most countries, the asset item referred to as credit investments mainly consists of mortgage lending transactions. This means that at times the evolution of the financial system is highly correlated with that of the real-estate sector.

57. Indirect investments are those considered to be limited or in which there is no direct control over the assets of the fund or investment vehicle. Moreover, real estate investment funds may or may not be publicly listed. If funds are unlisted it means that some or the entire fund or investment vehicle is capitalised by the financial institution. The number of co-investors generally ranges from two to ten.

58. The legal structures used for real estate investment funds vary:

- Investment trusts in the real estate sector, either listed or unlisted.[21]
- Companies operating in the real estate sector, either listed or unlisted.[22]
- Associations and unlisted limited companies.

59. A number of cases have revealed that criminal organisations can influence property investment funds in various ways, depending on their degree of involvement:

- Partners in limited companies.
- Co-investors in property investment funds.
- Managers with direct or indirect control over the investment decisions made by property investment funds.

60. Institutions frequently outsource the management of their real estate assets to advisors or intermediaries, who, if they are managers of assets held in trust, may also outsource this task. Thus, several counterparties may be involved in the investment process, beginning with the investment policy set by the financial institution and ending with the investment ultimately made. The criminal organisation or terrorist group may operate or be situated at any point along this chain.

61. Through investment schemes in the real estate sector, the bank or other financial institution may, whether wittingly or not, facilitate or involve itself or become a vehicle for third parties to launder money.

Case study 7.1: Investments in hotel complexes through a front-man

(Predicate offence: organised criminal activities)

On the French west seacoast, an individual presented a project to a district planning authority which involved several real-estate project management companies to develop a golf course with a hundred villas and apartments on property owned by the authority.

The total cost of the operation was very high and was to be funded mostly with funds originating from abroad. The analysis of the FIU revealed that the individual as well as close members of his family had already been involved in previous cases transmitted to the judicial authorities, in which the family had been implicated in the laundering of funds originating from Eastern Europe.

Indicators and methods identified in the scheme:

- **Instrument: real estate.**
- **Mechanisms: bank, district-planning authority, real-estate project management companies.**
- **Techniques: purchase of real estate, involvement of a natural person as an intermediary, high value.**
- **Opportunity taken: the FIU investigations revealed that this individual and members of his family had acted as a front-man for persons from Eastern Europe suspected of being linked with organised crime.**

Source: France, 2006.

[21] Known as *real estate investment trusts* (REITs) in the US and *property investment funds* (PIFs) in the UK.

[22] Known as *real estate operating companies* (REOC) in the US.

Typology 8: Concealing Money Generated by Illegal Activities

62. The use of real estate to launder money seems to afford criminal organisations a triple advantage, as it allows them to introduce illegal funds into the system, while earning additional profits and even obtaining tax advantages (such as rebates, subsidies, etc.).

63. Some areas within the real-estate sector are more attractive than others for money laundering purposes, since the financial flows associated with them are considerable. This makes the task of hiding the funds of illegal origin in the total volume of transactions easier. The real estate sector offers numerous possibilities for money laundering: hotel businesses, construction firms, development of public or tourist infrastructure (especially luxury resorts), catering businesses. It is worth highlighting that over the course of the study, trends in these activities were noticed that depend on different regional characteristics: for example, more cases occur in coastal areas, in areas with a pleasant climate, and where non-resident foreign nationals are concentrated, etc. It is also worth noting that countries which have regions of this kind are more aware of the problem and have increasingly begun to establish appropriate measures and controls in the real-estate sector.

Investment in Hotel Complexes, Restaurants and Similar Developments

64. Real estate is commonly acquired in what is known as the integration or final phase of money laundering. Buying property offers criminals an opportunity to make an investment while giving it the appearance of financial stability. Buying a hotel, a restaurant or other similar investment offers further advantages, as it brings with it a business activity in which there is extensive use of cash.

Case study 8.1: Purchase of real-estate in order to establish a restaurant

(Predicate offence: trafficking in illegal labour force)

An Asian national had purchased real estate in order to start a restaurant that he had financed by a mortgage at Bank A. This mortgage was repaid by transfers from an account opened with Bank B in name of his spouse. Within one year his spouse's account was credited by cash deposits and debited by cash withdrawals, as well as transfers to Bank A.

On the debit side of the account there were also various transfers to China in favour of a natural person. The repayment of the mortgage by transfers from an account opened with another bank in name of his spouse.

The main individual involved was known to be part of network that illegally smuggled foreign workers to Belgium.

Indicators and methods identified in the scheme:

- **Instruments: loan, wire transfer, cash, real estate.**
- **Mechanisms: bank.**
- **Techniques: personal account, purchase of real estate, physical person intermediary, cash deposit, withdrawal, outgoing wire transfer.**
- **Opportunity taken: repayment of the mortgage by transfers from an account opened with another bank in name of his spouse.**

Source: Belgium, 2004.

RED FLAG INDICATORS

65. Building on the cases and other information analysed, the participants in this study also identified a number of common characteristics that, when detected individually or in combination, might indicate potential misuse of the real estate sector for ML/TF purposes. These "red flag" indicators when available can assist financial institutions and others in the conduct of customer due diligence for new and existing clients. They also may help in performing necessary risk-analysis in the more general sense for the sector. Thus, valid indicators may help in identifying suspicious activity that should be reported to competent national authorities according to AML/CFT legislation.

66. The indicators developed by this study of the real estate sector are set out in Annex B. They are not intended to represent an exhaustive list of all the possible types of transactions that might be linked to money laundering or terrorist financing. Nor does it imply that the transactions listed are necessarily linked to such activities. It needs to be borne in mind that money laundering always aims to disguise itself as a "normal" transaction. The criminal nature of the activity derives from the origin of the funds and the aim of the participants.

67. Because the international standard in this field primarily focuses on prevention, it is essential to emphasise two types of measures: *i)* Detection of suspicious transactions before they are completed, so as to avoid the funds being fed into the system; and *ii)* analysis of these transactions in cases where it is impossible to detect suspicious activity in order to detect such activity in the future.

ISSUES FOR CONSIDERATION

68. Regarding the real estate sector, there are other issues for consideration apart from the ones previously mentioned that can play a key role in the process of detecting misuse within the sector as a way to channel illicit money. Additionally, all the concerns expressed in the report have policy implications which need to be considered by countries either at a national or international level.

69. This study of typologies should help to identify the weaknesses or loopholes in the prevention systems currently in place, and may lead to the setting up or development of measures to protect the sector from criminal activities linked to money laundering, and thus avoiding its becoming an attractive destination for money obtained from criminal sources.

70. It is therefore important to highlight that the preventive framework to which this report aims to contribute must be constructed in accordance with the preventive measures laid down in these practices or systems. In the same way, it must be pointed out that any relaxation of the controls on these practices or systems could represent an enormous boost to the success of investments in the real estate sector by criminals.

71. In this context, the FATF should play a central role – together with World Bank and International Monetary Fund – in helping develop appropriate measures in emerging markets, as a way to stop illegal money flows.

72. Finally, as the key parties to real estate transactions, DNFBPs need to be encouraged by organisations and legislators in the fight against ML/TF. Real estate agents in particular are involved in the vast majority of real estate transactions and therefore can play a key role in detecting money laundering and terrorist financing schemes. Although this research has demonstrated the growing use of emerging markets and new methods of payments to launder money or finance terrorism through the real estate sector, simpler schemes such as large cash transactions are still commonly used. Because they are in direct contact with buyers and sellers, real estate agents generally know their clients better than the other parties in the transactions. Therefore, they are well placed to detect suspicious activity or identify red flag indicators.

73. The FATF Recommendations recognise the importance of customer due diligence, record-keeping and reporting requirements for the real estate sector. To ensure effective compliance with these requirements, it is important that authorities inform the sector of its obligations and share sector-specific indicators with the industry.

74. Also, it was observed during the research for the project that wire transfers still constitute the best way to allocate money between countries. Although controls have been established within the financial sector and for certain actors within it, settlement systems are still not included in the ML/TF legislation in most countries.

75. Finally, as they are key figures within the real estate sector and its transactions, designated non-financial businesses and professions (DNFBPs) need to be encouraged by organisations and legislators to implement effective AML/CFT measures.

Emerging markets

76. The worldwide market growth of real estate-backed securities and the development of property investment funds has meant that the range of options for real estate investments has also grown. Emerging markets in particular can offer attractive returns at low prices with considerable room for growth. This has not gone unnoticed by many suspected criminals.

77. As a result of a the property boom in emerging markets, it has come to light that many money launderers believe that it is easier to camouflage genuine commercial transactions - funded by their illicitly obtained funds - among the huge number of transactions taking place. Complicating matters is the fact that often these less developed economies do not have an average market price for real estate but rather prices varying across sectors and districts. Examining each and every transaction is impossible, and obtain a clear valuation of its real price is therefore also impossible. At times this situation is made worse by the fact that the banking sector is insufficiently developed, in terms of its financial products and conditions, resulting in financial and company structures that make the tasks of supervision or investigation yet more difficult.

78. Emerging markets often contain several characteristics that are highly favourable for money laundering, including:

- A high level of state intervention as a result of private sector financial structures and banking systems still at the embryonic stage.
- Absence, or limited development, of AML/CFT legislation and absence of indicators of the seriousness and social impacts of these phenomena.
- Lack of foreign capital in sectors other than raw materials.
- Banking and competent authorities (*i.e.* police, tax authorities, courts, etc.) lack training and the means necessary to detect and combat money laundering and terrorist financing.

Wire transfers

79. This method is common to practically all the schemes analysed and is probably one of the most accessible and widely used methods by criminals. The growing introduction of new technologies in financial markets and their increasing globalisation have meant that borders are disappearing and there are fewer obstacles to both legal and illegal activities. It also needs to be borne in mind that as a result of their growing use, the regulatory standards applicable to the financial markets regarding these wire transfers are scant as regards preventing money laundering and terrorist financing, and focus almost exclusively on the standardisation of the data fields used in order to automate and speed up transactions.

80. It needs to be borne in mind that wire transfers can be performed by highly regulated financial institutions and also through by less regulated institutions, such as alternative remittance systems. We need to also include those institutions providing message services and settlement services (*e.g.* FEDWIRE, CHIPS, SWIFT, etc). Therefore differentiating between the providers of the activity on a risk based manner seems appropriate. Additionally, we need to take into consideration the system and instrument used in each institutions to perform their transactions in relation to the regulation level. It means that we need not only consider the institutional regulation, but also if the money flows go through saving accounts, correspondent accounts, cheques, etc that can be considered as wire transfers.

81. The minimal information customers are required to provide in some jurisdictions to prove their identity facilitates the abuse of the system by criminal organisations and terrorist groups by making it possible for them to be almost undetectable while moving large sums of money between countries in seconds. The speed of execution, whether in person or not, the minimal documentation required and the high level of anonymity mean that they are commonly used by money launders abusing these regulatory loopholes. The fact that in only a few countries wire transfer offices are being supervised and subject to anti money laundering and counter terrorist financing requirements, makes the offices even more vulnerable for misuse.

82. Wire transfer systems move billions every day in domestic and international transfers, and although some countries have introduced limited standards for their surveillance, they are extremely difficult to control. It may be concluded from the information compiled that there are no effective

international controls on wire transfers, particularly as regards international transfers. It would be worthwhile to look into the current standards for the category. It could be said that the reliable identification of the parties (payer, payee, etc.) in wire transfer is indispensable to any effective effort to combating money launderings.

Notaries, registrars and similar figures

83. As illustrated throughout this report, notaries and registrars seem to be the weakest link in the chain of real estate transactions, and they may be able to play a role in the detection of high risk transactions relating to the real estate sector. The importance of AML/CFT requirements for third parties has already been recognised by the FATF under Recommendation 9. Due to their central position in the legal system in relation to these real estate transactions, they could potentially also perform a role in centralising and filtering information. However according to the legal professions it is not clear what the boundaries are in complying with the requirements. The FATF is currently undertaking a dialogue with the legal professions and further work in guidance on the recommendation will be elaborated. Some FATF members have charged prevention bodies within the professional associations to which notaries and registrars belong with providing information to the authorities (both judicial and administrative) with powers in relation to money laundering and terrorist financing under the authority of national laws.

84. In countries where the legal professions are considered public servants, a possible solution would be that a system put in operation by notaries and registrars would encompass, in particular, the identification and analysis of patterns of transactions where there is a risk of their concealing money laundering or terrorist financing activities. These models should include mechanisms for notifying financial intelligence units, for example, of those cases in which the level of risk increases or does not decrease after analysis. On this basis, the co-operation of notaries and registrars in the fight against ML and TF would be more clearly supported. It should obviously be pointed out that only a small proportion of these transactions constitute or form part of real money laundering or terrorist financing activities, a conclusion which can only be reached by the competent authorities.

85. Some FATF members consider an overall database at the level of the professional association[23], which would include the majority of the details of all transactions authorised by a notary or registrar and thus serve as the central gathering point for information from these public servants. However, in establishing system like this, countries would also need to consider cost effectiveness and privacy protection issues. A series of risk templates could be applied to this database to extract the relevant information required automatically for subsequent analysis. Approaching openly these gatekeepers and raising awareness on their vulnerabilities and risks as regards to money laundering and or terrorism financing is crucial for the competent authorities in order to reinforce the preventive network against those offences.

[23] From the research, it was clear that, because of the complex nature of real estate transactions, authorities experience difficulties in getting a complete picture of the role played by a person in the financial system. The nationwide database of financial products through which the authorities would be able to locate accounts and other products and then approach the relevant financial institution or other actors in the sector to seek more information through appropriate investigative or judicial means could help in this regard to provide a more complete picture.

ANNEX A - TERMINOLOGY[24]

Beneficial owner: This term refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. As used in this study, the term *beneficial owner* applies as well to the true owner of real property.

Instrument – An ML/TF *instrument* is an object of value (or one which represents value) that in some way or other is used to carry out ML/TF activity. Examples of ML/TF *instruments* include cash funds, cheques, travellers' cheques, precious metals or stones, securities, real property, etc.

Legal arrangements – This term refers to express trusts or other similar structures, such as (for AML/CFT purposes) the *fiducie*, *Treuhand* and *fideicomiso*.

Legal persons – A legal person is a corporate body, foundation, Anstalt, partnership or association, or any similar entities that can establish a permanent customer relationship with a financial institution or otherwise own real property.

Mechanism – An ML/TF *mechanism* is a system or element that carries out part of the ML/TF process. Examples of ML/TF *mechanisms* include financial institutions, money remitters, legal entities and legal arrangements, etc.

Method – In the ML/TF context, a *method* is a discrete procedure or process used to carry out ML/TF activity. It may combine various techniques, mechanisms and instruments, and it may or may not represent a typology in and of itself.

Scheme – An ML/TF *scheme* is a specific operation or case of money laundering or terrorist financing that combines various methods (techniques, mechanisms and instruments) into a single structure.

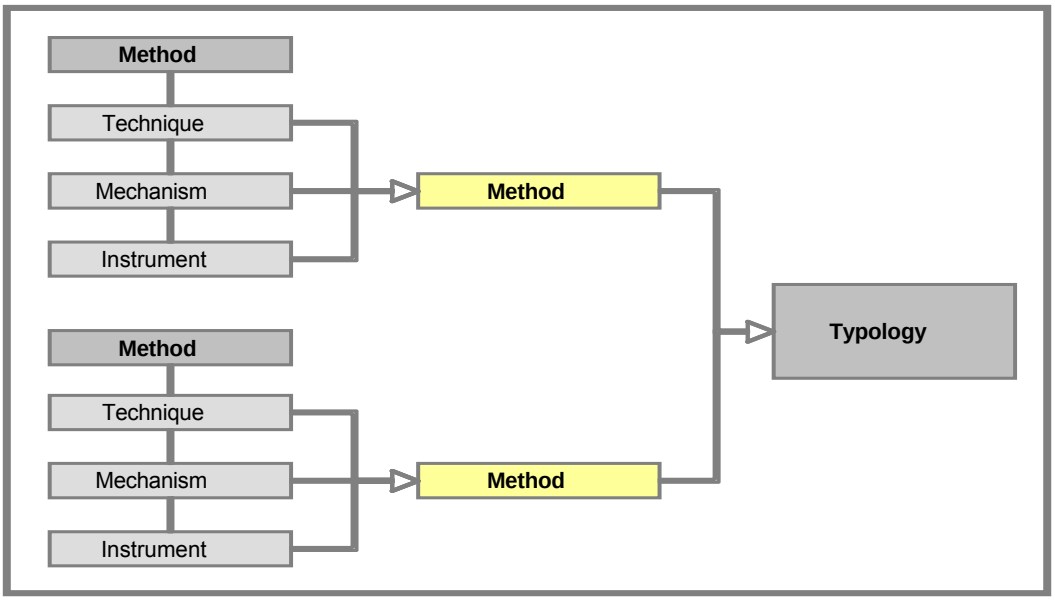
Technique – An ML/TF *technique* is a particular action or practice for carrying out ML/TF activity. Examples of ML/TF *techniques* include structuring financial transactions, comingling of legal and illegal funds, over- and under- valuing merchandise, transmission of funds by wire transfer, etc.

Trust and Company Service Provider (TCSP): This term refers to all persons or businesses that specialise in acting as a formation agent of legal persons for third parties. For a fuller definition of this type of activity, see the "Glossary" to the *FATF 40 Recommendations*.

Typology – An ML/TF *typology* is a pattern or series of similar types of money laundering or terrorist financing schemes or methods.

This report uses the terminology commonly used by the FATF in its typologies analysis. The following figure illustrates the relationship between the various elements of typologies analysis.

[24] Sources used for these terms include FATF (2003), FATF (2004) and FATF (2005).


Method
Technique
Mechanism
Instrument
Method
Method
Technique
Mechanism
Instrument
Method
Typology

ANNEX B - RED FLAG INDICATORS

Building on the cases and other information analysed, the participants in this study also identified a number of common characteristics that, when detected individually or in combination, might indicate potential misuse of the real estate sector for ML/TF purposes. These "red flag" indicators when available can assist financial institutions and others in the conduct of customer due diligence for new and existing clients. They also may help in performing necessary risk-analysis in the more general sense for the sector. Thus, valid indicators may help in identifying suspicious activity that should be reported to competent national authorities according to AML/CFT legislation.

These indicators are not intended to represent an exhaustive list of all the possible types of transactions that might be linked to money laundering or terrorist financing. Nor should it in any way be implied that the transactions listed here are *necessarily* linked to such activities. It should be remembered that activities related to money laundering or terrorist financing are always carried out with the aim of appearing to be "normal". The criminal nature of the activity derives from the origin of the funds and the aim of the participants.

Natural persons

- Transactions involving persons residing in tax havens or risk territories[25], when the characteristics of the transactions match any of those included in the list of indicators.
- Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases.
- Transactions involving persons who are being tried or have been sentenced for crimes or who are publicly known to be linked to criminal activities involving illegal enrichment, or there are suspicions of involvement in such activities and that these activities may be considered to underlie money laundering
- Transactions involving persons who are in some way associated with the foregoing (for example, through family or business ties, common origins, where they share an address or have the same representatives or attorneys, etc.).
- Transactions involving an individual whose address is unknown or is merely a correspondence address (for example, a PO Box, shared office or shared business address, etc.), or where the details are believed or likely to be false.
- Several transactions involving the same party or those undertaken by groups of persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Individuals who unexpectedly repay problematic loans or mortgages or who repeatedly pay off large loans or mortgages early, particularly if they do so in cash.

[25] The definition of a risk territory could be either one that is determined by the financial institution or another entity applying the indicator directly or else one that has been defined by the national authorities of the country in which the institution or entity is located.

Legal persons

- Transactions involving legal persons or legal arrangements domiciled in tax havens or risk territories, when the characteristics of the transaction match any of those included in the list of indicators.
- Transactions involving recently created legal persons, when the amount is large compared to their assets.
- Transactions involving legal entities, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity.
- Transactions involving foundations, cultural or leisure associations, or non-profit-making entities in general, when the characteristics of the transaction do not match the goals of the entity.
- Transactions involving legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Transactions involving legal persons whose addresses are unknown or are merely correspondence addresses (for example, a PO Box number, shared office or shared business address, etc.), or where the details are believed false or likely to be false.
- Various transactions involving the same party. Similarly, transactions carried out by groups of legal persons that may be related (for example, through family ties between owners or representatives, business links, sharing the same nationality as the legal person or its owners or representatives, sharing an address, in the case of legal persons or their owners or representatives, having a common owner, representative or attorney, entities with similar names, etc.).
- Formation of a legal person or increases to its capital in the form of non-monetary contributions of real estate, the value of which does not take into account the increase in market value of the properties used.
- Formation of legal persons to hold properties with the sole purpose of placing a front man or straw man between the property and the true owner.
- Contribution of real estate to the share capital of a company which has no registered address or permanent establishment which is open to the public in the country.
- Transactions in which unusual or unnecessarily complex legal structures are used without any economic logic.

Natural and legal persons

- Transactions in which there are signs, or it is certain, that the parties are not acting on their own behalf and are trying to hide the identity of the real customer.
- Transactions which are begun in one individual's name and finally completed in another's without a logical explanation for the name change. (For example, the sale or change of ownership of the purchase or option to purchase a property which has not yet been handed over to the owner, reservation of properties under construction with a subsequent transfer of the rights to a third party, etc.).
- Transactions in which the parties:
  - Do not show particular interest in the characteristics of the property (*e.g.* quality of construction, location, date on which it will be handed over, etc.) which is the object of the transaction.
  - Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms.
  - Show a strong interest in completing the transaction quickly, without there being good cause.

  - Show considerable interest in transactions relating to buildings in particular areas, without caring about the price they have to pay.
- Transactions in which the parties are foreign or non-resident for tax purposes and:
  - Their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying, even temporarily, etc.).
  - They are interested in large-scale operations (for example, to buy large plots on which to build homes, buying complete buildings or setting up businesses relating to leisure activities, etc.).
- Transactions in which any of the payments are made by a third party, other than the parties involved. Cases where the payment is made by a credit institution registered in the country at the time of signing the property transfer, due to the granting of a mortgage loan, may be excluded.

Intermediaries

- Transactions performed through intermediaries, when they act on behalf of groups of potentially associated individuals (for example, through family or business ties, shared nationality, persons living at the same address, etc.).
- Transactions carried out through intermediaries acting on behalf of groups of potentially affiliated legal persons (for example, through family ties between their owners or representatives, business links, the fact that the legal entity or its owners or representatives are of the same nationality, that the legal entities or their owners or representatives use the same address, that the entities have a common owner, representative or attorney, or in the case of entities with similar names, etc.).
- Transactions taking place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.

Means of payment

- Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction.
- Transactions in which the party asks for the payment to be divided in to smaller parts with a short interval between them.
- Transactions where there are doubts as to the validity of the documents submitted with loan applications.
- Transactions in which a loan granted, or an attempt was made to obtain a loan, using cash collateral or where this collateral is deposited abroad.
- Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments, or where payment is made by endorsing a third-party's cheque.
- Transactions with funds from countries considered to be tax havens or risk territories, according to anti-money laundering legislation, regardless of whether the customer is resident in the country or territory concerned or not.
- Transactions in which the buyer takes on debt which is considered significant in relation to the value of the property. Transactions involving the subrogation of mortgages granted through institutions registered in the country may be excluded.

Nature of the Transaction

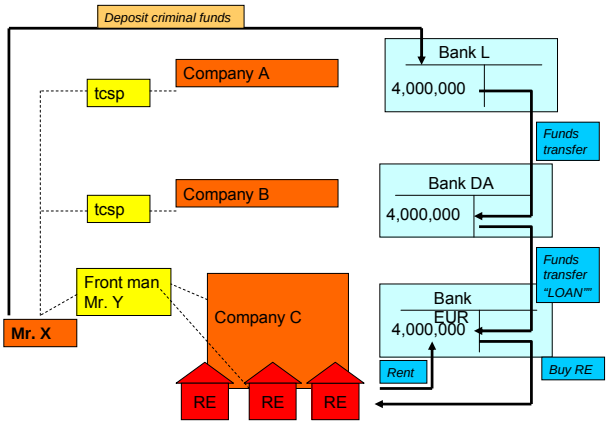
- Transactions in the form of a private contract, where there is no intention to notarise the contract, or where this intention is expressed, it does not finally take place.
- Transactions which are not completed in seeming disregard of a contract clause penalising the buyer with loss of the deposit if the sale does not go ahead.
- Transactions relating to the same property or rights that follow in rapid succession (for example, purchase and immediate sale of property) and which entail a significant increase or decrease in the price compared with the purchase price.

- Transactions entered into at a value significantly different (much higher or much lower) from the real value of the property or differing markedly from market values.
- Transactions relating to property development in high-risk urban areas, in the judgement of the company (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).
- Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics.
- Recording of the declaration of a completed new building by a non-resident legal person having no permanent domicile indicating that the construction work was completed at its own expense without any subcontracting or supply of materials.
- Transactions relating to property development in high-risk urban areas based on other variables determined by the institution (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).

ANNEX C – COMPLETE CASE STUDIES FOR TYPOLOGIES 1 AND 6

Case Study 1.1: Proceeds of drug trafficking laundered into real estate

Mr. X deposited money earned from drug activities into Company A's account at offshore Bank L. Mr. X set up Company A in order to disguise his identity and to place his criminal funds the bank under false pretences. Mr. X also held **bearer shares** issued by Company A., Mr X. established Company B in another offshore jurisdiction under the same circumstances.



Mr X was shareholder of Company A and B but was not registered as such in the public registers. Mr. X made use of a local trust in each location and gave them power-of-attorney to act as his legal representative (through a trust and company service provider: **TCSP**). The local trusts opened accounts at Bank L and at Bank DA on behalf of Company A and Company B respectively. The trusts explained to the banks that the companies that they represented were part of an international structure and that they wanted to benefit from favourable tax arrangements by means of **inter company loans**. This was the reason given for frequent debits and credits of the accounts for incoming and outgoing foreign funds transfers.

Mr X set up Company C in the European country where he is living. Mr. X is the owner of Company C; however, he uses a **front-man**, Mr Y, who is the owner and manager according to the public register at the Chamber of Commerce and the shareholder register. Company C conducted legal counselling activities. This way Mr. X was able to monitor and control the activities in Company C without becoming known to the authorities. Mr Y opened accounts on behalf of Company C with Bank EUR.

Mr X used Companies A, B and C to set up a **loan-back scheme** in order to transfer, layer and integrate his criminal money. The criminal funds, initially placed in the account of Company A in a bank in an offshore jurisdiction, were ultimately invested into real estate in Europe. The real estate was used to expand his legal counselling activities in Company C. The set up of the international loan-back structure, involving Company A, B and C, complicated the audit trail, legitimated the international funds transfers between the various bank accounts of the companies that Mr X controlled. Also Mr X **co-mingled** the criminal funds, disguised as a loan, with the funds originating from the legal activities of Company C, which made the criminal funds difficult to detect and to trace, thus involving a company with legitimate activities in the money laundering scheme, *i.e.* the integration phase (and avoiding attracting the attention of the authorities).

Mr. X arranged for Mr. Y to buy real estate. To finance the transaction, Mr. X arranged for a loan agreement to be drawn up between Companies B and C. The parties in the contract were the trust of Company B and Mr. Y of Company C. To execute the cash disbursement under the loan, Mr. X ordered the trust of Company A to transfer funds from the account in Bank L to the account of Company B in Bank DA. Next he ordered the trust of Company B to transfer funds from the account in Bank DA to the account of Company C in Bank EUR. The description given to Bank DA en Bank EUR referred to the loan agreement between Company B and C. Both banks did not know about the relationship between Companies B and C. The funds deposited in the account of Company C in Bank EUR were then transferred to the seller of the real estate. Periodically Company C made payments of the principal and interest to Company B from the earnings of the counselling activities. Company B transferred the money to Company A which was used by Mr. X to finance his criminal activities. The interest costs were deducted from the taxable result and declared in the tax return.

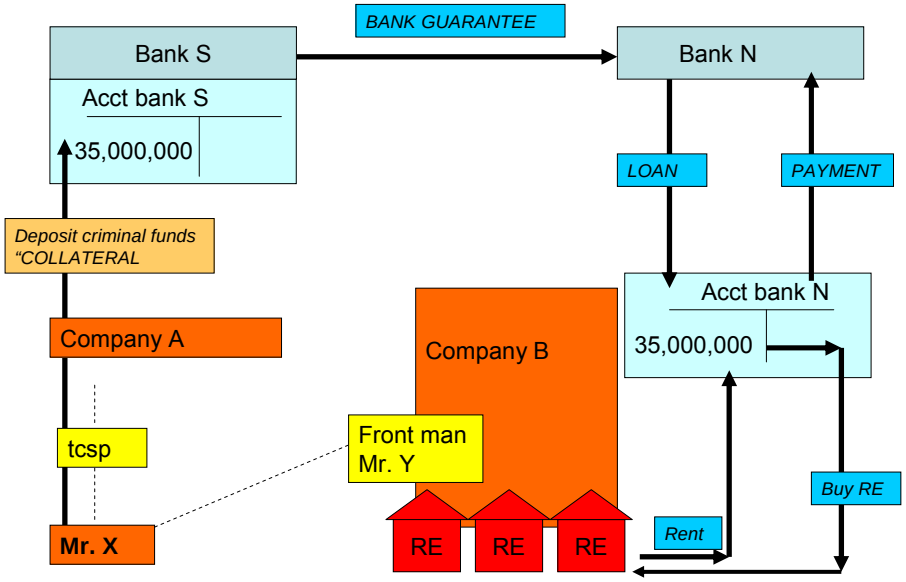
Indicators and methods identified in the scheme:

- **The source of the funds used to finance the real estate transaction was from abroad, in particular from off shore jurisdictions and jurisdictions that have strict bank secrecy.**
- **The lender of the money, an offshore company, had no direct relation with the borrower of the money**
- **A financial institution was not involved in the loan structure.**
- **There was no loan agreement between the lender and borrower.**
- **The loan agreement was legally invalid.**
- **The information in the loan agreement was inconsistent or incorrect.**
- **The conditions in the loan agreement were unusual, for example, there was no collateral required.**
- **No payment of interest or repayment of the principal.**
- **Transaction monitoring by the financial institutions showed payable-through accounts, by which incoming payments from abroad were transferred abroad immediately without a logical reason.**

Source: Netherlands.

Case Study 1.2: Back-to-back Loan Used to Launder Funds

(Predicate offence: forged loan agreement, in particular the failure to mention the security underlying the loan and money laundering)



Mr. X was a criminal who deposited funds via one of his corporate vehicles (Company A) into an account at Bank S. Company A was in an offshore jurisdiction that had strict bank secrecy. Mr X. was the owner of Company A, did not want to disclose his identity and thus used a **TCSP** to manage Company A. Mr. X used Company C to mask his real identity. Mr X also set up and controls Company B of which he is the owner. According to the public registers, the official owner and manager of Company B was Mr. Y who acts as a **front-man**. Company B owned several buildings that were rented out to natural persons and companies. This way Mr. X generated legal rental income via Company B.

Mr. X was short of money from legitimate sources to expand his legal activities. Based on the financial situation of Company B, Bank N was not willing to grant a loan without additional security. He set up a **back-to-back loan** structure to use his criminal money to invest in real estate.

Bank N was willing to lend money to Company B under the condition that Company B provided sufficient collateral and was willing to pay a high-risk premium on top of the market interest rate. Mr. X. arranged for Bank S to provide a **bank guarantee** to Bank N which could be drawn by Bank N on Bank S in case of a default on the loan. Bank N´s credit risk regarding Company B was then fully covered. The loan fit into the financial situation and activities of Company B.

Bank S was willing to provide the bank guarantee to Bank N in name of Company A, with the **pledged deposit** as collateral. The money deposited in Bank S originated from the criminal activities of Mr. X. If Bank N were to withdraw the guarantee on Bank S, Bank S would have used the deposit pledged by Company A to settle the payment with Bank N. For Bank N the original collateral provider Company A, *i.e.* Mr X, was not visible. Bank N only saw Bank S´s guarantee. Bank N lent the money to Company B. Through the payment by Bank N as part of the reimbursement of the back-to-back loan, Mr. X was able to provide a valid reason for the money used to finance the real estate. The collateral originated from criminal activities. The laundered money was invested in real estate that provided for legal rental income.

The earnings of Company B were continuously skimmed off by Mr. X to finance his illegal activities. Company B initially made loan and interest payments to Bank N. After a period of time, Company B stopped the payment of the principal and interest. Based on the loan agreement and the banking terms, Bank N withdrew the bank guarantee on Bank S. Bank S used the pledged deposit to settle the payment to Bank N.

Indicators and methods identified in the scheme:

- **No reference in the loan agreement to the underlying collateral.**
- **The collateral provided was not sufficient**
- **The collateral provider and other parties involved in the loan structure were not known.**
- **The borrower of the money was not willing to provide information on the identity and background of the collateral provider nor on the other parties involved in the loan structure.**
- **The complex nature of the loan scheme could not be justified**
- **There was an unexpected loan default.**

Source: Netherlands.

Case study 6.1: Use of Illegal Funds in Mortgage Loans and Interest Payments

(Predicate offence: forgery, deception, fraud, money laundering)

Mr. X was the owner of Company A and the individual controlling its activities. Mr. X hired Mr. Y as **front man** of Company A. Company A had some low-profile activities in managing and exploiting properties. During the life of Company A, Mr. Y set up a relationship with Bank EUR that provided for accounts and payment services. The property managed by Company A was used for activities by other companies owned by Mr. X (for storage, for example).

Mr. X. planned to buy office buildings for EUR 8 000 000 via Company A. The office buildings had to be renovated to be marketable. Mr. X. knew a licensed assessor (real estate agent), Mr. Z. Mr. X. and Mr. Z found a way to set up a **false but plausible assessments of the market value** of the office buildings after renovation (EUR 13 000 000). Mr. X ordered Mr. Y to negotiate a **mortgage** with Bank EUR to finance the purchase and renovation of the property. Based on the assessment, Bank EUR was willing to grant a mortgage of EUR 13 000 000. Mr. Y entered into the loan agreement on behalf of Company A as the buying party. After the disbursement of the loan, the real estate was paid for. Mr X. then paid Mr. Y EUR 500 000 and had the remaining EUR 4.5 million, together with the proceeds of other criminal activities, transferred into several bank accounts in countries with strict **bank secrecy**. The mortgage of Bank EUR was presented to the foreign banks as the legitimate source of the funds that were being transferred to the accounts. In this way, the money was layered and integrated. The renovation of the office buildings never took place. Meanwhile the activities of Company A rapidly decreased. Company A finally went into default. Bank EUR called the loan, but Mr. Y was not in a position to reimburse it along with the interest payment. Mr Y stated that he was not aware of the persons behind Company A, their whereabouts and the background of the accounts to which the money was transferred.

Indicators and methods identified in the scheme:

- **Applying for a loan under false pretences.**
- **Using forged and falsified documents.**
- **The client persisted in a picture of the financial situation that was unrealistic or that could not be supported by documents.**
- **The loan amount did not relate to the value of the real estate.**
- **Successive buying and selling of the real property involved.**
- **The client had several mortgage loans relating to several residences**

Source: Netherlands.

BIBLIOGRAPHY

European Central Bank (2006), "Assisting House Price Developments in the Euro Area", ECB Monthly Bulletin, ECB, Frankfurt, February 2006. *www.ecb.int/pub/mb/html/index.en.html*.

FATF (2001), *Typologies Report 2000-2001*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2003), *FATF Recommendations*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2004), *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2005), "Money Laundering and Terrorist Financing Trends and Indicators", *Typologies Report 2004-2005*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2006), *Misuse of Corporate Vehicles: Typologies Report*, FATF, Paris. *www.fatf-gafi.org*.

Serious Organised Crime Agency (2006), *The Vulnerability of UK Letting Agents to Money Laundering*, SOCA, London.

Appendix Q:

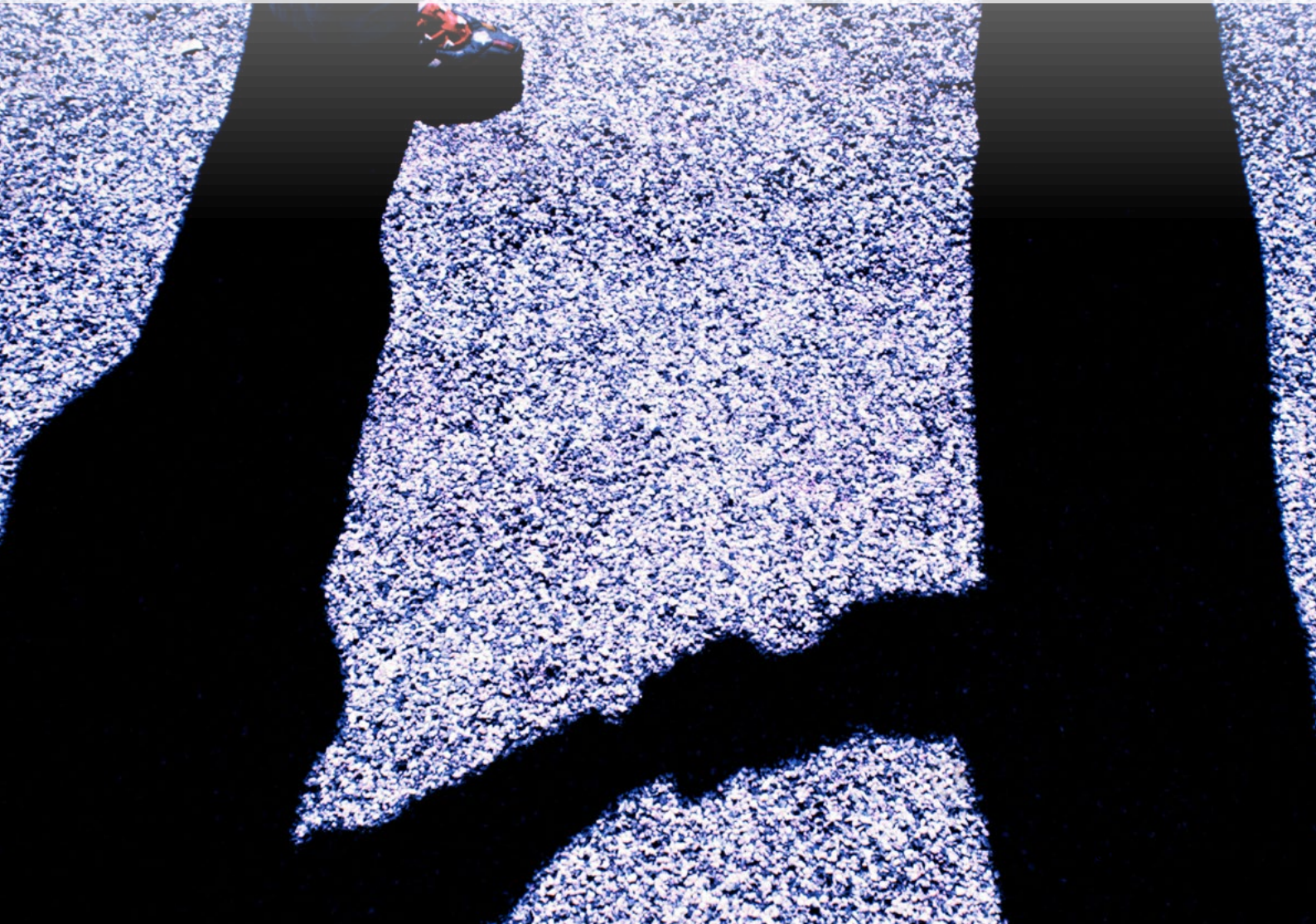
FATF, *Professional Money Laundering* (Paris: FATF, 2018)

FATF

FATF REPORT

Professional Money Laundering

July 2018



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2018), *Professional Money Laundering,* FATF, Paris, France,
www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html

TABLE OF CONTENTS

Boxes

TABLE OF ACRONYMS

CFATF	Caribbean Financial Action Task Force
EAG	Eurasian Group
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MVTS	Money Value Transfer Service
PML	Professional Money Launderer
PMLO	Professional Money Laundering Organisation
PMLN	Professional Money Laundering Network
OCG	Organised Crime Group
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider

EXECUTIVE SUMMARY

This is the first time the FATF is undertaking a project which concentrates on professional money launderers (PMLs) that specialise in enabling criminals to evade anti-money laundering and counter terrorist financing safeguards and sanctions in order to enjoy the profits from illegal activities. The report aims to describe the functions and characteristics that define a "professional" money launderer, namely those individuals, organisations and networks that are involved in third-party laundering for a fee or commission. This report is therefore focused on money laundering *threats* as opposed to *vulnerabilities*, and it addresses criminal actors, including organised crime groups that specialise in the provision of professional money laundering services and complicit actors who are knowingly involved, or are deliberately negligent, in the laundering process. While PMLs may act in a professional capacity (e.g. lawyer, accountant) and serve some legitimate clients, the report aims to identify those actors who serve criminal clients whether on a full-time or part-time basis.

PMLs provide services to criminals and organised crime groups by laundering the proceeds of their illegal activities. As the main purpose of PMLs is to facilitate money laundering, they are rarely involved in the proceeds-generating illegal activities. Instead, they provide expertise to disguise the nature, source, location, ownership, control, origin and/or destination of funds to avoid detection. PMLs generally do not differentiate between drug dealers, fraudsters, human traffickers or any other criminal with a need to move or conceal ill-gotten gains. These are all potential PML clients. PMLs operate under a number of business models and may be individuals; criminal organisations with a clear structure and hierarchy; or networks of loosely affiliated members. Providing services to criminals and organised crime groups, PMLs are criminal actors, profiting from these money laundering activities.

PMLs may provide the entire infrastructure for complex money laundering schemes (e.g. a 'full service') or construct a unique scheme tailored to the specific needs of a client that wishes to launder the proceeds of crime. These PMLs provide a menu of generally applicable services, with the result that the same laundering techniques (and potentially the same financial channels and routes) may be used for the benefit of multiple organised crime groups. As such, professional money laundering networks may act transnationally in order to exploit vulnerabilities in countries and particular businesses, financial institutions, or designated non-financial businesses or professions. PMLs, themselves, pose a threat to the financial system, as they facilitate money laundering and criminality more broadly, profiting from these illegal activities. The results of FATF's fourth round of mutual evaluations reveal that many countries are not sufficiently investigating and prosecuting a range of money laundering activity, including third-party or complex money laundering. Many countries continue to limit their investigations to *self-launderers*: criminals who

launder the proceeds of drug trafficking, fraud, tax evasion, human trafficking or other criminality. While this may address in-house or self-laundering, it does not impact on those specialised in providing criminals with money laundering services. PMLs, professional money laundering organisations and professional money laundering networks can survive law enforcement interdiction against any of its criminal or organised crime group clients, while still standing ready to support the next criminal clientele. Effective dismantling of PMLs requires focused intelligence collection and investigation of the laundering activities, rather than the associated predicate offences of the groups using the services of the PMLs. The dismantling of PMLs, can impact the operations of their criminal clients, and can be an effective intervention strategy against numerous criminal targets.

This report identifies the specialist skill sets that PMLs offer their clients in order to hide or move their proceeds, and provides a detailed explanation of the roles performed by PMLs to enable authorities to identify and understand how they operate. This can include locating investments or purchasing assets; establishing companies or legal arrangements; acting as nominees; recruiting and managing networks of cash couriers or money mules; providing account management services; and creating and registering financial accounts. This report also provides recent examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate ML. The analysis shows that PMLs use the whole spectrum of money laundering tools and techniques; however, the report specifically focuses on some of the common mechanisms used to launder funds, such as trade-based money laundering, account settlement mechanism and underground banking.

The project team also examined potential links between PMLs and terrorist financing, however, there was insufficient material provided to warrant a separate section on this topic. The *Khanani* provides the clearest example of a professional money laundering organisation, providing services to a UN designated terrorist organisation. One delegation also noted potential links between a loosely affiliated professional money laundering network and a domestically designated terrorist organisation. However, the vast majority of cases submitted relate to money laundering, rather than terrorist financing.

The non-public version report also explores unique investigative tools and techniques that have proved successful in detecting and disrupting PMLs to guide countries that are seeking to address this issue. The report includes a number of practical recommendations that are designed to enhance the identification and investigation of PML; identify strategies to disrupt and dismantle these entities; and identify steps to prevent PML. Combatting these adaptable PMLs requires concerted law enforcement and supervisory action at the national level, appropriate regulation and effective international co-operation and information exchange. This report emphasises the need for a more co-ordinated operational focus on this issue at a national level, and the importance of effective information sharing between authorities at an international level. The report also identifies the information and intelligence required to successfully identify, map, and investigate PMLs, with the objective of disrupting and dismantling those involved in PML and their criminal clientele.

This report intends to assist authorities at jurisdictional level target PMLs, as well as the structures that they utilise to launder funds, to disrupt and dismantle the groups that are involved in proceeds-generating illicit activity so that crime does not pay.

PROFESSIONAL MONEY LAUNDERING

SECTION I: INTRODUCTION

Purpose, Scope and Objectives

The FATF has conducted a number of studies on money laundering (ML) risks. The resulting reports have usually examined ML threats associated with particular proceeds generating offences or vulnerabilities associated with entities covered under the FATF Standards. This report assesses the threats associated with professional money launderers (PMLs), and does not assess ML vulnerabilities that are covered in other FATF reports. Specifically, the report aims to:

- raise awareness of the unique characteristics of professional money laundering (PML);
- understand the role and functions of those involved in PML;
- understand the business models and specific functions performed by PMLs;
- understand how organised crime groups (OCGs) and terrorists use the services of PMLs to move funds;
- identify relevant ML typologies and schemes;
- develop risk indicators for competent authorities and the private sector that are unique for PMLs; and
- develop practical recommendations for the detection, investigation, prosecution and prevention of PML.

Structure of the Report

Sections II and **III** provide the framework for the report, including key characteristics of PML; differences between individuals, organisations and networks involved in PML; and an explanation of the roles performed by those involved. The aim of these sections is to ensure a consistent dialogue on this topic as countries deepen their understanding of this issue.

Sections IV, **V** and **VI** highlight the main types of dedicated ML networks, including the types of complicit and criminal financial services providers and other professional intermediaries generally involved in PML, and common mechanisms used to launder funds. The types of information within these sections should not be considered finite, as PMLs utilise all ML tools and techniques available to them and continue to adapt their methods to take advantage of regulatory and enforcement gaps.

Methodology

This project was co-led by the Russian Federation and the United States and incorporates input from a variety of delegations across the FATF's Global Network. The project team received submissions from Argentina, Australia, Belgium, Canada, China, Germany, Israel, Italy, Malaysia, the Netherlands, the Russian Federation, Singapore, Spain, the United Kingdom, the United States, EAG Members (Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan), MONEYVAL (Ukraine), MENAFATF (Lebanon), CFATF (Belize) and EUROPOL.

Authorities provided detailed information, including from risk assessments and case examples of various schemes arranged by PMLs, strategic analysis outcomes, information on internal organisational and behavioural aspects of PMLNs and investigative techniques. The report includes select country examples to provide the necessary context.

Input was also gathered at the Middle East and Africa Joint Typologies and Capacity Building Workshop in Rabat, Morocco, from 22-25 January 2018, and input and feedback gathered at the FATF Joint Experts Meeting held in Busan, Republic of Korea, from 1-4 May 2018. The findings of this report also rely on feedback from financial intelligence units (FIUs) and law enforcement agencies (LEAs), based on their experiences in investigating PMLs.

There has been sparse research on this subject. However, the project team did take into consideration previous and ongoing work by the FATF on operational issues, including the 2012 *FATF Guidance on Financial Investigations*, 2013 *FATF Report on ML and TF Vulnerabilities of Legal Professionals* and the 2018 *Joint FATF/Egmont Report on the Vulnerabilities Linked to the Concealment of Beneficial Ownership*.

SECTION II: CHARACTERISTICS OF PROFESSIONAL MONEY LAUNDERING

This section of the report outlines the key characteristics, which make PML unique, and helps to frame the scope of this report. **Section III** then provides a list of specialised services, which include specific roles or functions performed by various individuals. The report has attempted to avoid the use of formal titles (e.g. controller, enabler and facilitator), as multiple and inconsistent terminology is used globally, which leads to confusion when describing these functions. **Section III** provides a business model demonstrating how PMLs generally conduct financial schemes.

Key Characteristics

PML is a subset of third-party ML. The FATF defines third-party ML as the laundering of proceeds by a person who was not involved in the commission of the predicate offence[1]. The main characteristic that makes PML unique is the provision of ML services in exchange for a commission, fee or other type of profit. While the specialisation in providing ML services is a key feature of PMLs, this does not mean that PMLs are not also involved in other activities (including legal businesses).

[1] FATF Methodology 2013, footnote to Immediate Outcome 7.

Similarly, this does not mean that they exclusively only launder illicit proceeds. PMLs also use specialised knowledge and expertise to exploit legal loopholes; find opportunities for criminals; and help criminals retain and legitimise the proceeds of crime.

Given that PMLs are third-party launderers, they are often not familiar with the predicate offence (e.g. narcotics or human trafficking) and are generally not concerned with the origins of the money that is moved. Nonetheless, PMLs are aware that the money that they move is not legitimate. The PML is concerned primarily with the destination of the money and the process by which it is moved. They are used by clients in order to create distance between those perpetrating the crimes and the illicit proceeds that they generate as profit, or because the criminal clients do not have the knowledge required to reliably launder the money without law enforcement detection.

Ultimately, PMLs are criminals, who often operate on a large scale and conduct schemes that are transnational in nature. The term "PMLs" is not intended to include unwitting or passive intermediaries who are exploited to facilitate an ML scheme. Other features of PMLs are that they sometimes operate on a large scale and often conduct schemes that are transnational in nature.

Commissions / Fees

A number of different and overlapping factors affect the fee paid to PMLs or the commission they receive for their services. The fee will often depend on the complexity of the scheme, methods used and knowledge of the predicate offence. The rate may change based on the level of risk that PMLs assume. For example, commission rates are often influenced by the countries or regions involved in the scheme, as well as other factors such as:

- the reputation of the individual PML;
- the total amount of funds laundered;
- the denomination (i.e. value) of the banknotes (in cases involving cash);
- the amount of time requested by a client to move or conceal funds (for example, if the laundering needs to be done in a shorter time period, the commission will be higher); and
- the imposition of new regulation(s) or law enforcement activities.

To obtain commission for their services, PMLs may (i) take commission in cash in advance, (ii) transfer a portion of money laundered to their own accounts or (iii) have the commission integrated into the business transaction.

Advertising / Marketing

Advertising and marketing of services can occur in numerous ways. Often, this involves the PMLs actively marketing their services by 'word-of-mouth' (through an informal criminal network). Criminal links and trust developed through previous criminal engagement also strengthens bonds and can encourage further co-operation. Authorities have also identified the use of posted advertisements for PML services on the Dark Web.

Record Keeping (Shadow Accountancy)

Law enforcement has reported that PMLs often keep a shadow accounting system that contains detailed records with code names. These unique accounting systems may use detailed spreadsheets that track clients (using code names); funds laundered; the origin and destination of funds moved; relevant dates; and commissions received. PMLs may either store their records electronically (e.g. a password-protected Excel spreadsheet) or use paper records. These records represent an invaluable resource for investigators.

Individuals, Organisations and Networks

PMLs can belong to one of three categories:

1. An **individual PML,** who possesses specialised skills or expertise in placing, moving and laundering funds. They specialise in the provision of ML services, which can also be performed while acting in a legitimate, professional occupation. These services can include, but are not limited to, the following: accounting services, financial or legal advice, and the formation of companies and legal arrangements (see *specialised services*, below). Individual PMLs often spread their risks across diverse products, and carry out business activities with several financial specialists and brokers (see examples below).

2. A **Professional money laundering organisation (PMLO)**, which consists of two or more individuals acting as an autonomous, structured group that specialises in providing services or advice to launder money for criminals or other OCGs. Laundering funds may be the core activity of the organisation, but not necessarily the only activity. Most PMLOs have a strict

hierarchical structure, with each member acting as a specialised professional that is responsible for particular elements of the ML cycle (see **Section III**).

3. A **Professional money laundering network (PMLN)**, which is a collection of associates or contacts working together to facilitate PML schemes and/or subcontract their services for specific tasks. These networks usually operate globally, and can include two or more PMLOs that work together. They may also operate as informal networks of individuals that provide the criminal client with a range of ML services. These interpersonal relationships are not always organised, and are often flexible in nature.

These extensive PML networks are able to satisfy the demands of the client by opening foreign bank accounts, establishing or buying foreign companies and using the existing infrastructure that is controlled by other PMLs. Collaboration between different PMLs also diversifies the channels through which illicit proceeds may pass, thereby reducing the risk of detection and seizure.

PMLOs work with OCGs of all nationalities, on a global basis or in a specific region, often acting as a global enterprise. The same PML can be used to facilitate ML operations on behalf of several OCGs or criminal affiliates. They are highly skilled and operate in diverse settings, adept at avoiding the attention of law enforcement. One relevant case has been identified demonstrating that the same money launderers provided services to both OCGs and terrorist organisations (see Box 1, below).

Box 1. Khanani Money Laundering Organisation

The Altaf Khanani Money Laundering Organisation (MLO) laundered illicit proceeds for other OCGs, drug trafficking organisations and designated terrorist groups throughout the world. The Khanani MLO was an OCG composed of individuals and entities operating under the supervision of Pakistani national, Altaf Khanani, whom the US Drug Enforcement Administration (DEA) arrested in 2015. The Khanani MLO facilitated illicit money movements between Pakistan, the United Arab Emirates (UAE), the United States, the United Kingdom, Canada, Australia and other countries. It was responsible for laundering billions of dollars in criminal proceeds annually.

The Khanani MLO offered ML services to a diverse clientele, including Chinese, Colombian and Mexican OCGs, as well as individuals associated with a US

domestically designated terrorist organisation. The Khanani MLO has also laundered funds for other designated terrorist organisations. Specifically, Altaf Khanani, the head of the Khanani MLO and Al Zarooni Exchange, has been involved in the movement of funds for the Taliban, and Altaf Khanani is known to have had relationships with Lashkar-e-Tayyiba, Dawood Ibrahim, al-Qa'ida and Jaish-e-Mohammed. Furthermore, Khanani was responsible for depositing drug proceeds via bank wires from a foreign business account in an effort to conceal and disguise the nature, source, ownership and control of the funds. Khanani conducted transactions, which involved multiple wire transfers from a number of general trading companies. Khanani's commission to launder funds was 3% of the total value of funds laundered.

The Khanani MLO itself was designated by OFAC in 2015 as a "transnational criminal organisation[1]," pursuant to Executive Order 13581. On the same day, OFAC designated the exchange house utilised by the Khanani MLO, Al Zarooni Exchange. In 2016, the US Treasury's Office of Foreign Assets Control (OFAC) designated four individuals and nine entities associated with the Khanani MLO. On October 26, 2016 Altaf Khanani pleaded guilty to federal ML charges. Approximately USD 46 000 in criminal proceeds was also confiscated from Khanani. In 2017, Altaf Khanani was sentenced to 68 months in prison for conspiracy to commit ML.

Extensive law enforcement co-ordination took place between multiple law enforcement agencies from Australia, Canada and the US who all held a different piece of the puzzle. The designation of Al Zarooni Exchange complements an action taken by the Central Bank of the UAE, with assistance from the AML Unit at Dubai Police General Headquarters, which closely coordinated with the DEA prior to the action taken.

Note: 1. Transnational Criminal Organisation (TCO) is a specific technical term used in the US designation process and is synonymous with organised crime group (OCG), the latter of which is used throughout this report.

Source: United States, Australia, Canada, UAE

OCGs use both outsiders and OCG members to perform ML services on behalf of the group. In cases where there is an in-house component of an OCG that is responsible for ML, these members may receive a portion of the proceeds of the group, rather than a fee or commission. The extent to which PMLs get involved in ML schemes depends on the needs of the criminal group, the complexity of the laundering operation that they wish to execute, as well as the risks and costs associated with such involvement.

When OCGs employ the services of PMLs, they often choose PMLs who are acquainted with persons close to, or within, the OCG network. They can be family members or close contacts. They may also be professionals that previously acted in a legitimate capacity, and who now act as:

- accountants, lawyers, notaries and/or other service providers;
- Trust and Company Service Providers (TCSPs);
- bankers;
- MVTS providers;

- brokers;
- fiscal specialists or tax advisors;
- dealers in precious metals or stones;
- bank owners or insiders;
- payment processor owners or insiders; and
- electronic and cryptocurrency exchanger owners or insiders.

OCGs also make use of external experts on a permanent or ad hoc basis. These experts knowingly operate as entrepreneurs and often have no criminal record, which can aid in avoiding detection. These complicit professionals are increasingly present on the criminal landscape, coming together as service providers to support specific criminal schemes or OCGs (see **Section VI**). PMLs can also provide services to several OCGs or criminal affiliates simultaneously, and are both highly skilled at operating in diverse settings and adept at avoiding the attention of law enforcement.

Compartmentalised relationships also exist, particularly within PMLNs, whereby there may be no direct contact between OCGs and the lead actors responsible for laundering the funds In these instances, transactions are facilitated via several layers of individuals who collect the money (see **Section III**) before funds are handed over to PMLs for laundering.

SECTION III: SPECIALISED SERVICES AND BUSINESS MODELS

PMLs can be involved in one, or all, stages of the ML cycle (i.e. placement, layering and integration), and can provide specialised services to either manage, collect or move funds. PMLOs act in a more sophisticated manner and may provide the entire infrastructure for complex ML schemes or construct a unique scheme, tailored to the specific needs of a client.

There are a number of specialised services that PMLs may provide. These include, but are not limited to:

- consulting and advising;
- registering and maintaining companies or other legal entities;
- serving as nominees for companies and accounts;
- providing false documentation;
- comingling legal and illegal proceeds;
- placing and moving illicit cash;
- purchasing assets;
- obtaining financing;
- identifying investment opportunities;
- indirectly purchasing and holding assets;
- orchestrating lawsuits; and
- recruiting and managing money mules.

Roles and Functions

This section identifies numerous roles and functions that are necessary to the operation of PMLs. These specific functions, outlined below, should not be considered an exhaustive list. Depending on the type of PML, an individual may perform a unique function or perform several roles simultaneously. Understanding these roles is important in order to identify all of the relevant players and ensure that all relevant aspects of PMLs are detected, disrupted and ultimately dismantled.

- ***Leading and controlling***: There may be individuals who provide the overall leadership and direction of the group, and who are in charge of strategic planning and decision making. Control over ML activities of the group is normally exercised by a leader, but may also be exercised by other individuals who are responsible for dealing with the funds from the time they are collected from clients until delivery (e.g. arranging the collection of cash and organising the delivery of cash at a chosen international destination). These individuals are also responsible for determining the commission charged and paying salaries to other members of the PMLO/PMLN for their services.
- ***Introducing and promoting***: There are often specific individuals who are responsible for bringing clients to the PMLs and managing communications with the criminal clients. This includes managers who are responsible for establishing and maintaining contact with other PMLOs or individual PMLs that operate locally or abroad. Through the use of these contacts, the PMLO gains access to infrastructure already established by other PMLs.
- ***Maintaining infrastructure***: These individuals are responsible for the establishment of a range of PML infrastructure or tools. This could include setting up companies, opening bank accounts and acquiring credit cards. These actors may also manage a network of registrars who find and recruit nominees (e.g. front men) to register shell companies on behalf of the client, receive online banking logins and passwords, and buy SIM-cards for mobile communication.

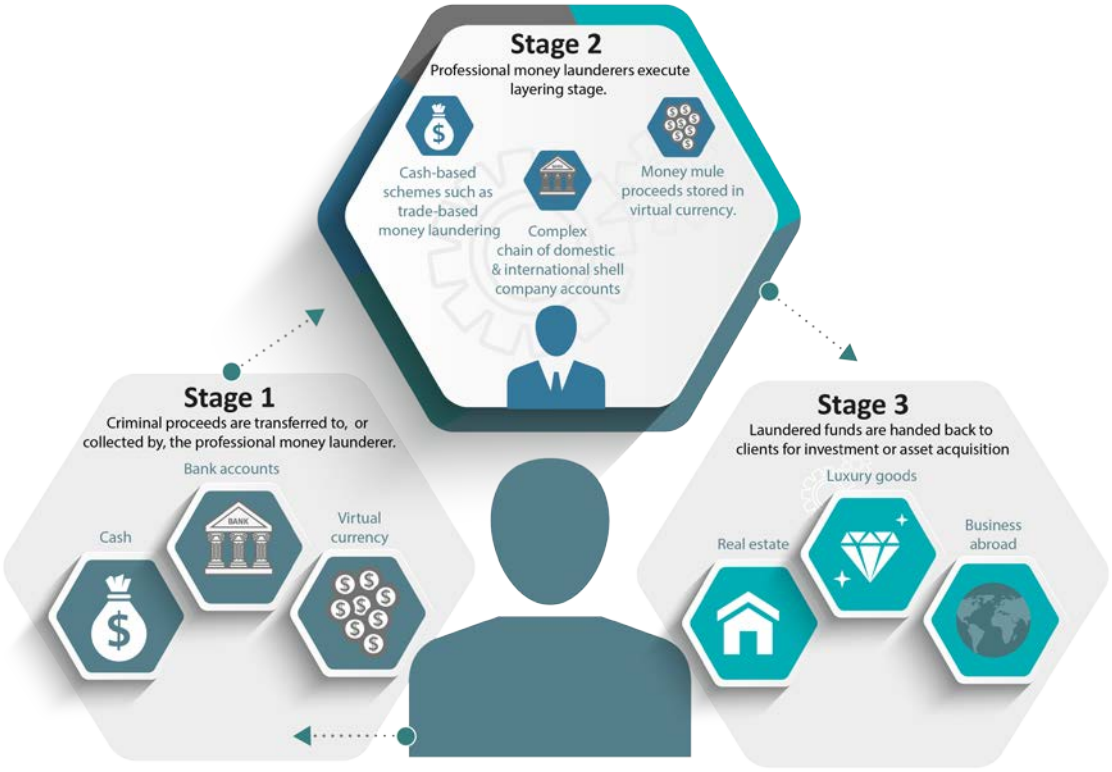
  One example of managing infrastructure is the role of a *money mule herder*, who is responsible for recruiting and managing money mules (e.g. via job ads and via a personal introduction), including the payment of salaries to mules. This salary can be paid either as a fee for their money transfer services or as a one-time payment for their services (see **Section IV** for a wider description of money mule networks and the roles within these specific networks).
- ***Managing documents***: These individuals are responsible for the creation of documentation needed to facilitate the laundering process. In some cases, these individuals are responsible for either producing or acquiring fraudulent documentation, including fake identification, bank statements and annual account statements, invoices for goods or services, consultancy arrangements, promissory notes and loans, false resumes and reference letters.
- ***Managing transportation***: These individuals are responsible for receiving and forwarding goods either internationally or domestically, providing

customs documentation and liaising with transport or customs agents. This role is particularly relevant to TBML schemes.

- ***Investing or purchasing assets***: Where needed, real estate or other assets, such as precious gems, art or luxury goods and vehicles, are used to store value for later sale. Criminals seek assistance in purchasing real estate overseas, and PMLs have been known to use elaborate schemes involving layers of shell companies to facilitate this.
- ***Collecting***: These individuals are responsible for collecting illicit funds, as well as the initial placement stage of the laundering process. Given that they are at the front end of the process, they are most likely to be identified by law enforcement. However, they often leave little paper trail and are able to successfully layer illicit proceeds by depositing co-mingling funds using cash-intensive businesses. These individuals are aware of their role in laundering criminal proceedings (compared to some money mules, who may be unwitting participants in a PML scheme).
- ***Transmitting***: These specific individuals are responsible for moving funds from one location to another in the PML scheme, irrespective of which mechanism is used to move funds. They receive and process money using either the traditional banking system or MVTS providers, and are also often responsible for performing cash withdrawals and subsequent currency exchange transactions.

General Business Model of Professional Money Laundering Networks

Figure 1. Three stages of professional money laundering



In general, financial schemes executed by PMLs consist of three stages:

Stage 1: Criminal proceeds are transferred to, or collected by, PMLs

In the first stage, funds are transferred, physically or electronically, to PMLs or to entities operating on their behalf. The precise manner of introduction of the funds into the ML scheme varies depending on the types of predicate offence(s) and the form in which criminal proceeds were generated (e.g. cash, bank funds, virtual currency, etc.):

Cash: When illicit proceeds are introduced as currency, they are usually passed over to a cash collector. This collector may ultimately deposit the cash into bank accounts. The collector introduces the cash into the financial system through cash-intensive businesses, MVTS providers or casinos, or physically transports the cash to another region or country.

Bank accounts: Some types of criminal activity generate illicit proceeds held in bank accounts, such as fraud, embezzlement and tax crimes. Unlike drug proceeds, proceeds of these crimes rarely start out as cash but may end up as cash after laundering. Clients usually establish legal entities under whose names bank accounts may be opened for the purposes of laundering funds. These accounts are used to transfer money to a first layer of companies that are controlled by the PMLs.

Virtual Currency: Criminals who obtain proceeds in a form of virtual currency (e.g. owners of online illicit stores, including Dark Web marketplaces) must have e-wallets or an address on a distributed ledger platform, which can be accessed by the PMLs.

Stage 2: Layering stage executed by individuals and/or networks

In the layering stage, the majority of PMLs use account settlement mechanisms to make it more difficult to trace the funds. A combination of different ML techniques may be used as part of one scheme. The layering stage is managed by individuals responsible for the co-ordination of financial transactions.

Cash: ML mechanisms for the layering of illicit proceeds earned in cash commonly include: TBML and fictitious trade, account settlements and underground banking.

Bank Accounts: Funds that were transferred to bank accounts managed by PMLs are, in most cases, moved through complex layering schemes or proxy structures. Proxy structures consist of a complex chain of shell company accounts, established both domestically and abroad. The funds from different clients are mixed within the same accounts, which makes the tracing of funds coming from a particular client more difficult.

Virtual Currency: Criminals engaged in cybercrime or computer-based fraud, as well as in the sale of illicit goods via online stores, often use the services of money mule networks (see Section IV). The illicit proceeds earned from these crimes are often held in the form of virtual currency, and are stored in e-wallets or virtual currency wallets that go through a complex chain of transfers.

Stage 3. Laundered funds are handed back over to clients for investment or asset acquisition

In the last stage, funds are transferred to accounts controlled by the clients of the PML, their close associates or third parties acting on their behalf or on behalf of affiliated legal entities. The PML may invest the illicit proceeds on behalf of these clients in real estate, luxury goods, and businesses abroad (or, in some cases, in countries where the funds originated from). The funds can also be spent on goods deliveries to a country where the funds originated or to a third country.

SECTION IV: TYPES OF DEDICATED ML ORGANISATIONS AND NETWORKS

As mentioned in the previous sections, PMLs may move funds through dedicated networks, utilising multiple mechanisms to move funds. These networks, often used during the placement and layering stages in the laundering cycle, are able to quickly adapt and adjust to shifting environmental factors (such as new regulation) and law enforcement activities. PMLs may also provide detailed guidance to assist with the entire ML scheme and often sell "packages" that contain the instruments and services required to facilitate an ML scheme. This section describes the key types of dedicated ML organisations and networks identified through an analysis of case studies: (i) money transport and cash controller networks; (ii) money mule networks; (iii) digital money and virtual currency networks; and (iv) proxy networks.

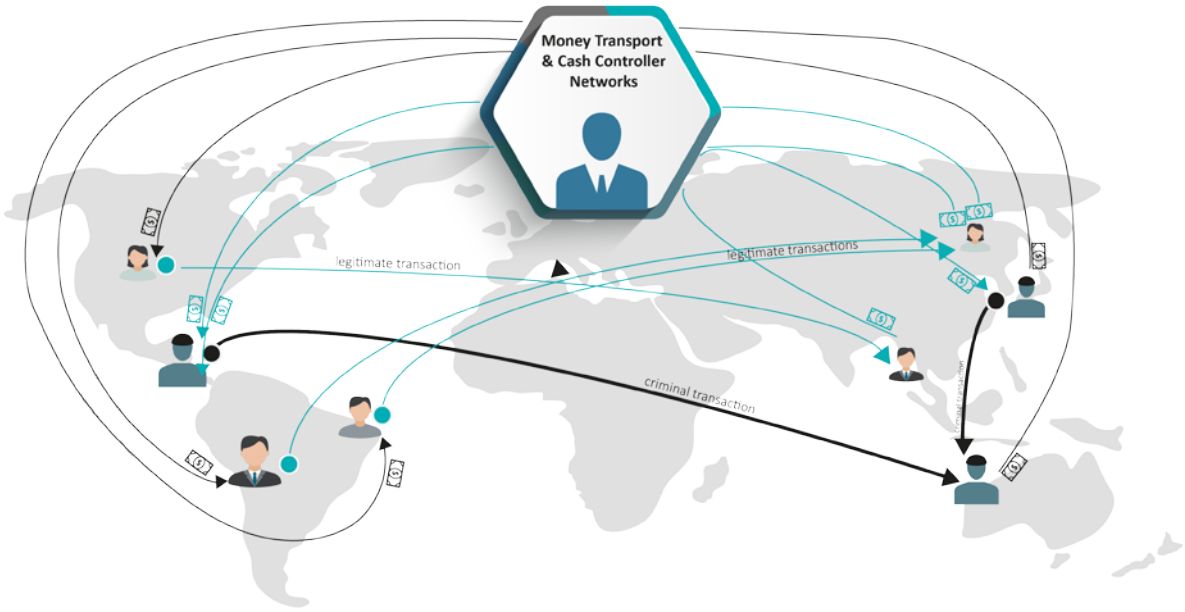
Money Transport and Cash Controller Networks

Criminals and OCGs that generate significant amounts of cash often use the services of cash controller networks that are capable of transferring vast sums of cash on their behalf. These international controller networks have the capacity to receive, hand over and transfer criminal proceeds, while charging a processing fee. Generally the structure of these networks consists of individuals who *control, co-ordinate, collect and transmit illicit funds,*[2] and who operate together to negotiate deals with the OCG.

Cash controller networks often orchestrate the laundering of the proceeds of crime for multiple OCGs located worldwide through an account settlement system, whereby illicit proceeds are substituted for legitimate funds. The ML technique employed sometimes involves the transfer of criminal funds through the accounts of unwitting customers who receive funds or payments from abroad. In this scheme, legal funds, which are to be transferred into the bank account of an unwitting third party, are substituted by the launderer with the illicit proceeds of the OCG. The launderer deposits the money in amounts under the reporting threshold to avoid detection.

[2] See roles and functions defined in Section III

Figure 2. Money Transport and Cash Controller Network



Amounts deposited do not immediately match the overall sums of illicit proceeds. However, in the long term, the value of illicit proceeds collected against the value of deposits tends to be equivalent. Where this is not the case, the PML may resort to other trade-based techniques, such as fake or over invoicing, in order to legitimise the movement of funds between two or more jurisdictions, to balance the system. This technique allows the PML to oversee payments made in another country, without the risk of being detected by holding bank accounts in their own name(s).

If an international cash controller network works with criminals and OCGs operating in different countries, it may easily avoid conducting cross-border transfers of funds, with the support of an account settlement mechanism (see Section V). The chart, below, illustrates the operations of an international cash controller network in four different situations.

Box 2. Cash Controller Network and Account Settlement Scheme

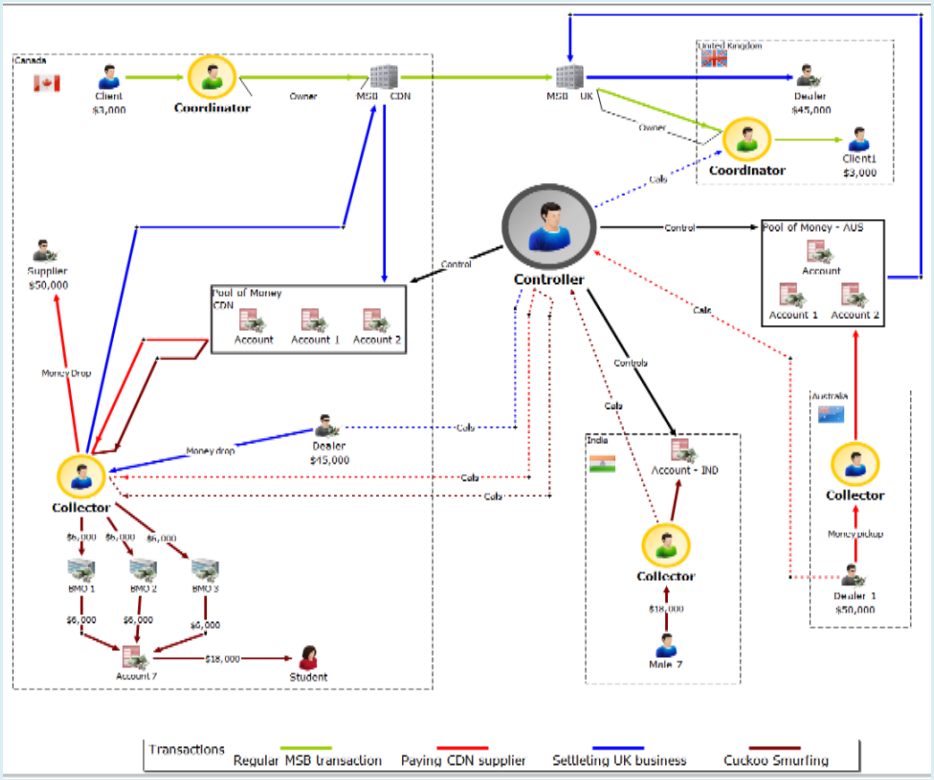
USD 3 000 GREEN: Basic transaction. The Canadian client wants to send money to another client in the UK. It is conducted through the MVTS provider's intermediary.

USD 50 000 RED: An Australian dealer wants to pay its Canadian supplier. The dealer contacts the controller to arrange the transfer. The controller instructs the collector to pick up money. The money is now part of a pool of money in that country under the control of the controller. The controller instructs his Canadian collector to take money from his Canadian pool of money to conduct a money-drop.

USD 45 000 BLUE: The Canadian dealer wants to settle an account in the UK.

The dealer contacts the controller and arranges a pick-up. The collector picks up the money and is instructed to deliver it to a complicit transmitter to place the money into bank accounts (structuring). This increases the Canadian pool of money. The controller then takes money from the UK pool and instructs the UK collector to deliver the money.

USD 18 000 MAROON: A father in India wants to send money to his daughter in Canada. The funds are sent through a hawala network[1]. The collector secures the contract for the controller. The controller then directs his Canadian collector to disperse deposits into the individual`s bank account. He visits three different branches to structure the deposits into the account.



Note: 1. For further information about hawala, see FATF, *Role of Hawala and Other Similar Service Providers in ML and TF*, October 2013

Source: Australia

The laundering of criminal proceeds generated in cash may include the physical transportation of bulk cash. Recent cases show that services to transport cash are also being outsourced to specialised cash transportation networks that are responsible for collecting cash, transporting it to pre-determined locations and facilitating its placement in the financial system. One of the recent examples of efforts taken to combat cash transportation networks that provide services to drug trafficking organisations operating in Europe is EUROPOL's Operation Kandil. The network was responsible for collecting the proceeds of heroin sales throughout Europe (Spain, the Netherlands, Italy and the UK) and transporting this cash to Germany, where it was placed into the financial system through the purchase of second-hand cars, spare parts and equipment.

Box 3. Operation Kandil – Use of Cash Courier Network

In 2016, authorities from Germany, supported by EUROPOL experts, took action against an Iraqi OCG (based in Germany) that was suspected of performing ML services for international heroin traffickers. The operation was preceded by extensive and complex criminal investigations, supported by EUROPOL, which coordinated the law enforcement authorities in France, Spain, Germany and the Netherlands, mirrored by EUROJUST's co-ordination of judicial authorities.

This criminal syndicate, composed mainly of Iraqi nationals, was responsible for collecting the proceeds of heroin sales throughout Europe (Spain, the Netherlands, Italy and the UK) and laundering these funds to the Middle East through Germany, with an estimated total amount of EUR 5 million already laundered.

The criminals' modus operandi involved the use of cash couriers traveling by car to pick up dirty cash all over Europe. This was followed by the use of TBML techniques to transmit the value to the Middle East, primarily through the shipment of second-hand cars; heavy machinery and construction equipment purchased in Germany and exported to Iraq, where the goods were ultimately resold in exchange for clean cash.

The OCG was then able to make use of MVTS services and unregulated financial channels (the hawala system) to integrate and further transfer funds into the regulated financial system. This left virtually no paper trail for law enforcement.

Professional service providers, such as solicitors, accountants and company formation agents, provided the skills and knowledge of financial procedures necessary to operate this scheme. Although, few groups are known to provide these services, they launder large amounts of money, and have a considerable impact on the ability of other OCGs to disguise and invest criminal proceeds. These syndicates are a significant obstacle to tracing criminal assets.

Source: EUROPOL (Germany)

Money Mule Networks

One of the significant elements of many PML schemes is the use of money mules. Money mules are people who are used to transfer value, either by laundering stolen money or physically transporting goods or other merchandise. Money mules may be willing participants and are often recruited by criminals via job advertisements for 'transaction managers' or through online social media interactions. Money mule recruiters are also known as mule 'herders.' Money mules may be knowingly complicit in the laundering of funds or work unwittingly, or negligently, on behalf of a PMLN or OCG. Cyber criminals tailor their recruitment techniques based on the prospective mule's motivations. For example, these criminals will also offer off-the-record cash payments and free travel to incentivise and recruit "witting" mules motivated by easy money and free travel.

Box 4. Use Of Money Mules to Launder Criminal Proceeds

Person A was recruited by a Nigerian syndicate to receive money in her bank accounts. She was promised commissions of up to SGD 5 000 (EUR 3 160) for each transaction. Person A received criminal proceeds from fraud committed in the US and the Bahamas into her bank accounts. Most of the funds were transferred out or withdrawn within a few days of receipt, upon instructions of the Nigerian-based OCG.

Not only did Person A serve as a receptacle for illicit proceeds, she also recruited two other money mules. The control of the mules' bank accounts allowed her to obscure the locations of the illicit proceeds through layering, and enabled her to evade detection as the funds were spread out over multiple accounts. Through this network, Person A and her money mule network received a total of 12 fraudulent wire transfers, amounting to SGD 5 million (EUR 3 16 million) from overseas victims into their bank accounts in Singapore, within a period of six weeks.

Person A was convicted and sentenced to 72 months' imprisonment for receiving stolen property and ML offences.

Source: Singapore

PMLs frequently recruit money mules from diaspora networks and ethnic communities. A sizeable amount of money mule transactions are linked to online illicit stores and cybercrime, such as phishing, malware attacks, credit card fraud, business e-mail compromise and various types of other scams (including romance, lottery and employment scams).

Some money mules are unaware that they are being used to facilitate criminal activity. Unwitting mules are used by OCGs to cash counterfeit checks and money orders or purchase merchandise using stolen credit card numbers or other personal identification information. In some cases, the mules may suspect that the source of the money that they are moving is not legitimate. Such wilfully blind money mules often use income earned to supplement their regular income because they are facing financial difficulties or are motivated by greed.

In the past, money mules have been viewed as low-level offenders, transferring small amounts of cash. However, organised, sophisticated money mule schemes have evolved as a PML mechanism. These money mule networks are controlled by a hierarchical structure, and are well-resourced and highly effective in laundering funds. Money mule networks are usually associated with OCGs that operate cross-border, particularly those involved in cybercrime and the sale of illicit goods through online stores. Typically, these schemes involve criminals that create apparently legitimate businesses, hiring unsuspecting individuals whose jobs involve setting up bank accounts to receive and pass along supposedly legitimate payments. In reality, these unsuspecting individuals act as money mules, processing the criminals' illicit proceeds and wiring them to other criminals.

Money mule networks have been used to open numerous individual bank accounts locally as well as in global financial centres to facilitate the movement of criminal

proceeds. Bank accounts, opened by the mules, serve as the initial layering stage in the laundering process. This indicates that criminals still find the combination of money mule accounts, cash withdrawals and wire transfers to be an effective way to layer proceeds.

Box 5. Avalanche Network

Avalanche is an example of a criminal infrastructure dedicated to facilitating privacy invasions and financial crimes on a global scale. Avalanche was a hosting platform composed of a worldwide network of servers that was controlled via a highly organised central system. This cyber network hosted more than two dozen of the world's most pernicious types of malware and several large scale ML campaigns.

The Avalanche network, in operation since at least 2010, was estimated to serve clients operating as many as 500 000 infected computers worldwide on a daily basis. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of USD worldwide.

The Avalanche network offered cybercriminals a secure infrastructure, designed to thwart detection by law enforcement and cyber security experts. Online banking passwords and other sensitive information stolen from victims' malware-infected computers was redirected through the intricate network of Avalanche servers and ultimately to back-end servers controlled by the cybercriminals. Access to the Avalanche network was offered to the cybercriminals through postings on exclusive, dark web criminal forums.

The types of malware and money mule schemes operating over the Avalanche network varied. Ransomware such as Nymain, for example, encrypted victims' computer files until the victim paid a ransom (typically in a form of crypto-currency) to the cybercriminal. Other malware, such as GozNym, was designed to steal sensitive online banking credentials from victims in order to use those credentials to initiate fraudulent wire transfers from the victims' bank accounts.

The ML schemes operating over Avalanche involved highly organised individuals, who controlled server networks and money mules, which were a crucial part of the criminal network. In some cases, the leaders would use a network of individuals to open bank accounts in major global financial hubs to facilitate wire transfers. The mules were often sponsored by the leader of a particular, country-based network and brought to the US, or, they were unwitting individuals who were recruited. The mules purchased goods with stolen funds, enabling cybercriminals to launder the money they acquired through malware attacks or other illegal means.

Source: United States

Digital Money and Virtual Currency Networks

PMLs also arrange schemes that allow criminals to cash out proceeds generated in virtual currency via online illicit markets (e.g. Dark Web drug-trafficking marketplaces). In many cases, payments for illicit drugs purchased online are transferred to e-wallets held in fiat currency or in virtual currency (e.g. Bitcoin). Afterwards, virtual currency is transferred through a complex chain of e-wallets, which may include the use of mixers and tumblers to further enhance the anonymity of the virtual currency transactions. Funds are then sent back to the e-wallet of the OCG, and subsequently transferred to bank cards and withdrawn in cash.

Financial instruments are issued under the names of money mules (usually students who obtain a bank card and then sell the bank card to criminals for a fee, knowing nothing about its subsequent usage and associated criminal activities). Money mules employed by the PML conduct ATM withdrawals in a coordinated manner, and then give the money to members of the client OCGs.

There are cases when the same financial scheme and the network of individuals worked for the benefit of multiple OCGs operating on the Dark Web. These persons then re-distributed funds to the respective OCGs.

Box 6. Laundering Proceeds from Dark Web Drug Stores

The Russian Ministry of Internal Affairs and FIU conducted an investigation into OCGs that sold drugs via the Dark Web. Customers could choose two ways to pay and transfer funds for their order either by an indicated e-wallet, held in fiat currency, or to a Bitcoin address. The majority of clients preferred using e-wallets held in fiat currency, instead of Bitcoins.

The financial scheme for the drug stores was arranged and managed by a financier and his network. The ML network was responsible solely for moving funds and had no links to drug trafficking. Numerous e-wallets and debit cards were registered in the names of front men. This usually involved students who issued e-wallets and credit cards, and then sold them to members of the ML network, unaware of the criminal purpose of their further usage. Some e-wallets were used at the placement stage of the laundering process and had a limit of USD 300 000, while other e-wallets had a higher limit.

To simplify the ML process, the network's IT specialists developed a 'transit-panel' that had a user-friendly interface and was accessible via the TOR browser. The transit panel automatically switched between e-wallets that were used for drug payments. Digital money was automatically moved through a complex chain of different e-wallets.

Money from e-wallets was then transferred to debit cards and withdrawn in cash via ATMs. Withdrawals via ATMs were conducted by "cash co-ordinators" who had multiple debit cards at hand (all cards were issued on the names of straw men[1]). Afterwards, cash was handed over to interested parties. In order to increase the complexity, proceeds were re-deposited on a new set of debit cards and transferred to the OCGs (usually located abroad).

In similar schemes, funds from e-wallets were exchanged into Bitcoins via virtual currency exchangers. The Bitcoins were used to pay salaries to members of the drug trafficking organisation. This included low-level members, such as small dealers and runners who facilitated the sale of drugs. The same financier worked with multiple owners of the Dark Web stores, distributing the laundered funds to the respective OCGs.

Note: 1. The term "straw men" refers to informal nominee shareholders and directors who are being controlled by the actual owner or controller of the company.

Source: The Russian Federation

Proxy Networks

Proxy networks are PMLs who supply a type of banking service to OCGs, generally through the use of multi-layered transfers via bank accounts. These specialised services offer all of the advantages that come with moving funds globally via the legitimate financial sector. The main task of these proxy networks is to move client funds to the final, pre-determined destination and to obfuscate the trail of the financial flows. In many cases, these schemes are supported by TBML mechanisms.

PML schemes that are arranged with the use of bank accounts consist of multiple layers of shell companies in different jurisdictions, which have been established purely to redistribute and mix funds from various sources. These shell companies could be located in the country where the predicate offence occurred, transit countries or countries where the final investment of funds is conducted. This scheme is designed to make the portion of funds that belong to a client untraceable. In most cases, laundered funds are transferred to a client's personal bank account(s), affiliated companies or foundations under their control, or handed over to them as physical cash.

In general, a cross-border ML scheme arranged by a proxy network has the following structure:

- **Step 1:** Clients' funds are transferred to accounts opened in the name of shell companies controlled by the PML, often through the use of legal entities controlled by them, or entities operating on their behalf. If the criminal proceeds were obtained in cash, controllers arrange to collect and deposit the cash into the accounts of PML-controlled shell companies.
- **Step 2:** Funds are moved through a complex chain of accounts established by domestic shell companies under fictitious contracts. The funds from different clients are mixed within the same accounts, which makes it difficult for investigators to trace the funds coming from a particular client.
- **Step 3:** Funds are transferred abroad under fictitious trade contracts, loan agreements, securities purchase agreements, etc. In most cases, accounts of the first-level layer of foreign companies are controlled by the same money launderers, who facilitated Step 1, or by foreign PMLs who act in collaboration with the domestic money launderers.
- **Step 4:** Funds are moved through a complex chain of international transfers. The ML infrastructure used (i.e. accounts set up by shell companies) is typically used to channel money that comes from all over the world. These

international money transfers often demonstrate similar geographical patterns.

- **Step 5:** Funds are returned to the accounts controlled by the initial clients, their close associates or affiliated legal entities and arrangements. Alternatively, the PML will purchase goods and services on behalf of the OCG. PMLs that arrange these schemes provide different reasons to justify or legitimise the wire transfers they conduct. These may include trade in various goods and services, import/export services, loans, consultancy services or investments. PMLs look for loopholes and other possible purposes for payments that give the veneer of legitimacy to these transactions. Bank accounts are chosen to make the activity appear legitimate, and to avoid suspicious transactions reporting and/or instances where the transaction are blocked by financial institutions. For example, PMLs use accounts of various characteristics (i.e. accounts where the activity volume was small, medium or large), in accordance with the sums laundered.

Box 7. Facilitating the Laundering of Proceeds from Bank Fraud

In 2015, Russian law enforcement authorities, in co-operation with the FIU and the Central Bank, disrupted a large-scale scheme to embezzle funds and subsequently conduct illicit cross-border transfers.

During the course of the investigation, it was established that OCG members assisted in stealing assets from a number of Russian banks. Typically, the bank management team knowingly granted non-refundable loans and conducted fictitious real estate deals, which led to the bank's premediated bankruptcy. Illicit proceeds were then moved abroad via accounts of shell companies.

Law enforcement authorities and the FIU, in co-operation with foreign counterparts, detected a wider scheme of illicit cross-border money transfers that was used to move proceeds from several predicate offences abroad. Funds were moved via accounts of domestic shell companies and offshore companies (registered in the UK, New Zealand, Belize and other jurisdictions), with their accounts held by banks in Moldova and Latvia, under the pretext of fictitious contracts and falsified court decisions.

One of the major launderers of this scheme received profits for his services in his own personal bank accounts from two offshore companies that were used in the scheme.

The OCG consisted of more than 500 members. Law enforcement authorities seized more than 200 electronic keys of online bank accounts; more than 500 stamps of legal entities; shadow accountancy documents, copies of fictitious contacts; and cash. Bank managers and other complicit individuals were arrested.

Source: The Russian Federation

Social engineering frauds and other types of Internet-based fraud are often a source of illicit proceeds that may be laundered through a proxy network:

Box 8. Creating Infrastructure to Launder Funds

This investigation was conducted by a specially designated Israeli Task Force for PML investigations, which includes members from the Israeli Police, Tax Authority, IMPA (FIU) and Prosecution. The investigation also involved the co-operation of LEAs in another country.

The suspects of the investigation were criminals conducting massive fraud and extortion, as well as PMLs, who assisted the predicate offenders in laundering the proceeds of crimes. Funds were laundered using shell companies established in Europe and the Far East. "Straw men," couriers and hawala-type services. The companies were established in advance in countries that were less susceptible for illegal activity in the eyes of the fraud victims.

The PML built the infrastructure that enabled the ML activity, which in turn was part of a global ML network. The PML, through the use of other individuals, opened foreign bank accounts, established foreign companies, and also used a repatriation network of foreign immigrants to move funds as part of the ML network.

The suspects transferred fraudulent proceeds to bank accounts opened in the name of the shell companies and straw men. The funds were then transferred to other bank accounts in the Far East and immediately the suspects withdrew money in cash by using couriers, hawala networks and MVTS providers in Israel to transfer the funds to their final destinations.

During the investigation, an Israeli suspect (one of the PMLs) was arrested by an LEA of a third country. This assisted the investigation in understanding the modus operandi of the PMLN. It was established that the PML of the network was also able to provide bank accounts of various characteristics (i.e. accounts where the activity volume was small, medium or large in accordance with the sums laundered). The bank accounts were thus chosen to make the activity look legitimate, avoiding unusual activity reports and/or instances where the transaction is blocked by the financial institution concerned.

Source: Israel

Proxy networks that facilitate cross-border movement of funds often tie into a wider network of other PMLs in several countries for the purpose of moving and laundering funds to and from the country where the predicate offence took place. PMLs who facilitate the outgoing flow of funds from the country where the predicate offence was conducted are typically part of a broader, global ML network that specialises in moving illicit proceeds around the globe. Some third-party money launderers, identified by responding countries, also acted through collaboration with other PMLs operating abroad which provided ML services at their request. The use of a global network of PMLs, located in different countries, as well as using different methods to transfer funds internationally, ensures the diversification of financial transactions and helps to limit the risk of detection. An analysis of proxy networks shows that PMLs may change their *modus operandi* and employ different contacts as needed.

Box 9. Large-Scale International Money Laundering Platform

A financial investigation was initiated into the embezzlement of public funds and suspected corruption, which led to the detection of a large-scale international ML platform that was used to move funds originating from different sources.

The proceeds of crime were moved to accounts of shell companies held with banks in Latvia, Cyprus and Estonia. The criminal proceeds were further transferred to accounts of companies controlled by the beneficiary's close associates and then moved back to Russia. Further investigation revealed that various companies used the same channel to move the funds.

A criminal proceeding on articles "Fraud", "Arrangement of organised criminal group" and "Money Laundering," according to the Criminal Code of the Russian Federation, was opened. The Central Bank of the Russian Federation withdrew the license of the Russian bank that facilitated frequent cross-border money transfers under fictitious contracts for violations of AML legislation. The European Central Bank also withdrew the license of a Latvian bank that facilitated the redistribution of criminal proceeds. A significant portion of funds was frozen on the accounts held by Latvian banks.

While the investigation of the case started with a particular predicate offence, it led to the identification of a wide international PML scheme that was used to move funds originating from various crimes. There are also indications that clients from other countries used this ML scheme. In a demonstration of the interconnectedness of PML, some companies involved in this scheme have financial links with a UAE company designated by the US in relation to the Altaf Khanani Money Laundering Organisation,[1] described in Box 1.

Note: 1. See Section III for the case study on this MLO.

Source: The Russian Federation

PML schemes and infrastructure can also be used to launder funds and to facilitate large-scale tax evasion schemes. In such schemes, multiple layers of shell companies may be used between the importer and producer of goods that are located abroad. Funds used for the purchase of foreign goods thus go through a complex chain of transactions, with only one portion of these funds used for the import deal. The rest is directed to accounts controlled by beneficiaries.

Proxy networks also use layering schemes to transform illicit proceeds generated within the financial system into cash. This is mostly arranged for those clients who need to move criminal proceeds from bank accounts to physical cash. The majority of such clients are involved in public funds embezzlement, tax fraud and cyber fraud schemes. At the final stage, funds are transferred to corporate bank cards, followed by subsequent cash withdrawals. The number of shell companies and personal bank accounts involved may exceed several thousands. This limits the risk of detection and diversifies possible losses.

In some cases, cash withdrawals may be conducted abroad. In one case, funds were channelled to accounts of companies registered in the Middle East, with subsequent

cash withdrawals via exchange houses. Cash was then transported back to the country of origin and declared on the border as profits from legitimate business activities in the Middle East, which were intended to be used for the purchase of real estate.

SECTION V: SUPPORTING MECHANISMS USED BY PROFESSIONAL MONEY LAUNDERERS

PMLNs use a wide variety of ML tools and techniques. Among the most significant mechanisms are TBML, account settlement mechanisms and underground banking.

Trade-Based Money Laundering (TBML)

TBML is defined as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin."[3] There are various TBML variations that can be employed by PMLs. These include:

- *The purchase of high-value goods using the proceeds of crime*, followed by the shipment and re-sale of goods overseas;
- *The transfer of funds which purport to be related to trade*, or to the purchase of goods that are ultimately never shipped or received (also known as "phantom shipments");
- *Falsifying the number and/or value of goods being shipped* to be higher or lower than the corresponding payment, allowing for the transfer or receipt of the value of proceeds of crime (also known as over or under-invoicing);
- *Using the proceeds of crime to purchase goods for legitimate re-sale*, with payment for goods made to drug traffickers/distributors by legitimate business owners (e.g. the Black Market Peso Exchange - BMPE); and
- *Using Money (Peso) Brokers*, who are third parties that seek to purchase drug proceeds in the location where illicit proceeds are earned by drug cartels (e.g. Colombia, Mexico) at a discounted rate. Money brokers often employ many individuals responsible for collecting narcotics proceeds and disposing of those proceeds, as directed by either the drug trafficking organisation or the money brokers who serve as PMLOs.

Box 10. ML Network, Operating as a Trade-Based ML Scheme1

Project OROAD was a joint task force financial investigation, launched from a drug investigation into ML activities of a suspicious group[2]. Information received from FINTRAC helped identify a complex TBML where two of the group's central figures hired 10 nominees to establish 25 shell companies. The shell companies were opened using names across a diverse number of

[3] FATF, 2006.

industries: landscaping, interior design, electronics, metal recycling, plastics recycling, construction supplies, beauty supplies, etc.

The laundering network included legitimate businesses, operating in the financial and real estate sectors, as well as a small financial company, which was complicit in laundering the funds. The money launderer provided his accomplice at the financial company with large bags of cash, which were then deposited into business accounts in the name of shell companies. This continued until the accounts were closed by the financial institution that held the shell company's accounts, due to a high volume of suspicious transactions.

Investigators believe the ML group used a TBML scheme. The ML operation and the network of shell companies were largely centred on a logistics company. One of the money launderers was seen leaving the logistics company location with large bags of bulk cash, which were believed to be the proceeds of drug sales. The money launderer used nominees to make multiple cash deposits into their personal and business accounts.

The money launderer instructed nominees to either i) transfer funds back to the logistics company; or ii) transfer funds to other business accounts, held by nominees located in Canada, China, Panama and the US. Funds were sent by wire transfer, bank draft or cheque, some of which were then returned to the logistics company. In each case, the money launderer used fraudulent invoices to account for the proceeds of drug sales so that they could be more easily integrated into the financial system.

Investigators believe that some of the funds were transferred back to the Mexican drug trafficking organisation and to other companies controlled by the drug trafficking organisation in China, Mexico and the US. In some cases, funds were used for to purchase goods located in Panama or Mexico. The ringleaders in Canada established companies in these countries in attempts to make the transfers seem legitimate. The purchased goods were then shipped to other foreign countries for sale. Once the purchased goods arrive at the destination country, they were sold, and the proceeds of the sale (in the destination country's currency) were then transferred to the drug trafficking or ML organisation to provide the criminals with "clean" funds, laundered through TBML.

Notes:

1 See case study "Operation Snake" in Section III, which involves another professional ML network using a TBML and MVTS scheme

2 The investigation also revealed a number of bulk cash transactions between the ring and illegal money brokers; however, the focus here is on the ML ring.

Source: Canada

PMLs may also create and use false documentation, layer related financial transactions and establish shell and/or shelf companies to facilitate purported trade transactions. By using TBML mechanisms, PMLs can break the link between the predicate crime and related ML, making it difficult to associate the criminals with the ML activity.

Box 11. Venezuelan Currency Smuggling Network

During 2015, 10 limited liability companies established by a single person in Spain processed more than 110 000 transactions, totalling EUR 22.4 million, through mobile payment "point of sale (POS)" terminals. Nine of these companies were purportedly active as travel agencies, eight shared the same registered offices and six had the same associate and director.

The POS terminals held by these companies exclusively accepted payment cards issued by the Venezuelan government (Comisión de Administración de Divisas - CADIVI). Given strict currency controls in Venezuela, residents can only obtain foreign currencies when traveling abroad. Therefore, a maximum of USD 3 000 at a rate of 6.3 bolivars per dollar can be exchanged. This led to a large currency exchange fraud called "el raspao," where Venezuelan residents accessed euros or dollars, under the false pretence of a journey abroad. The payment cards issued by the CADIVI, at the official exchange rate, were debited abroad while drug traffickers received the counter value in cash, in euro or dollar notes, which was then smuggled back into Venezuela and sold on the black market at a rate of about ten times the official exchange rate. Authorities in Luxembourg suspect that the payment cards issued by CADIVI were smuggled in bundles to Spain and swiped through the POS terminals of complicit traders who operated through Spanish front companies.

Drug traffickers and Colombian cartels are believed to have taken advantage of this currency smuggling network in order to repatriate the proceeds generated in cash through drug sales in Europe back to South America. These criminals washed their illicit cash by handing it out to Venezuelan currency traffickers. Once processed, the debited amounts were credited to linked bank accounts. These bank accounts had International Bank Account Numbers (IBANs), issued by a former Luxembourg-licensed electronic money remitter.

AML investigations by the regulator and the financial intelligence unit (FIU) revealed that the Luxembourg electronic money remitter did not manage these accounts itself, as stipulated in regulation, but handed them over to a Bulgarian-licensed electronic money remitter, which used the accounts for its own customers. The POSs were sold to the Spanish front companies by the Bulgarian electronic money remitter. Additionally, the Spanish front companies applied for hundreds of withdrawal cards (most front companies had more than 10 withdrawal cards each), issued by the Bulgarian electronic money remitter, in order to allow them to withdraw cash from their accounts. About 106 000 withdrawals, totalling more than EUR 20 million were made at ATMs situated in Colombia. These withdrawals did not comply with the daily, weekly and monthly limits as laid out in the general terms and conditions of the Bulgarian electronic remitter. Authorities in Luxembourg were not aware of any related suspicious transaction reports that were reported to the Bulgarian FIU. The Luxembourg and Bulgarian electronic remitters were held by the same beneficial owner. Commissions received by the Bulgarian electronic remitter on the operations totalled as much as EUR 1.9 million, or 9 % of the amounts processed through the POSs.

Source: Luxembourg

Account Settlement Mechanisms

PMLNs can facilitate the settlement of accounts between multiple OCGs. They may do this for OCGs operating in different countries that generate proceeds from cash and hold funds within bank accounts. A PML may, for example, simultaneously provide ML services to criminals who have cash and want to send funds to bank accounts in other countries, and to criminals who have money in their bank accounts but need cash (e.g. to pay their networks and workers). This *modus operandi* is called an *account settlement mechanism*.

The case, below, illustrates how a PMLO accepted and moved cash by car to Belgium, as part of an account settlement mechanism.

Box 12. Money Laundering as Part of an "Account Settlement Scheme" Between Various Criminal Organisations

Several Belgian corporate customers transferred funds to the accounts of Belgian construction or industrial cleaning companies and their managers. These companies had a similar profile: they operated in the same industry, the managers were often from the same country, the articles of association were copied with slight modifications, and the companies' financial health was poor. Some companies had already gone bankrupt or no longer complied with their legal requirements.

Funds were channelled through different accounts: Part of the funds credited to the accounts was withdrawn in cash, presumably to pay workers. Another part of the funds were transferred to companies located abroad, in Europe and in Asia.

The funds transferred to Europe were credited to the accounts of other companies in the same industry. Often no explanation was provided for these transfers, even though the scale was significant. The references accompanying these transfers, if any, were vague. The majority of the funds were subsequently withdrawn in cash.

The funds transferred to Asia, mainly China and Hong Kong, were credited to the accounts of limited liability companies, which were not linked to the construction or industrial cleaning industry in any way.

Information received from a counterpart FIU revealed links with a criminal organisation involved in drug trafficking. This organisation, which held large amounts of cash, used an organisation that laundered the funds and transported the cash to Belgium by car. In Belgium, intermediaries then handed over the cash to various companies in Belgium that required cash to carry out their activities.

Based on this information, authorities have concluded that the Belgian construction and industrial cleaning companies involved in this case were part of an account settlement scheme. The cash proceeds of drug trafficking were used to pay illegal workers of Belgian companies.

Source: Belgium

Underground Banking and Alternative Banking Platforms

Underground banking is one tool often used by PMLs. This mechanism is used, with the goal of bypassing the regulated financial sector and creating a parallel system of moving and keeping records of transactions and accountancy.

Box 13. Investigation of Massive Underground Banking System

Subject X and his network of associates in British Columbia, Canada, are believed to have operated a PMLO that offered a number of crucial services to Transnational Criminal Organisations including Mexican Cartels, Asian OCGs, and Middle Eastern OCGs. It is estimated that they laundered over CAD 1 billion per year through an underground banking network, involving legal and illegal casinos, MVTSs and asset procurement. One portion of the ML networks illegal activities was the use of drug money, illegal gambling money and money derived from extortion to supply cash to Chinese gamblers in Canada.

Subject X allegedly helped ultra-wealthy gamblers move their money to Canada from China, which has restrictions on the outflow of fiat currency. The Chinese gamblers would transfer funds to accounts controlled by Subject X and his network in exchange for cash in Canada. However, funds were never actually transferred outside of China to Canada; rather, the value of funds was transferred through an Informal Value Transfer System. Subject X received a 3-5% commission on each transaction. Chinese gamblers were provided with a contact, either locally or prior to arriving, in Vancouver. The Chinese gamblers would phone the contact to schedule cash delivery, usually in the casino parking lot, which was then used to buy casino chips. Some gamblers would cash in their chips for a "B.C. casino cheque", which they could then deposit into a Canadian bank account. Some of these funds were used for real estate purchases. The cash given to the high-roller gamblers came from Company X, an unlicensed MVTS provider owned by Subject X. Investigators believe that gangsters or their couriers were delivering suitcases of cash to Company X, allegedly at an average rate of CAD 1.5 million a day. Surveillance identified links to 40 different organisations, including organised groups in Asia that dealt with cocaine, heroin and methamphetamine.

After cash was dropped off at Company X, funds were released offshore by Subject X or his network. Most transactions were held in cash and avoided the tracking that is typical for conventional banking. Subject X charged a 5% fee for the laundering and transfer service. As the ML operation grew, the money transfer abilities of Company X became increasingly sophisticated to the point where it could wire funds to Mexico and Peru, allowing drug dealers to buy narcotics without carrying cash outside Canada in order to cover up the international money transfers with fake trade invoices from China. Investigators have found evidence of over 600 bank accounts in China that were controlled or used by Company X. Chinese police have conducted their own investigation, labelling this as a massive underground banking system.

Source: Canada

An *alternative banking platform (ABP)* is an alternative bank that operates outside the regulated financial system. However, an ABP may use the facilities of the formal banking system, while creating a parallel accountancy and settlement system. ABPs are a form of shadow banking that make use of bespoke online software to provide banking services, without the regulated and audited customer due diligence checks. They are an effective way to transfer the ownership of money anonymously and provide banking services within a bank account across a number of individuals, without being reflected in traditional banking transactions. Usually, it is supported with special software that can encrypt traffic, manage transactions between accounts within the same platform, apply fees and assist with interaction with the outside financial system.

Box 14. Alternative Banking Platforms

An alternative banking platform (ABP) was used to assist organised crime groups (OCGs) in the UK to launder funds from VAT fraud. The ABP had a registered office in one jurisdiction with a holding company in a second jurisdiction and a bank account in a third jurisdiction. It was operated by a PMLN based in a fourth jurisdiction all outside of the UK. The ABP was used for a year with over EUR 400 million moved through it. The ABP was shut down and the creator of the financial software was arrested by international partners, with assistance from Her Majesty's Revenue and Customs (HMRC). The data gathered from the ABP servers was used to identify other ABPs and develop additional cases.

Source: United Kingdom

In some cases, PMLs use specialised software to create an ML scheme to move funds randomly through numerous accounts. This software is generally based on a random data generator principle.

SECTION VI: COMPLICIT/CRIMINAL FINANCIAL SERVICE PROVIDERS AND OTHER PROFESSIONALS

As mentioned in **Section II**, PMLs may occupy positions within the financial services industry (e.g. bankers and MVTS agents) and DNFBP sectors (e.g. lawyers, accountants and real estate professionals), and use their occupation, business infrastructure and knowledge to facilitate ML for criminal clients. The use of occupational professionals can provide a veneer of legitimacy to criminals and OCGs. As such, OCGs actively seek out insiders as potential accomplices to help launder illicit proceeds. In rare instances, complicit actors who facilitate PML schemes come from within a government institution (i.e. a corrupt official).

Box 15. Corrupt Official Joining Criminal Enterprise to Launder Funds

Ukraine's law enforcement and prosecution services conducted an investigation of a high-ranking official who abused his power and official position for approximately three years. The official agreed to participate in the

creation of a criminal organisation and implemented an illegal scheme for minimising tax liabilities, which led to the illegal use of a tax credit. The public official received a cash fee for his services, which were performed with the participation of other public officials and other members of the criminal organisation.

The public official conducted a number of functions to make illicit proceeds appear legitimate, including creating, registering and owning a number of shell companies on behalf of members of the criminal organisation and purchasing property on their behalf. The official also established offshore companies in Cyprus and the BVI using his relatives as nominees. The high-ranking official also acquired entities registered in Ukraine, which were controlled by his offshore companies, by transferring funds from a bank in Liechtenstein. Funds transferred into Ukraine were used to purchase property. Fictitious contacts or agreements (e.g. for consultation services) were also established using a network of fictitious entities for services that were never rendered.

Source: Ukraine

PMLs often ignore or circumvent AML/CFT requirements or actively conceal AML/CFT failures within a particular institution or business. They may also ignore professional obligations, such as restrictions associated with their licenses or professional ethics rules. While the exact definition of complicity is a matter of domestic law, it is widely understood as intentional acts carried out with knowledge or wilful blindness of the illicit nature of the funds with which the person is dealing. The ability of a criminal to purchase or gain ownership or control of a financial business is the ultimate measure of success.

Criminals will actively seek to recruit complicit insiders within existing institutions or businesses, since these individuals have insider access and may be able to falsify records or initiate transactions in a manner, which bypasses AML/CFT regulations or institutional practices. In rare circumstances, criminals may be able to compromise entire institutions or businesses, including by acquiring ownership or control of the institution and appointing their own criminal management. The complicit activity described above (insider compromise and institutional compromise) should not be confused with instances of lax compliance, weak internal controls or inadequate corporate governance structures, which can result in compliance deficiencies with AML/CFT requirements. A reputation for weak compliance, however, may make the institution more attractive for an OCG seeking out a corrupt insider.

Money Value Transfer Services (MVTS) Providers

Case studies and insight provided by delegations show that MVTS providers have knowingly facilitated PML activities, including currency conversions (i.e. foreign exchange), cash-based transactions, and/or electronic funds transfers. Complicit MVTS providers can play an important role in the placement stage of the ML process. The most common ML transactions facilitated by MVTS providers are:

- cash purchases of funds transfers at the physical location of MVTS providers;

- large cash deposits made in the accounts of individuals and businesses followed by a domestic transfer to the account of an MVTS provider, or the purchase of bank drafts (e.g. cashier's check) payable to an MVTS provider; and
- the purchase of bank drafts for the benefit of individuals and businesses, which are negotiated by MVTS providers to fund the purchase of funds transfers.

Box 16. Use of Foreign Exchange Broker and "Quick Drop" Facilities

A mechanic in the UK acted as a professional launderer for an unknown PMLN. The mechanic opened bank accounts in the UK, which were used to deposit GBP 5.3 million in cash between October 2013 and December 2014. Multiple deposits of GBP 25 000 were paid into the bank accounts per day using bank 'quick-drop' facilities. Once paid into the bank accounts, money was transferred to third-party bank accounts held in the UK and six other jurisdictions using bank and foreign exchange broker transfers. The mechanic was paid GBP 20 000 for moving the cash abroad. The launderer pleaded guilty to three charges of ML and, in April 2018, was sentenced to six years in jail and banned from being a company director for nine years.

Quick drop is a facility to deposit, cash either at the bank directly or at a third-party facility, where the money is counted and then transferred to the bank to be deposited[4]. Quick drop facilities allow cash to be deposited quicker, at more locations and often without coming into contact with staff.

Source: United Kingdom

Analysis conducted by some competent authorities indicates that complicit MVTS providers may continue to file suspicious transaction reports (STRs). For example, STRs may be filed so as not to arouse suspicion or give the perception that the MVTS provider is otherwise compliant. In jurisdictions that require other forms of transaction reporting, such as threshold cash transactions, complicit MVTS may operate two sets of account records (i.e. shadow accountancy), one of which is used exclusively for criminal clients and for which no reports are filed. Alternatively, these complicit MVTS providers may report the transactions using fictitious transaction details.

Box 17. Complicit MVTS Agents to Facilitate Third-Party ML

The Italian FIU identified a significant reduction in remittances sent to Country "A" within a three year period (from EUR 2.7 billion in 2012 to EUR 560 million in 2015). This data highlighted the specific exposure of this 'corridor' to the risk of channelling illegal funds.

Further analysis of STRs led to the detection of alternative channels, used by

[4] UK National Risk Assessment of Money Laundering and Terrorist Financing, October 2015

PMLNs, to transfer significant amounts to Country A. A significant portion of the reduction of remittances towards Country A was related to the migration of many Italian MVTS agents towards foreign ones that do not produce statistical reports under national legislations, and are not subject to Italian AML and fiscal requirements.

The FIU received many STRs concerning suspicious activity traced back to Italian money transfer agents. Financial flows were mainly characterised by significant cash deposits and wire transfers in favour of the Italian bank accounts of the foreign MVTS. Such financial flows allegedly referred to money remittances performed by MVTS agents. However, suspicion was triggered given that the agents sometimes deposited cash into their accounts through a branch of the bank located far away from their business. The FIU extended its studies to gain a better understanding of financial flows performed by the MVTS and agents, which revealed that in some cases:

- the MVTS legal representatives were involved;
- the MVTS had been recently incorporated;
- the MVTS had links to subjects originating from Country A;
- the MVTS had opened a branch in an Italian city that is well known for its growing economic and business links with Country A;
- many agents of the same foreign MVTS – all originating from Country A – had already been reported to the Italian FIU or had been prohibited from performing agent activities by the competent financial supervisory authority of Country A, for anomalous transactions and use of false ID documents for CDD purposes;
- the MVTS agents allowed their customers to structure transactions by splitting up remittances with several accomplices; and
- certain MVTS agents revealed tangible links to a common customer base.

In view of analysis carried out, the MVTS provider and agents were found to have disregarded AML obligations, exploiting asymmetries in the regulatory framework among different countries. A well-organised, skilled and complicit network of agents and foreign MVTS had been used to collect funds in Italy, and to transfer significant amounts abroad, splitting up remittances with several accomplices.

Source: Italy

Financial Institutions

The use of the international financial system has been instrumental in facilitating large-scale PML schemes. All of the complex layering schemes described in **Section IV** involve moving significant volumes of funds through various bank accounts in different jurisdictions opened on behalf of shell companies. These well-structured schemes often go undetected by banks, even in situations where there is an insider involved.

Investigative authorities have been able to detect patterns in how PMLs choose certain jurisdictions and banks that are used to move illicit proceeds. For example,

some criminals seek to use banks that operate in lax regulatory environments or have reputations for non-compliance with AML/CFT regulations.

It is challenging for competent authorities to establish factual evidence, which demonstrates that financial institutions are actively complicit in facilitating ML. Bank insiders generally do not communicate openly about their criminal conduct and may be able to leverage their insider status to conceal misdeeds. This can make it difficult to detect and prosecute wilful misconduct by complicit financial services professionals. A range of employees within financial institutions (from lower-level tellers to higher-level management) pose a significant vulnerability that can be exploited by money launderers, but also senior insiders who knowingly assist in ML may cause more damage.

Complicit bank employees may perform functions such as:

- Creating counterfeit checks;
- Monitoring (or not appropriately monitoring) money flows between accounts controlled by the co-conspirators;
- Co-ordinating financial transactions to avoid STR reporting;
- Accepting fictitious documents provided by clients as a basis for transactions, without asking any additional questions; and
- Performing 'virtual transactions' on the accounts of their clients – numerous transactions conducted, without an essential change of the net balance at the beginning and end of a working day.

Box 18. General Manager and Chairman of a Foreign Bank

An investigation by Italian authorities uncovered various ML operations that were carried out by senior foreign bank officials (general manager and chairman), together with a complicit accountant and a lawyer. The illicit proceeds were derived from an international cocaine trafficking organisation.

The criminals were put in contact with the general manager and the chairman of the foreign bank, which was experiencing a serious liquidity crisis at the time. The criminals and the bank executives agreed that one of the drug traffickers would deposit, in his own name, about EUR 15 million at the bank in crisis. This bank committed to provide the two professionals (the lawyer and accountant, noted above, who were also brothers) with a given amount of money in compensation for the intermediation work they performed, to be credited to accounts specifically opened in their names at the bank.

The accountant was also in charge of performing accounting tasks for several companies belonging to the drug trafficker. Following the intermediation activity, the bank's general manager received EUR 1.3 million, in two instalments, from a deposit made in the name of the drug trafficker. Subsequently, the bank's general manager, with the approval of the bank's chairman, started complex financial operations aimed at concealing the unlawful origin of the money deposited.

Authorities were able to ascertain the role played by the lawyer, leaving no

doubt as to his function as an intermediary between his client (custodian) and the bank, and the lawyer's knowledge of the actual illicit source of the money involved.

Source: Italy

The case below demonstrates a combination of different elements and tools, including the sale of shell companies, facilitation of transactions by complicit bank employees and the execution of deals on securities markets.

Box 19. Complicit Bank Employees, Securities Market Deals and the Sale of Shell Companies

An investigation by Russian authorities, conducted in co-operation with foreign FIUs, uncovered an ML and tax evasion scheme that was arranged by complicit bank employees and brokers.

Funds accumulated in bank accounts of shell companies were transferred abroad under the pretext of securities purchases by order of broker "R." At the same time, two broker companies operating on the London Stock Exchange sold shares for the same price, thus facilitating the transfer of money via mirror trading.

All limited liability companies used in this scheme were established by a legal service firm, specialising in the sale of "off-the-shelf" companies. Criminal proceedings were opened. The licenses of one of the banks that facilitated cross-border transfers, and of the securities company, were withdrawn for violations of the AML legislation.

Source: The Russian Federation

1. The cases analysed and information received also demonstrated that private banking advisors may act as PMLs and provide services to conceal the nature, source, ownership and control of the funds in order to avoid scrutiny, by employing various techniques, including:

- Opening and transferring money to and from bank accounts held in the names of individuals or offshore entities, other than the true beneficial owners of the accounts;
- Making false statements on bank documents required by the bank to identify customers and disclose the true beneficial owners of the accounts;
- Using "consulting services" agreements and other similar types of contracts to create an appearance of legitimacy for illicit wire transfers;
- Maintaining and using multiple accounts at the same bank so that funds transfers between those accounts can be managed internally, without reliance on international clearing mechanisms that are more visible to law enforcement authorities; and

- Opening multiple bank accounts in the names of similarly-named companies at the same, or different, institutions so wires do not appear to be coming from third parties.

Legal and Professional Services

In order to place greater distance between their criminal activity and the movement of funds, some OCGs use the services of third-party money launderers, including professional gatekeepers, such as attorneys, accountants and trust and company service providers (TCSPs). One delegation noted that OCGs tend to use professional service providers to set up corporate structures, and that accountants are favoured due to the range of skills and services that they may provide. There are case examples demonstrating that these types of professionals have been recruited to work as PMLs on behalf of larger criminal enterprises, such as DTOs. FATF's 2013 Report on *ML and TF Vulnerabilities of Legal Professionals* mentions that criminals often seek out the involvement of legal professionals in their ML/TF activities because they may be required to complete certain transactions or provide access to specialised legal and notarial skills and services, both of which can assist the laundering of the proceeds of crime

Box 20. A Complicit Lawyer and Bank Employee

A lawyer in Texas was convicted for laundering money for an OCG and engaging in a variety of fraud schemes. The OCG operated in the US, Canada, Africa, Asia and Europe. A complicit bank employee was also convicted for her role in creating counterfeit checks and monitoring money flows between the numerous accounts controlled by the OCG.

All of the victims of these various fraud schemes were instructed to wire money into funnel accounts held by other co-conspirators (money mules), who then quickly transferred the money to other US accounts as well as accounts around the world before victims could discover the fraud. Several millions of dollars were laundered in this manner. The numerous bank accounts opened by the mules served as the initial "layer" in the laundering process, which allowed co-conspirators to distance or conceal the source and nature of the illicit proceeds. For example, during a one-year period, a key money mule opened 38 fraudulent bank accounts.

The fraud schemes took several forms. Many victims were law firms that were solicited online provided counterfeit cashier's checks for deposit into the firms' trust accounts. The law firms were then directed to wire money to third-party shell businesses controlled by the co-conspirators. The fraud conspiracy also employed hackers who compromised both individual and corporate e-mail accounts, ordering wire transfers from brokerage and business accounts to shell accounts controlled by co-conspirators. The shell companies were incorporated in Florida with fictitious names and then used to open bank accounts at banks in Florida in those names.

The licensed attorney in Texas worked for the co-conspirators by laundering victim money through an interest on lawyers trust account (IOLTA). He also

met with individual money mules to retrieve cash from their funnel accounts. The lawyer recruited his paralegal and others to open accounts used in the laundering scheme.

Source: United States

One case involves a licensed attorney who was considered a full member of an OGC. As in the case above, the attorney facilitated ML services by using his interest on lawyers trust account, or ILOTA[5], to transfer the proceeds of drug trafficking and fraud.

Box 21. Operation CICERO

This case was initiated by a special currency police unit within the Guardia di Finanza as a follow-up investigation to a judicially authorised search conducted on the boss of a major organised crime group (La Cosa Nostra or LCN) in Palermo, Italy. This investigation was aimed at identifying those individuals acting as nominees, as well as individuals who facilitated the movement of criminal proceeds on behalf of LCN. The investigation identified that a well-known lawyer was the beneficial owner of the companies used to launder funds via a Palermo-based construction company, which was linked to family members of the organised crime boss.

The lawyer performed a "money box" function for the LCN, which consisted of managing the financial resources of the crime group with the purpose of concealing the origins of the illicit proceeds and avoiding detection by authorities of any assets purchased from these proceeds. Through his professional relationships, the lawyer developed and tapped into an elite social network, which he also made available to the organised crime group.

The lawyer, who was operating as a PML, conducted a number of services, such as: (a) obtaining a mortgage to purchase an apartment with EUR 450 000 in criminal proceeds on behalf of an organised crime family member; (b) using a fictitious contract to purchase an apartment with EUR 110 000 on behalf of the organised crime group; and (c) layering and integrating legal funds with criminal assets derived from construction work carried out on land purchased with criminal proceeds.

This investigation led to confiscation proceedings against nine individuals totalling EUR 550 000 as well as seven properties owned by the lawyer.

Source: Italy

[5] An IOLTA is an account opened by an attorney with the intention of holding client funds for future services. It is opened at a bank with a presumed higher level of confidentiality accorded to attorney-client relationships and related transactions.

PMLs also often use shell companies to facilitate complex ML schemes. Professional services may be used, such as the services of a TCSP or a lawyer, when setting up a shell company. Such professionals can supply a full range of services, including the incorporation of the company, the provision of resident or nominee directors, and the facilitation of new bank accounts.

Box 22. Use of Shell Companies and Accountant Providing Corporate Secretarial Services

Person G was a chartered accountant in the business of providing corporate secretarial services to small and medium-sized enterprises. As part of these services, he incorporated companies on behalf of his clients and acted as the resident director of companies whose directors were not ordinarily residents in Singapore.

Persons N and S, members of a foreign syndicate, approached Person G to set up three companies, Company K, Company W and Company M, and to apply for their corporate bank accounts in Singapore. Once the accounts were set up, Persons N and S left Singapore and never returned. Person G was appointed the co-director of the three companies; although, he was neither a shareholder, nor the authorised bank signatory of these companies.

These companies received criminal proceeds in their bank accounts derived from various frauds amounting to over SGD 650 000. The funds were quickly transferred by Person S to overseas bank accounts.

The companies had committed the offence of transferring benefits of criminal conduct, attributable to Person G's neglect. There was a lack of supervision by Person G over the companies' affairs, which allowed the foreign syndicate to have unfettered control over the companies and partake in their ML activities unimpeded. In January 2016, G was convicted of ML offences and for failing to exercise reasonable diligence in discharging his duties as a director. He was sentenced to a total jail term of 12 months, fined SGD 50 000 and disqualified from acting as a company director for the five years following his sentence.

Source: Singapore

After opening bank accounts in the name of shell companies, professional launderers may operate these accounts from overseas, receiving criminal proceeds from different individuals and companies to layer funds. The funds received in the shell companies' accounts are usually transferred out of the jurisdiction within a few days.

TCSPs are often blind to what their clients actually use the companies for, and therefore do not consider themselves complicit in ML schemes. However, a number of case studies have demonstrated that some TCSPs market themselves as 'no questions asked,' or being immune from official inquires. Moreover, if the TCSP also acts as the director of the company, the TCSP has to perform these duties as a director and could be held liable for the offences committed by the company, as illustrated in the above case study.

Law enforcement agencies worldwide have noted that corporate structures are often used in PML schemes and that professional service providers are used in setting up structures. Law enforcement agencies have identified the use of complex corporate structures and offshore vehicles to conceal the ownership and facilitate the movement of criminal proceeds and that PMLNs exploit some TSCP services in the creation of structures. A handful of current investigations across the globe have indicated that TCSPs act as nominee directors of corporate structures with similar behaviours, observed whether large corporates or smaller TCSPs, including:

- using a 'tick the box' approach for compliance activity;
- distancing themselves from risk (i.e. downplay their responsibility);
- utilising chains of formation agents in multiple jurisdictions;
- engaging in deliberately negligent behaviour; and
- forging signatures and fraudulently notarising documents.

Box 23. Money Laundering through Real Estate Investments, Gastronomic Services and Show Production Services Linked With Drug Trafficking

An investigation was triggered by information received from OFAC, which revealed that an illicit network was conducting business activities in Argentina. This network was linked to an individual, J.B.P.C., who was suspected of being a member of a criminal organisation.

J.B.P.C., his family and business partners were also shareholders in a number of companies around the globe. More specifically, three Argentine companies (two operating companies and a management company) were suspected of developing ambitious real estate projects across the country. The president and main shareholder of those companies was Mr. B, a lawyer and friend of J.B.P.C. This person provided knowledge and experience on how to develop the businesses. Additional analysis revealed that J.B.P.C. was the shareholder of two other companies, which appeared as owners of the land where major real estate developments were to be undertaken.

Tax information that was collected by authorities revealed that these companies received accounting advice from Mr. C, who was a chartered accountant. He was also a shareholder and member of the Board of Directors of the concerned companies. Other transactions from J.B.P.C. were also detected during the same period. They were linked to two additional Argentine companies that provided bar services, coffee services and show production services. For one of the OFAC listed companies, it was discovered that the stock of the company was owned in its entirety by J.B.P.C.'s closest relatives. Likewise, management positions were occupied by his partners and close relatives. Another company, also with ties to J.B.P.C., opened an office in Argentina with the help of another lawyer, Mr. D.

The investigation into this case was conducted by FIU-Argentina in co-ordination with other domestic LEAs, as well as foreign counterparts in

Colombia (FIU-Colombia) and the United States (OFAC and DEA). Strong international co-operation was crucial to the success of this investigation, and joint efforts led to a significant number of simultaneous searches in Argentina, as well as in the other foreign jurisdiction where J.B.P.C. ran a majority of his illegal business. As a result, J.B.P.C., Mr. B and his spouse, Mr. C and Mr. D were arrested. Their property was also seized. Currently, they are facing prosecution in Argentina.

Source: Argentina

Payment Processing Companies

Payment processing companies provide payment services to merchants and other business entities, such as credit card processing or payroll processing services. Typically, bank accounts held by payment processors are used to facilitate payments on behalf of their clients. In certain circumstances, payment processing companies essentially act as "flow-through" accounts – there is no requirement for them to divulge the identities of their individual clients to financial institutions. Traditionally, payment processing companies were established to process credit card transactions for conventional retail outlets. However, over time, payment processing companies have evolved to serve a variety of domestic and international merchants, including Internet-based and conventional retail merchants, Internet gaming enterprises and telemarketing companies.

Payment processing companies can be used by criminal organisations to mask transactions and launder the proceeds of crime. For example, payment processing companies have been used to place illicit proceeds that originated from foreign sources directly into financial institutions[6].

A number of countries have observed the use of payment processing companies by suspected ML networks. In other instances, telemarketing companies have also been suspected of providing payment processing services, where illicit proceeds are co-mingled with payments suspected of being related to mass marketing fraud. Authorities suspect that these types of payment processors may be used by members and associates of multiple transnational OCGs.

Box 24. International Payment Processor Providing ML Services

PacNet, an international payment processor and MVTS provider based in Vancouver, Canada, helped dozens of fraudsters gain access to US banks. PacNet has a 20-year history of engaging in ML and mail fraud, by knowingly processing payments on behalf of a wide range of mail fraud schemes that target victims throughout the world. When it was shut down, PacNet consisted of 12 individuals and 24 entities across 18 countries. The network collectively has defrauded millions of vulnerable victims across the US out of hundreds of

[6] FINCEN, 2012 and FFIEC, nd.

millions of dollars.

With operations in Canada, Ireland and the UK, and subsidiaries or affiliates in 15 other countries, PacNet was the third-party payment processor of choice for perpetrators of a wide range of mail fraud schemes. US consumers receive tens of thousands of fraudulent lottery and other mail fraud solicitations nearly every day that contain misrepresentations designed to victimise the elderly or otherwise vulnerable individuals.

PacNet's processing operations helped to obscure the nature of the illicit funds and prevented the detection of fraudulent schemes. In a typical scenario, scammers mailed fraudulent solicitations to victims and then arranged to have victims' payments (both checks and cash) sent directly, or through a partner company, to PacNet's processing operations. Victims' money, minus PacNet's fees and commission, were made available to the scammers through wire transfers from the PacNet holding account, as well as by PacNet making payments on behalf of the scammers, thereby obscuring the link to the scammers. This process aimed to minimise the chance that financial institutions would detect the scammers and determine their activity to be suspicious.

The mail schemes involved a complicated web of actors located across the world and each scheme followed a similar pattern. These schemes involve a consortium of entities, including direct mailers, list brokers, printer/distributors, mailing houses, "caging" services[7], and payment processors. These six diverse groups worked together to (i) mail millions of solicitation packets each year, (ii) collect and distribute tens of millions of dollars in annual victim payments, and (iii) attempt to obscure their true identities from victims and law enforcement agencies worldwide.

Source: United States

Virtual Currency Payment Products and Services (VCPPS)

As noted in **Section IV**, PMLs offer a variety of services including the use of virtual currency in an attempt to anonymise those committing crimes and their illicit transactions. The use of complex, computer-based fraud schemes has led cyber criminals to create large-scale mechanisms to move the proceeds earned from these schemes. More specifically, virtual currency exchangers have been used as unlicensed or unregistered MVTS providers to exchange criminal proceeds in the form of virtual currency to fiat currency. In 2015, FATF issued guidance to demonstrate how specific FATF Recommendations should apply to convertible virtual currency exchangers in the context of VCPPS, and identify AML/CFT

[7] The processing of responses to direct mail is often conducted by a third party hired to perform various services, which may include processing payments, compiling product orders, correcting recipient addresses, processing returned mail, providing lockbox services, and depositing funds and the associated data processing for each of these services. Caging is a shorthand term for the service bundle.

measures that could be required[8]. Case studies have nonetheless shown that complicit virtual currency exchangers, which have been intentionally created, structured, and openly promoted as criminal business ventures, are being used.

Digital payment systems can also facilitate other crimes, including computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption and drug trafficking. Complicit virtual currency providers also utilise shell companies and affiliate entities that cater to an online, worldwide customer base to electronically transfer fiat currency into, and out of, these exchangers (effectively serving as electronic money mules). Users of these complicit services have openly and explicitly discussed criminal activity on these providers' chat functions, and their customer service representatives have offered advice on how to process and access money obtained from illegal drug sales on Dark Web markets.

Box 25. Complicit Virtual Currency Exchanger

On July 26, 2017, a grand jury in the Northern District of California indicted a Russian national and an organisation that he allegedly operated, BTC-e, for operating an unlicensed money services business, ML and related crimes. The indictment alleges that BTC-e was an international ML scheme that allegedly catered to criminals, particularly cyber criminals, and evolved into one of the principal means by which criminals around the world laundered the proceeds of their illicit activity. The indictment alleges that one of the operators of BTC-e who directed and supervised BTC-e's operations and finances, along with others, intentionally created, structured, operated and openly promoted BTC-e as a criminal business venture, developing a customer base for BTC-e that was heavily reliant on criminals. BTC-e was also one of the world's largest and most widely used digital currency exchangers. The investigation has revealed that BTC-e received more than USD 4 billion worth of virtual currency over the course of its operations. In addition to the indictment charging BTC-e and one of its operators with the violations noted above, FinCEN – in close co-ordination with the Justice Department – assessed a USD 110 million civil money penalty against BTC-e for wilfully violating US. anti-money-laundering laws.

Source: United States

SECTION VII: CONCLUDING REMARKS

This threat report addresses criminal actors, including organised crime groups that specialise in the provision of professional money laundering services and complicit actors who are knowingly involved, or are deliberately negligent, in the laundering process. A number of characteristics have been identified, based on an extensive case review (including, the role and functions of PMLs; the business models used; and relevant typologies and schemes). A non-public version of the report is available to Members of the FATF and the FATF Global Network upon request. This non-

[8] FATF, 2015.

public version includes further information, such as practical recommendations for the detection, investigation, prosecution and prevention of ML.

REFERENCES

FATF (2006), *Trade-Based Money Laundering*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html

FATF (2012a), *FATF Recommendations*, FATF, Paris, France, www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FATF (2012b), *FATF Guidance on Financial Investigations*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/operationalissues-financialinvestigationsguidance.html

FATF (2013a), *FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems – FATF Methodology*, FATF, Paris, France, www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

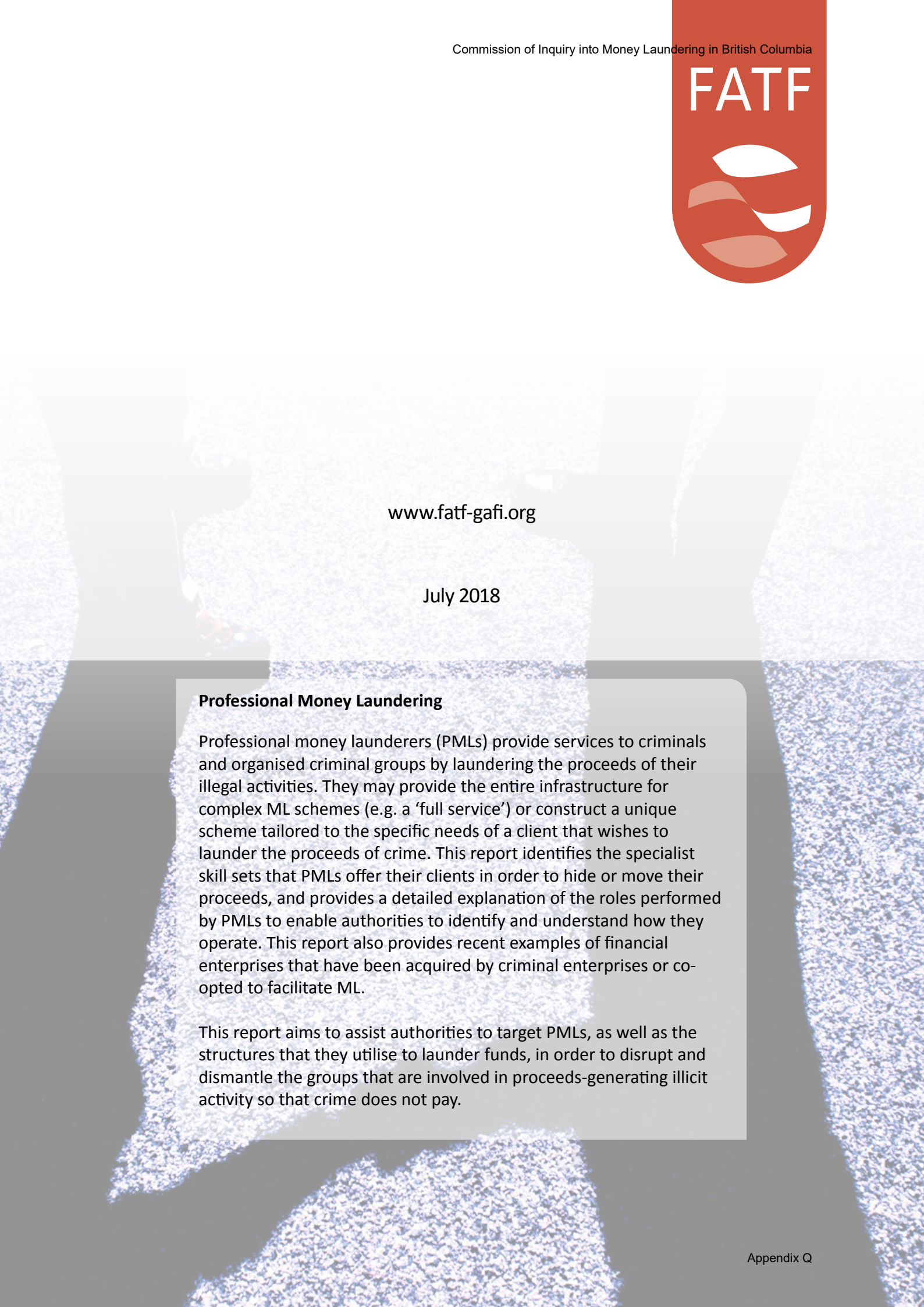
FATF (2013b), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals,* FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html

FATF (2015), *Guidance for a Risk Based Approach to Regulating Virtual Currency*, FATF, Paris, France www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

FATF – Egmont Group (2018), Concealment of Beneficial Ownership, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html

FFIEC (nd), Bank *Secrecy Act, Anti-Money Laundering Examination Manual, Third-Party Payment Processors—Overview,* Bank Secrecy Act/Anti-Money Laundering InfoBase, Federal Financial Institutions Examination Council: www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm

FINCEN (2012), *Risk Associated with Third-Party Payment Processors,* FIN-2012-A010. October 22, 2012, Department of the Treasury – Financial Crimes Enforcement Network, Washington, United States, October 22, 2012, https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A010.pdf



www.fatf-gafi.org

July 2018

Professional Money Laundering

Professional money launderers (PMLs) provide services to criminals and organised criminal groups by laundering the proceeds of their illegal activities. They may provide the entire infrastructure for complex ML schemes (e.g. a 'full service') or construct a unique scheme tailored to the specific needs of a client that wishes to launder the proceeds of crime. This report identifies the specialist skill sets that PMLs offer their clients in order to hide or move their proceeds, and provides a detailed explanation of the roles performed by PMLs to enable authorities to identify and understand how they operate. This report also provides recent examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate ML.

This report aims to assist authorities to target PMLs, as well as the structures that they utilise to launder funds, in order to disrupt and dismantle the groups that are involved in proceeds-generating illicit activity so that crime does not pay.

Appendix R:

FATF, *FATF Report: Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (Paris: FATF, 2013)

FATF

FATF REPORT

Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals

June 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

ACRONYMS

AML/CFT	Anti-money laundering/counter financing of terrorism
APG	Asia/Pacific Group on Money Laundering
CDD	Customer due diligence
CFATF	Caribbean Financial Action Task Force
DNFBPs	Designated non-financial businesses and professions
ECHR	European Convention on Human Rights
FIU	Financial intelligence units
GIABA	Intergovernmental Action Group against Money Laundering in West Africa
GIFCS	Group of International Finance Centre Supervisors
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money laundering
OECD	Organisation for Economic Co-operation and Development
PEP	Politically exposed person
SRBs	Self-regulatory bodies
STR	Suspicious transaction report
TF	Terrorist financing

EXECUTIVE SUMMARY

In June 2012, the Financial Action Task Force (FATF) Plenary met in Rome and agreed to conduct typology research into the money laundering and terrorist financing (ML/TF) vulnerabilities of the legal profession.

Since the inclusion of legal professionals in the scope of professionals in the FATF Recommendations in 2003, there has been extensive debate as to whether there is evidence that legal professionals have been involved in ML/TF and whether the application of the Recommendations is consistent with fundamental human rights and the ethical obligations of legal professionals.

The purpose of this typology is to determine the degree to which legal professionals globally are vulnerable for ML/TF risks in light of the specific legal services they provide, and to describe red flag indicators of ML/TF which may be useful to legal professionals, self-regulatory bodies (SRBs), competent authorities and law enforcement agencies.

This typology report does not offer guidance or policy recommendations, nor can it serve as a "one-size-fits-all" educational tool for individual legal professionals practicing in different settings, across countries with varying supervisory regimes and secrecy, privilege and confidentiality rules.

The report concludes that criminals seek out the involvement of legal professionals in their ML/TF activities, sometimes because a legal professional is required to complete certain transactions, and sometimes to access specialised legal and notarial skills and services which could assist the laundering of the proceeds of crime and the funding of terrorism.

The report identifies a number of ML/TF methods that commonly employ or, in some countries, require the services of a legal professional. Inherently these activities pose ML/TF risk and when clients seek to misuse the legal professional's services in these areas, even law abiding legal professionals may be vulnerable. The methods are:

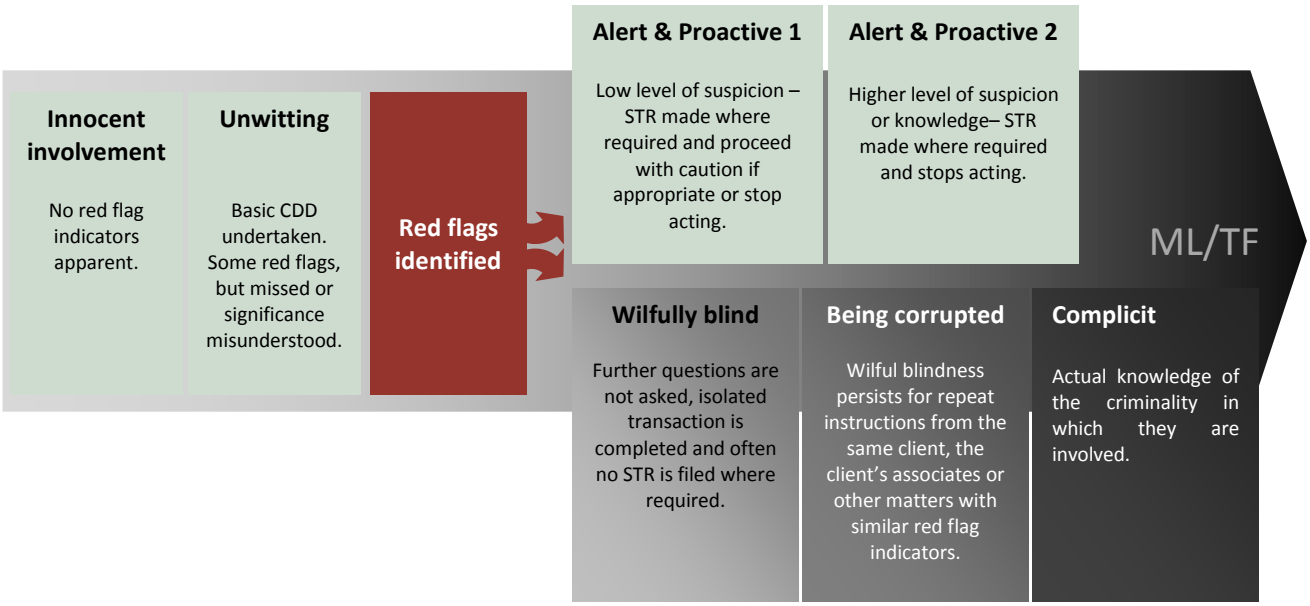
- misuse of client accounts;
- purchase of real property;
- creation of trusts and companies;
- management of trusts and companies;
- managing client affairs and making introductions;
- undertaking certain litigation; and
- setting up and managing charities.

In this report, over 100 case studies referring to these and other ML/TF methods were taken into account. While the majority of case studies in this report relate to ML activity, similar methodologies are capable of being used for TF activity.

While some cases show instances where the legal professional has made a suspicious transaction report (STR), a significant number involve a prosecution or disciplinary action, so a higher standard

of intent had to be proven, meaning those cases were more likely to involve a legal professional who was or became complicit. From reviewing the case studies and literature as a whole, the involvement of legal professionals in the money laundering of their clients is not as stark as complicit or unwitting, but can best be described as a continuum.

Involvement of Legal Professionals in money laundering and terrorist financing (ML/TF)



Red flag indicators relating to the client, the source of funds, the type of legal professional and the nature of the retainer, were developed with reference to these cases and educational material provided by SRBs and competent authorities. Whatever the involvement of the legal professional, the red flag indicators are often consistent and may be useful for legal professionals, SRBs, competent authorities and law enforcement agencies. Red flag indicators should be considered in context and prompt legal professionals to undertake risk-based client due diligence. If the legal professional remains unsatisfied with the client's explanation of the red flags, the next step taken will depend on the unique and complex ethical codes, law governing his or her professional conduct and any national AML/CFT obligations.

Combating ML/TF relies on legal professionals:

- being alert to red flags indicating that the client is seeking to involve them in criminal activity
- choosing to abide by the law, their ethical obligations and applicable professional rules; and
- discerning legitimate client wishes from transactions and structures intended to conceal or promote criminal activity or thwart law enforcement.

While some SRBs and professional bodies are quite active in educating their members on the ML/TF vulnerabilities they face and the red flag indicators which could alert them to a suspicious

transaction, this level of understanding or access to information on vulnerabilities was not consistent across all countries which replied to the questionnaire. A lack of awareness and attendant lack of education increases the vulnerability of legal professionals to clients seeking to misuse otherwise legitimate legal services to further ML/TF activities.

Case studies show that not all legal professionals are undertaking client due diligence (CDD) when required. Even where due diligence is obtained, if the legal professional lacks understanding of the ML/TF vulnerabilities and red flag indicators, they are less able to use that information to prevent the misuse of their services. Greater education on vulnerabilities and awareness of red flag indictors at a national level may assist to reduce the incidence of criminals successfully misusing the services of legal professionals for ML/TF purposes.

Finally, the report challenges the perception sometimes held by criminals, and at times supported by claims from legal professionals themselves, that legal professional privilege or professional secrecy would lawfully enable a legal professional to continue to act for a client who was engaging in criminal activity and/or prevent law enforcement from accessing information to enable the client to be prosecuted. However, it is apparent that there is significant diversity between countries in the scope of legal professional privilege or professional secrecy. Practically, this diversity and differing interpretations by legal professionals and law enforcement has at times provided a disincentive for law enforcement to take action against legal professionals suspected of being complicit in or wilfully blind to ML/TF activity.

CHAPTER 1

INTRODUCTION

BACKGROUND

As financial institutions have put anti-money laundering (AML) measures into place, the risk of detection has become greater for those seeking to use the global banking system to launder criminal proceeds. Increasingly, law enforcement see money launderers seeking the advice or services of specialised professionals to help them with their illicit financial operations.[1]

In 2004, Stephen Schneider[2] published a detailed analysis of legal sector involvement in money laundering cases investigated by the Royal Canadian Mounted Police. This is the only academic study to date which has had access to law enforcement cases and contains a section focussed solely on the legal sector, both in terms of vulnerabilities and laundering methods. His research identified a range of services provided by legal professionals which were attractive to criminals wanting to launder the proceeds of their crime. Some of the services identified include: the purchasing of real estate, the establishment of companies and trusts (whether domestically, in foreign countries or off-shore financial centres), and passing funds through the legal professional's client account.

Financial Action Task Force (FATF) typologies have confirmed that criminals in many countries are making use of mechanisms which involve services frequently provided by legal professionals, for the purpose of laundering money.[3]

A particular challenge for researching money laundering / terrorist financing methods that may involve legal professionals is that many of the services sought by criminals for the purposes of money laundering are services used every day by clients with legitimate means.[4]

There is evidence that some criminals seek to co-opt and knowingly involve legal professionals in their money laundering schemes. Often however the involvement of the legal professional is sought because the services they offer are essential to the specific transaction being undertaken and because legal professionals add respectability to the transaction.[5]

Schneider's study noted that in some cases the legal professional was innocently involved in the act of money laundering. In those cases, there were no overt signs that would alert a legal professional

1 FATF (2004)

2 Schneider, S. (2004)

3 FATF (2006) and FATF (2007)

4 Schneider, S. (2004)

5 Schneider, S. (2004)

that he/she was being used to launder the proceeds of crime. However, Schneider identified other cases where legal professionals continued with a retainer in the face of clear warning signs. He questioned whether it might be the case that legal professionals lacked awareness of the warning signs that they were dealing with a suspicious transaction or were simply wilfully blind to the suspicious circumstances. [6]

Subsequent FATF typologies research mentions the involvement of legal professionals in money laundering/terrorist financing (ML/TF). This research has generally tended to focus more on how the transactions were structured, rather than on the role of the legal professional or his/her awareness of the client's criminal intentions.

Organisations representing legal professionals and some academics have sometimes criticised claims that legal professionals are unwittingly involved in money laundering.[7] They have questioned whether it is even possible to identify key warning signs which might justify imposing anti-money laundering/counter financing of terrorism (AML/CFT) requirements on legal professionals and even whether this might be an effective addition to the fight against money laundering and terrorist financing.[8]

Further, certain sources suggest that legal professionals are required to adhere to strict ethical or professional rules and this fact should therefore be a sufficient deterrent to money laundering or terrorist financing occurring in or through the legal sector. Following this same line of thinking, these sources of existing criminal law may sufficiently deter legal professionals from wilfully engaging in money laundering[9].

Since Schneider's 2004 study, a number of countries have implemented the FATF Recommendations for legal professionals.[10] This extension of AML/CFT requirements to the legal professions has created the need for legal professionals, their supervisory bodies and financial intelligence units (FIUs) to better understand how legal services may be misused by criminals for money laundering and terrorist financing.

This typology study was undertaken to synthesise current knowledge, to systematically assess the vulnerabilities of the legal profession to involvement in money laundering and terrorist financing, and to explore whether red flag indicators can be identified so as to enable legal professionals to distinguish potentially illegal transactions from legitimate ones.

---

6 Schneider, S. (2004), pp. 72

7 Middleton, D.J. and Levi, M. (2004), pp 4

8 Middleton, D.J. and Levi, M. (2004), pp 4

9 For example the CCBE Comments on the Commission Staff Working Document "The application to the legal profession of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering" www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_130207_CCBE_comme1_1194003555.pdf

10 FATF Recommendations 22(d), 23(a) and Interpretative Note to Recommendations 23 and 28 (b).

OBJECTIVES

The key objectives of this report:

1. Identify the different functions and activities within the legal profession on a world-wide basis, the different types of AML/CFT supervision for the legal profession and the key issues raised by stakeholders on why applying an AML/CFT regime to the legal profession has been challenging.

2. Identify examples where legal professionals have been complicit in money laundering, with a view to identifying red flag indicators and why their services were of assistance to criminals.

3. Identify specific types of transactions in which legal professionals may have been unknowingly involved in money laundering, with a view to identifying red flag indicators and why their services are of assistance to criminals.

4. Obtain information on the level of reporting from the legal profession and the types of matters reported, with a view to identifying red flag indicators.

5. Consider how the supervisory structure and legal professional privilege, professional secrecy, and confidentiality influences reporting approaches across the legal profession, along with the role ethical obligations did play or should have played in the case studies obtained.

6. Identify good practice in terms of awareness raising and education of the legal profession, positive interaction between law enforcement and professional bodies, and the role of effective sanctioning by either professional bodies for ethical breaches and law enforcement for criminal conduct.

There is extensive literature and litigation on the question of the appropriateness of the inclusion of legal professionals in the AML/CFT regime in the light of their ethical obligations and a client's fundamental rights.[11] There has also been extensive debate as to whether legal professionals are complying with legal obligations to undertake CDD and make suspicious transaction reports (STRs) when this requirement applies to the profession.[12]

Analysing these issues from a policy perspective is not within the scope of a typology study. This report discusses some of the ethical obligations of legal professionals and considers the remit of legal professional privilege/professional secrecy; however, it does so to describe the context in which legal professionals operate. The report also examines the context in which legal professionals covered by the FATF Recommendations undertake their activities and how those Recommendations have been applied in a range of countries. This in turn, will assist in assessing the ML/TF vulnerabilities facing the legal profession. Likewise, the report looks at suspicious transaction reporting by legal professionals with the aim of identifying areas of potential vulnerability, which legal professionals are themselves recognising.

11 Gallant, M. (2010); Levi, M. (2004); Chervier, E. (2004)

12 European Commission(2006); Deloitte (2011)

METHODOLOGY USED IN THIS STUDY

Led by the Netherlands and the United Kingdom, the project team was made up of experts from: the Asia Pacific Group on Money Laundering (APG), Australia, Austria, Canada, China, Denmark, France, the Group of International Finance Centre Supervisors (GIFCS), Italy, the MONEYVAL Committee of the Council of Europe, Switzerland, the United States and the World Bank. In addition, to government and law enforcement representatives, the project team included members from the private sector having supervisory responsibilities for AML/CFT compliance.

In preparing this report, the project team has used literature and initiatives from the sources listed below (a detailed list of these sources is included in Annex 1). The research relies on literature and studies from 2003 onwards to ensure a focus on more current case examples and determine whether vulnerabilities persisted following the inclusion of legal professionals in the FATF Recommendations.

- Typologies studies previously undertaken by FATF.
- Other studies produced by international organisations such as the World Bank and the Organisation for Economic Co-operation and Development (OECD).
- Research initiatives carried out by academics and consultants either within individual countries or on a regional basis.
- Research initiatives carried out by government authorities.
- Research initiatives undertaken by AML/CFT supervisors, non-government organisations and the private sector.

To supplement information from these sources, the project team also developed two questionnaires: one for FATF members and associate members and one for self-regulatory bodies (SRBs) and professional bodies (a list of countries who responded to the questionnaire is available in Annex 2).

The project team received 76 responses to the questionnaire were received from October 2012 to January 2013 from 38 countries. Responses were from both civil and common law countries and included members of FATF, the Caribbean Financial Action Task Force (CFATF), GIFCS, the Middle East and North Africa Financial Action Task Force (MENAFATF) and Moneyval. SRBs and professional bodies also provided responses.

A workshop on money laundering and terrorist financing in the legal sector was held during the joint FATF/GIABA (Intergovernmental Action Group against Money Laundering in West Africa) experts' meeting on typologies held in Dakar, Senegal, in November 2012. Presentations were made by participating representatives from government departments, FIUs and law enforcement agencies (Netherlands, Canada, Nigeria, the United Kingdom) as well as from AML/CFT supervisors (Spain, Gibraltar and the Netherlands) and from the International Bar Association.

The workshop considered:

- Ethical challenges for the legal profession;

- Good practice in supervision;
- The usefulness of STRs filed by legal professionals; and
- Money laundering case studies demonstrating different types of involvement by legal professionals, in order to identify vulnerabilities and red flag indicators.

Informal workshops were also held in February 2013 with the American Bar Association and the Council of European Bars to consider a number of the case studies identified from the literature review and the FATF questionnaire responses. The purpose of these workshops was to consider case studies from the perspective of the private sector to understand the professional, ethical and legal obligations of the range of legal professions in different countries, as well as identify warning signs of money laundering for either the legal professionals themselves or the SRBs representing them.

The literature review, workshops and questionnaire responses painted a consistent picture of the vulnerabilities of legal professionals, as well as a consistent view of the red flag indicators, which may be of use for legal professionals, supervisors and law enforcement.

These sources also provided an extensive collection of cases demonstrating different types of involvement of legal professionals in money laundering and a few cases involving possible terrorist financing. While the majority of case studies in this report relate to ML activity, similar methodologies are capable of being used for TF activity.

In May 2013, a consultation on the draft report took place in London with representatives from the legal sector, who had previously contributed to the typology project. This consultation aimed to ensure that nuances specific to different legal systems and countries where sufficiently recognised and that the responses provided to the questionnaire by SRBs and professional bodies where accurately reflected in the report.

CHAPTER 2

SCOPE OF THE LEGAL SECTOR

The FATF Recommendations, including in the most recent revision of 2012, apply to legal professionals only when they undertake specified financial transactional activities in the course of business. The Recommendations do not apply where a person provides legal services 'in-house' as an employee of an organisation.[13]

This section examines the context in which legal professionals covered by the FATF Recommendations undertake their activities and how those Recommendations have been applied in a range of countries[14].

TYPES OF LEGAL PROFESSIONALS AND THEIR ROLES

Legal professionals are not a homogenous group, from one country to another or even within an individual country.

There are approximately 2.5 million legal professionals practicing in the countries covered by the questionnaire responses.. The size of the sector within each country ranged from 66 legal professionals to over 1.2 million. Titles given to different legal professionals varied between countries, with the same title not always having the same meaning or area of responsibility from one country to another. While some generalisations can be made depending on whether the country has a common law or civil law tradition, even these will not always hold true in all countries. See Annex 4 for a discussion of the types of activities undertaken by legal professional identified through the questionnaire responses.

The range of activities carried out by legal professions is diverse and varies from one country to another. It is therefore important that competent authorities understand the specific roles undertaken by different legal professionals within their respective country when assessing the vulnerabilities and risks that concern their legal sector.

13 Annex 3 contains the relevant definitions for the range of legal professions considered in this report.

14 Jurisdictions that responded to the questionnaire.

APPLICATION OF AML/CFT OBLIGATIONS

In 2003, FATF issued updated Recommendations, which for the first time specifically included legal professionals.

The FATF Recommendations have explicitly required legal professionals to undertake CDD[15] and to submit STRs since the revision of the Recommendations in 2003. From that time, competent authorities have also been required to ensure that legal professionals are supervised for AML/CFT purposes.

As evidenced by mutual evaluation reports[16], full implementation of these specific Recommendations has not been universal. As a consequence, a major part of the legal profession is not covered.

In order to assess the current vulnerabilities, the project team felt it was important to understand in what situations legal professionals were covered by the AML/CFT obligations within their countries and how these obligations applied to them. The application of the CDD and reporting obligations are discussed below, while the approach to the supervisory obligations is covered in Chapter 3.

From the questionnaire responses, while countries have continued to transpose the requirements almost every year since 2001, the majority of countries did so between 2002 and 2004 and between 2007 and 2008.

CLIENT DUE DILIGENCE

Box 1: **Recommendation 22**

The customer due diligence and record-keeping requirements set out in Recommendations 1, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

(d) Lawyers, notaries, other independent legal professionals and accountants – where they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

15 CDD includes identifying and verifying the identity of the client, beneficial owners where relevant, understanding the nature and purpose of the business relationship (including the source of funds). Records of the CDD material must be maintained.

16 The third round of mutual evaluations was based on the 40+9 Recommendations. The FATF Recommendations were revised in 2012, for the fourth round of mutual evaluations, due to begin after the publication of this report.

The majority of countries that apply CDD obligations to legal professionals have done so through national law. A few countries also have SRB-issued guidance to reinforce the legal requirements or provide specific details of the requirements.

In three of the four responses to the questionnaire, where legal professionals are not currently subject to CDD provisions as set out in the FATF Recommendations[17], a number of professional bodies have applied some CDD requirements to their members.

To ensure compliance with international obligations imposed by the United Nations and the FATF regarding targeted financial sanctions, many countries require legal professionals to have regard to whether a client is on a sanctions list. In the United States this list also includes known terrorists, narcotics traffickers and organised crime figures. While this is a separate requirement, apart from the AML/CFT CDD obligations, it does require legal professionals to have some understanding of the identity of their client.

REPORTING OBLIGATIONS

Box 2: **Recommendation 23**

The requirements set out in Recommendation 18 to 21 apply to all DNFBPs, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transaction when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

Interpretive Note to Recommendation 23

1. Lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.
2. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: a) in the course of ascertaining the legal position of their client, or b) in performing their task of defending or representing the client in, or concerning judicial, administrative, arbitration or mediation proceedings.
3. Countries may allow lawyers, notaries, other independent legal professionals and

17 Australia, Canada (although notaries in British Columbia are covered in law), and the United States. In Turkey the law applying the obligations has been suspended awaiting the outcome of legal action, but no specific due diligence requirements have been applied by the relevant professional body. In Canada, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated regulations provide that lawyers must undertake client identification and due diligence, record-keeping and internal compliance measures when undertaking designated financial transactions. These provisions are in force but are inoperative as a result of a court ruling and related injunctions.

accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU.

4. Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

The reporting obligations in the countries which responded to the questionnaire can be characterised as follows:

- Where the obligation to file an STR is applied to legal professionals the obligation is always contained in law rather than guidance.
- In the majority of countries, the STR is submitted directly to the FIU. In seven[18] of the countries, the STR is filed with the SRB. These are civil law countries in Europe.
- In the two of the four countries where AML/CFT obligations for filing an STR have not been extended to legal professionals[19], there is a requirement to comply with threshold reporting, which applies to cash payments above a certain amount. In such cases, the legal professional reports with the knowledge of the client.
- A few[20] countries combine the requirement to make an STR with threshold reporting.

UNIQUE FEATURES OF THE SECTOR

ETHICAL OBLIGATIONS

Ethical obligations apply to legal professionals and the work they undertake.

During the joint FATF/GIABA experts' meeting in November 2012 the International Bar Association (IBA) presented its *International Principles on Conduct for the Legal Profession*[21] and outlined some of the competing ethical requirements that legal professionals (other than notaries) must consider when complying with AML/CFT requirements.

The IBA principles were adopted in 2011 and are not binding for member bar associations and law societies. Each professional association and legal sector regulator or supervisor has its own ethical or professional rules or code of conduct[22]. Many – but not all -- are able to enforce compliance with those rules and have the power to remove legal professionals from practice.

18 Belgium, Czech Republic, Denmark, France, Germany, Luxembourg, and Portugal.

19 Australia and the United States.

20 Curacao requires all cash transactions over 20 000 to be reported, while in Montenegro all contracts for sale of real property must be filed in addition to STRs being made.

21 International Bar Association (2011)

22 Note – in countries which have a federal system, this can differ from state to state as well.

While differences may apply in individual countries, the relevant principles from the IBA are outlined below to give an indication of the types of professional obligations which apply to legal professionals other than notaries.

Box 3: **The IBA principles on conduct for the legal profession**

1. **Independence**

   A legal professional shall maintain independence and be afforded the protection such independence offers in giving clients unbiased advice and representation. A legal professional shall exercise independent, unbiased professional judgment in advising a client, including as to the likelihood of success of the client's case.

2. **Honesty, integrity and fairness**

   A legal professional shall at all times maintain the highest standards of honesty, integrity and fairness towards the lawyer's clients, the court, colleagues and all those with whom the lawyer comes into contact.

3. **Conflicts of interest**

   A lawyer shall not assume a position in which a client's interest conflict with those of the lawyer, another lawyer in the same firm, or another client, unless otherwise permitted by law, applicable rule of professional conduct, or, if permitted, by client's authorisation.

4. **Confidentiality/professional secrecy**

   A legal professional shall at all times maintain and be afforded protection of confidentiality regarding the affairs of present or former clients, unless otherwise allowed or required by law and/or applicable rules of professional conduct.

   Commentary on the principle: However a legal professional cannot invoke confidentiality/professional secrecy in circumstances where the legal professional acts as an accomplice to a crime.

5. **Clients' interests**

   A legal professional shall treat client interests as paramount, subject always to there being no conflict with the legal professional's duties to the court and the interests of justice, to observe the law, and to maintain ethical standards.

   Commentary on the principle: Legal professionals must not engage in, or assist their client with, conduct that is intended to mislead or adversely affect the interests of justice, or wilfully breach the law.

The role of a notary varies significantly depending on whether the professional is a civil-law notary or public law notary, and accordingly the professional and public obligations of a notary vary from country to country. However, the relevant principles from the International Union of Notaries code of ethics[23] provides an indication of the general principles:

[23] International Union of Notaries (2004)

Box 4: **International Union of Notaries Code of Ethics**

Notaries must carry out their professional duties competently and with adequate preparation, performing their essential functions of advising, interpreting and applying the law, acquiring specific knowledge of notarial matters and conforming to professional standards.

Notaries must always verify the identities of parties and the capacity in which they are acting. They must also give expression to their wishes.

Notaries must comply with their professional duty of confidentiality both in the course of their professional services and thereafter. They are also obliged to ensure that this requirement is similarly satisfied by their employees and agents.

Notaries are not bound by their professional duty of confidentiality purely as a result of their obligation to act in concert with any public authorities with which they become involved because of a specific regulation or an order of a judicial or administrative body, including in particular the authority responsible for monitoring the propriety of commercial transactions.

Notaries must conduct themselves in the course of their professional duties with impartiality and independence, avoiding all personal influence over their activities and any form of discrimination against clients.

When acting in their official capacity notaries must balance the respective interests of the parties concerned and seek a solution with the sole objective of safeguarding both parties.

Notaries must act suitably and constructively in the discharge of their duties; they must inform and advise the parties as to the possible consequences of their instructions, having regard to all aspects of normal legal procedure for which they are responsible; they must select the judicial form most appropriate to their intentions and ensure its legality and relevance; they must provide the parties with any clarification requested or necessary to ensure conformity with decisions taken and awareness of the legal force of the deed.

Many SRBs consider that these codes of conduct and professional rules prevent legal professionals from being knowingly involved in money laundering or terrorist financing. Furthermore, if a member had doubts about a transaction or client, that the member would either stop acting or refuse to act, as he or she could not, according to the code of ethics, engage in criminal activity with the client.

The case studies show that many areas of the legal professional's work are open to exploitation by criminals and may attract misuse for money laundering or terrorist financing, as criminals identify weaknesses in processes, legislation and understanding of red flag indicators.

Under professional obligations, the duties to the court (and in the case of the notaries - to the public), take precedence over duties to the client, with the result that the legal professional must not engage in criminal conduct and must not act in a way which facilitates their client engaging in criminal conduct.

Participants at the Dakar meeting acknowledged that the FATF Recommendations specifically recognise the challenges posed by legal professional privilege and professional secrecy. The

Recommendations seek to ease that conflict for legal professionals by specifying that there is no requirement to submit an STR when privilege or secrecy applies.

Further, where legal professionals fail to act with integrity by becoming involved in money laundering or terrorist financing, then professional disciplinary action can be considered. Depending on the specific involvement of the legal professional, this can be in addition to, or instead of, taking criminal action against the professional.

However, there are a number of other ethical or professional challenges highlighted in responses to questionnaires and in meetings, particularly with regard to the manner in which the AML/CFT regime applied to legal professionals other than notaries:

- Where there was a requirement in national law to obtain due diligence information and provide it to law enforcement or other competent authorities, especially without the requirement for a court order, many legal professionals considered this to impinge upon their ability to act with appropriate independence.
- Where following the filing of an STR, legal professionals were required to continue with a transaction or expected to do so to avoid tipping off, but were unable to discuss the STR with the client, then some legal professionals felt they were being required by law to continue to act in the face of a conflict of interest. Many expressed the view that if an STR was warranted, it was a sign that the trust at the heart of the client/legal professional relationship had been broken and it was no longer appropriate to act on behalf of the client.

As this is a typology project, it is not appropriate for this report to comment on the merits of these views or to recommend a policy response. However, further consideration of these challenges by others at a future date may assist in more effectively addressing the vulnerabilities identified later in this report.

CLIENT FUNDS

Most legal professionals are permitted to hold client funds.

From the questionnaire responses, the professional body holds the client funds in a few civil law countries[24]. The professional body requires an explanation of who the funds are held for and why, and will monitor the accounts for any unusual transactions which would suggest money laundering.

In almost all other countries however, legal professionals are required to hold client funds in a separate account[25] with a recognised financial institution, and use it only in accordance with their client's instructions and in relation to the provision of legal services.

---

24 Belgium, France, the Netherlands , In Austria the legal professional holds the money but must notify the Bar of any payment over EUR 40 000, while all deposits with a notary in Italy must be recorded in a public register.

25 These accounts have various names, including client accounts and trust accounts.

In many countries there is a requirement to provide an annual report to the professional body that could also inspect the accounts. In a few[26] countries, rules prohibit the acceptance of cash over set limits, although these limits varied significantly. Within some countries, cash is an acceptable form of payment for legal professionals' services, but its receipt is subject to threshold reporting requirements.

These obligations are often outlined in law or professional rules and could be enforced by disciplinary sanctions.

Box 5: **Example of professional body holding client funds: CARPA (France)**

The system in France known as CARPA is outlined below[1]:

This system was introduced by an Act of 25 July 1985 and requires that all income be credited to a special account. There is one CARPA for each Bar, one account for each legal professional member of the Bar and one sub-account for each case.

Any withdrawal of money must be authorised by the CARPA. Any receipt of fees cannot be done without a written authorisation by the client. Any movement of capital from one sub-account to another is forbidden unless authorised by the President of the CARPA.

The sums of money only pass in transit through the CARPA and the CARPA immediately controls the suspicious lack of movement on a sub-account. No sub-account is allowed to be overdrawn.

The CARPA is controlled by an internal committee but also by the bankers and an independent accountant: they check the nature of the case handled by the legal professional, the origin of the money and the identity of the beneficiary of a payment.

1. Chervrier, E. (2004) pp. 194-196.

The use of client accounts has been identified previously[27] as a potential vulnerability, as it may enable criminals to either place money within the financial system and / or use the money as part of their layering activity, with fewer questions being asked by financial institutions because of the perceived respectability and legitimacy added by the involvement of the legal professional.

CONFIDENTIALITY, PRIVILEGE AND PROFESSIONAL SECRECY

The right of a client to obtain legal representation and advice, to be candid with his legal adviser and not fear later disclosure of those discussions to his prejudice, is recognised as an aspect of the fundamental right of access to justice laid down in the Universal Declaration of Human Rights.

26 Canada, Italy, the Netherlands and Spain.

27 Schneider (2004); FATF (2004).

As outlined above, the FATF Recommendations recognise this right by excluding information covered by legal professional privilege or professional secrecy from the obligation to file an STR and provides that it is a matter for each country as to what those terms cover.[28]

The terms **confidentiality**, **legal professional privilege** and **professional secrecy** are often used interchangeably to describe the protection provided for this right, but legally each term has a different application, meaning and consequence, depending on the country under consideration.

The area of legal professional privilege and professional secrecy is complex, with subtle differences in application from country to country. The summary below is taken from questionnaire responses and provides a high-level overview.

The concept of **confidentiality** seems to apply to all types of legal professionals and to all information obtained in the course of the legal professional's interaction with clients and potential clients. In most countries, it appears that confidentiality can be waived by the client or overridden by express provisions in law.

Legal **professional privilege** and **professional secrecy** appear to offer a higher level of protection to information than does confidentiality. The remit of legal professional privilege and professional secrecy is often contained in constitutional law or is recognised by common law, and is tied to fundamental rights laid down in treaty or other international obligations.

Often, the protection offered to information subject to legal professional privilege and professional secrecy is also contained in criminal law, either in a statute or a rule of evidence. In many countries, the protection will be given to information received or given either for the purpose of current or contemplated litigation, or for the seeking of advice where the legal professional is exercising their skill and judgement as a legal professional. However, some of the questionnaire responses suggested that the protection applies to all information obtained by or provided to the legal professional

In many countries:

- The client can waive his or her right to legal professional privilege or professional secrecy, but in some countries, the legal professional is obliged to ignore the client's waiver if the professional decides that a waiver is not in the client's best interests.
- Legal professional privilege or professional secrecy will be lost if the legal professional is being used for the purpose of committing a crime or a fraud. However the extent of information needed to invoke the crime/fraud exemption varies from country to country, but is usually higher than the basis on which an STR is required to be filed.
- Legal professional privilege or professional secrecy can be removed by express words contained in a statute but only for limited purposes.

The consequences of a breach of legal professional privilege and professional secrecy also vary from one country to another.

---

28 FATF (2012).

In some countries, such a breach will constitute a criminal offence and the legal professional could be subject to imprisonment. In other countries a breach is sanctioned by disciplinary action and/or the client can sue the legal professional. Therefore, any uncertainty over the extent to which legal professional privilege or professional secrecy is exempt from the STR obligations within a country may expose the legal professional to significant personal liability.

In most countries, if evidence is obtained in breach of legal professional privilege or professional secrecy, that evidence cannot be used in court, and in some cases any other evidence obtained as a result of the inappropriately obtained evidence is also inadmissible. This may cause the prosecution to collapse.

A number of respondents indicated that legal professional privilege and/or professional secrecy did not apply to notaries in their country.

A number of countries also reported there were significant restrictions on their ability to obtain search warrants for a legal professional's office or other orders for the production of papers from a legal professional.

Essentially the remit of confidentiality, legal professional privilege and professional secrecy depends on the legal framework in place in the country under consideration and the specific type of legal professional involved.

There have been four completed legal challenges[29] to the application of AML/CFT obligations to legal professionals in Europe. Each of these cases related to the national implementation of the FATF Recommendations in the specific country and considered the rights of access to justice and to privacy enshrined in the European Convention on Human Rights (ECHR).

In each of those cases, the infringement of the broader rights under consideration by the application of the AML/CFT regime to legal professionals was considered proportionate and appropriate, on the basis that legal professional privilege/ professional secrecy was sufficiently protected. For two of the countries[30], this protection required that STRs be submitted via the SRB rather than directly to the FIU.

Box 6: **Summary of decision in the Michaud case**

In its final decision, given on 6 March 2013, in the case of Michaud v France (request no 12323/11), the European Court of Human Rights unanimously held that there was no violation of Article 8 (right to respect for private life) of the ECHR.

The case concerned the application of the AML/CFT requirements on legal professionals, with respect to the requirement to file STRs. The applicant claimed this obligation contradicted Article 8 of the Convention which protects the confidentiality of the exchanges between a legal professional and his client.

29 Bowman v Fels (2005) EWCA Civ 226; ECJ C-305/05, *Ordre des barreaux francophones et germanophone et al. v. Conseil des Ministres*, 2007; ECHR *André et autres v. France*, 2008 and Michaud v. France ECtHR (Application no. 12323/11).

30 Belgium and France.

The Court underlined the importance of the confidentiality of the exchanges between legal professionals and their clients, as well as the professional secrecy of legal professionals. However the Court considered that the obligation to report suspicious transactions was necessary to achieve the justifiable purpose of the defence of order and the prevention of criminal offences, since it is aimed at fighting against money laundering and associated offences. The Court decided that the implementation of the obligation to report suspicious transactions in France was not a disproportionate infringement on the professional secrecy of legal professionals for two reasons.

Firstly, because they were not required to make a report when they are defending a citizen; and secondly, because French law allows legal professionals to make the report to the president of their bar rather than directly to the authorities.

The questionnaire responses indicate that further litigation on similar issues is currently underway in Monaco and Turkey. In Canada, the Court of Appeal for British Columbia[31] has recently upheld an earlier decision that the application of CDD obligations to legal professionals was constitutionally invalid. The requirement to retain the CDD material was found to constitute an unacceptable infringement of the indepence of legal professionals because of the court's concern that law enforcement might obtain an use this material to investigate clients. The Canadian government is seeking to appeal the decision.

31 Federation of Law Societies of Canada v Canada (Attorney General) 2013 BCCA 147.

CHAPTER 3

VULNERABILITIES

VULNERABILITIES IDENTIFIED IN LITERATURE

The literature reviewed for this typology suggested that criminals would seek out the involvement of legal professionals in their money laundering schemes, sometimes because a legal professional is required to complete certain transactions, but also, to access specialised legal and notarial skills and services which could assist in laundering the proceeds of crime and in the financing of terrorism.

Key ML/TF methods that commonly employ or, in some countries, require the services of a legal professional were identified in the literature as follows:

- use of client accounts
- purchase of real property
- creation of trusts and companies
- management of trusts and companies
- setting up and managing charities

While not all legal professionals are actively involved in providing these legitimate legal services which may be abused by criminals, the use of legal professionals to provide a veneer of respectability to the client's activity, and access to the legal professional's client account, is attractive to criminals.

There is also a perception among criminals that legal professional privilege/professional secrecy will delay, obstruct or prevent investigation or prosecution by authorities if they utilise the services of a legal professional.

In terms of TF, while few case studies specifically mention the involvement of legal professionals, they do mention the use of companies, charities and the sale of property. As such it is clear that similar methods and techniques could be used to facilitate either ML or TF, although the sums in relation to the later may be smaller, and therefore the vulnerability of legal professionals to involvement in TF cannot be dismissed.[32]

[32] FATF (2008)

VULNERABILITIES IDENTIFIED THROUGH STRS AND ASSET RECOVERY

STRs and confiscated assets are two data sets that can provide information for competent authorities to assess the extent of AML/CFT risk and vulnerability within their country. The observations below are taken from responses to the FATF questionnaire.

CONFISCATION OF ASSETS

The types of assets acquired by criminals with the proceeds of their crime are evidence of the laundering methods utilised and highlight areas of potential vulnerability. Real estate accounted for up to 30% of criminal assets confiscated in the last two years, demonstrating this as a clear area of vulnerability.

REPORTS ABOUT LEGAL PROFESSIONALS

Analysis of the STRs information provided in the FATF questionnaire responses reveals that financial institutions and other designated non-financial businesses and professions (DNFBPs) were reporting suspicious transactions involving legal professionals, whether they were complicitly or unknowingly involved in their client's criminality. These STRs mentioning potential involvement of legal professionals in money laundering amounted to between .035% and 3% of all STRs reported[33].

REPORTING BY LEGAL PROFESSIONALS

The table below shows the number of reports as identified via the FATF questionnaire[34].

The wide range of activities undertaken by different types of legal professionals in different countries complicates comparisons. In certain countries, notaries and/or solicitors undertake the majority of transactional activities and advocates, barristers or legal professionals have a predominantly advocacy-based role. In these situations, there are naturally more reports originated by the former group than the latter.

The level of reporting by the legal sector is unlikely to be at the same level as that of the financial institutions. There is a significant difference in the volume of transactions undertaken by legal professionals in comparison to financial institutions. Also, the level of involvement in each transaction, which affects the basis on which a suspicion may arise and be assessed, is significantly different.

A more relevant comparison may be to other DFNBPs, especially those providing professional services. From the figures below, the reports by legal professionals averaged 10% of those of DFNBPs, ranging from less than 1% to 20%. Understanding the proportion of the legal sector to the rest of the DFNBPS in a country makes such a comparison more informative.

---

33 These figures were calculated by comparing the number of STRs identified by the FIU in the questionnaire response as having a legal professional as a subject, with the total number of STRs in that jurisdiction for the relevant year.

34 Not all of the thirty-eight jurisdictions which responded to the questionnaire provided STR figures.

However, given the number of legal professionals in each of the countries responding to the FATF questionnaire and the range of transactions they are involved in, reporting levels of zero or even single figures year after year, raises the question as to the underlying reasons relevant to that country. Chapter 6 of this report considers a number of possible contributing factors to the current reporting levels.

Table 1: **Sampling of Suspicious Transaction Reports Filed in 2010 from those countries responding to the questionnaire**

	Legal professionals			DNFBPs	Total
Country	Advocate/ Barrister/ Lawyer	Notary/Other	Solicitor		
Austria	23			-	2 211
Belgium	0	163		1 179	18 673
Curacao	0	0		69	757
Denmark	4			26	2 315
Finland	7			4 040	21 454
France		881		1 303	19 208
Hong Kong/China	99			157	19 690
Ireland			19	82	13 416
Italy	12	66		223	37 047
Jordan	0			0	208
Liechtenstein [1]	5			113	324
Montenegro	0			-	68
Netherlands [2]	27	356		-	198 877
Norway	7			82	6 660
Portugal	5			-	1 459
St Vincent and Grenadines	0			1	502
Spain	39	345		580	2 991
Sweden	1			321	12 218
Switzerland	13			322	1 146
Trinidad and Tobago	0			25	111
United Kingdom	11	141	4 913	13 729	228 834

Table Notes:

1. Legal professionals in Liechtenstein only report when acting as a financial intermediary, rather than when performing activities set forth in the list contained in FATF Recommendation 22(d).

2. The Netherlands requires reports of unusual transactions rather than suspicious transactions.

Table 2: **Sampling of Suspicious Transaction Reports Filed in 2011 from those countries responding to the questionnaire**

Country	Legal Professionals			DNFBPs	Total
	Advocate/ Barrister/ Lawyer	Notary/Other	Solicitor		
Austria	10			-	2 075
Belgium	1	319		1 382	20 001
Curacao	3	7		887	10 421
Denmark	5			14	3 020
Finland	16			6 247	28 364
France		1 357		1 691	22 856
Hong Kong/China	116			161	20 287
Ireland			32	129	11 168
Italy	12	195		492	48 836
Jordan	0			0	248
Liechtenstein [1]	5			142	289
Montenegro	1			-	50
Netherlands [2]	11	359		-	167 237
Norway	11			68	4 018
Portugal	7			-	1 838
St Vincent and Grenadines	0			1	255
Spain	31	382		537	2850
Sweden	0			321	11 461
Switzerland	31			527	1 615
Trinidad and Tobago	2			90	303
United Kingdom	4	166	4 406	11 800	247 160

Table Notes:

1. Legal professionals in Liechtenstein only report when acting as a financial intermediary, rather than when performing activities set forth in the list contained in FATF Recommendation 22(d).

2. The Netherlands requires reports of unusual transactions rather than suspicious transactions.

Most countries who responded to the survey indicated that they did not separate record STRs relating to TF from those relating to ML. A handful of jurisdictions reported receiving TF specific STRs from DNFBPs and one jurisdiction reported receiving STRs in double figures for 2010 and 2011 from legal professionals which related specifically to TF.

In light of the approach to recording statistics and the similarities of the methodologies for ML and TF, while the STRs do not provide a clear picture of the vulnerabilities of the legal profession to TF, again they certainly do not provide a case for dismissing that vulnerability.

REPORTING ON CLIENTS

Respondents to the FATF questionnaire advised that almost all the STRs submitted by the legal profession are on their own clients. The FATF Recommendations state that STRs should relate to all funds, irrespective of whether they are held by the client or third parties. Only the United Kingdom and Norway identified STRs being made by legal professionals in this broader context.

VULNERABILITIES IDENTIFIED BY LEGAL PROFESSIONALS

Respondents to the FATF questionnaire identified that, among the STRs submitted by legal professionals, the top four areas reported are:

- Purchase and sale of real property,
- Formation, merger, acquisition of companies,
- Formation of trusts and
- Providing company or trust services.

A number of countries' legal professionals also identify probate (administering estates of deceased individuals), tax advice and working for charities as areas giving rise to circumstances requiring them to file an STR.

The top five predicate offences featuring in STRs from legal professionals among the respondent countries were:

- corruption and bribery
- fraud
- tax crimes
- trafficking in narcotic drugs and psychotropic substances
- unclear offences, but unexplained levels of cash or private funding

STRs from legal professionals in a few countries also identified a range of other offences such as terrorism, trafficking in human beings and migrant smuggling, insider trading, and forgery. .

USEFULNESS OF STRS BY LEGAL PROFESSIONALS

It is difficult to assess the direct usefulness of individual STRs, as the collection of feedback in many countries is sporadic. However, from the level of case studies and questionnaire responses, it appears that STRs submitted by legal professionals are often of high quality and lead to further action.

For example, Switzerland reported that 93.5% of STRs from legal professionals were passed to law enforcement, with 62% resulting in proceedings being instituted. In addition, Belgium, Italy, Liechtenstein, Ireland and the United Kingdom commented positively on the general quality of the STRs provided by legal professionals. While the United Kingdom and the Netherlands noted that STRs from legal professionals contributed to both law enforcement activity and prosecutions, as well as assisting in identifying and locating the proceeds of crime for confiscation activity.

A number of case studies contained in Chapter 4 and Annex 6 of this report demonstrate successful prosecutions, where a legal professional has filed an STR.

SUPERVISION OF LEGAL PROFESSIONALS

Box 7: **Recommendation 28**

Countries should ensure that other categories of DNFBPS are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by a) a supervisor or b) by an appropriate SRB, provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a 'fit and proper' test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML.CFT requirements.

APPROACH TO SUPERVISION

Supervisors generally have the opportunity to monitor the conduct of all of their members, irrespective of whether there has been a complaint of potentially criminal conduct or professional misconduct. Therefore, they are a potential source of information on vulnerabilities of a sector, even where the existence or exploitation of the vulnerability has not yet come to the attention of law enforcement agencies. An absence of supervision may aggravate pre-existing vulnerabilities.

The questionnaire responses show a number of different supervisory frameworks which have been implemented for legal professionals:

- Twenty-three countries have allocated supervisory responsibility to SRBs. In many cases there is interaction with either the FIU or a relevant government ministry on the overall approach to supervision.
- Five countries have allocated supervisory responsibility to the FIU. In all cases, the professional bodies are involved in providing advice on compliance to their members.
- Three countries have allocated supervisory responsibility to other external supervisors. In each of those cases the professional bodies liaised with the external supervisor on compliance and education.
- In two countries it was unclear from responses who had supervisory responsibility, and another two countries were in the process of establishing supervisors for the legal profession.

- In three of the four countries that responded to the questionnaire where AML/CFT obligations have not been extended to legal professionals[35], the FIU, relevant government departments and/or professional bodies provide some advice on ML/TF risks. They either have a role in monitoring compliance with professional rules or in monitoring compliance with threshold reporting obligations.

The SRBs generally indicated that they had the ability to refuse membership admission to those persons who either did not meet a fit and proper test or who had relevant criminal convictions.

The SRBs also indicated they had the power to monitor compliance and take disciplinary action, although some mentioned they had very limited resources with which to undertake this role.

A few of the external supervisors/FIUs mentioned that due to constitutional requirements regarding access to the offices of legal professionals, they either undertook their supervisory functions with the consent of the legal professionals or they had delegated the onsite inspections to the professional body.

EDUCATION AND RAISING AWARENESS

Almost all countries that responded to the questionnaire provide education, advice and guidance to legal professionals on AML/CFT compliance, and a number provided links to a large range of detailed educational material.

However, debate is ongoing within some countries about the type of red flag indicators that legal professionals should be educated about:

- Twenty-two countries either did not answer the question or said that there were no specific risks or red flag indicators for legal professionals;
- Two countries have only recently applied the AML/CFT obligations to legal professionals and are in the processes of developing red flag indicator relevant to their country;
- Of the remaining respondents in some cases both the FIU and the SRB or professional body were able to articulate risks to the legal sector and red flag indicators relevant to the activities of legal professionals. In other cases it was only the FIU or the SRB which provided that information.

In one country, the two SRBs who responded, had actively co-operated with the FIU in compiling a very detailed list of red flag indicators for legal professionals, although in their responses they stated that they were not aware of specific risks to their members.

Only one SRB said that the lack of information about warning signs and lack of disciplinary action suggested to them that the potential for misuse of their members was high. On the other hand a number of SRBs who did not provide information on red flag indicators thought that the fact that they did not need to take disciplinary action against their members was an indication that the

35 Australia, Canada and the United States – although the Canadian FIU is the AML/CFT supervisor for the Notaries in British Columbia.

ML/TF risks to their members must be low or that their members were able to deal with the risks adequately.

The questionnaire specifically asked about the interaction between SRBs and professional bodies, and FIUs. Five of the private sector respondents mentioned that they did not have any interaction with the FIU in their country, and four of those were SRBs. A further three SRBs did not respond to the questions about interaction with the FIU. Generally these respondents indicated that they would have welcomed dialogue with the FIU and thought that this would assist them in helping to improve compliance by their members.

DISCIPLINARY AND CRIMINAL SANCTIONS IMPOSED ON LEGAL PROFESSIONALS

Disciplinary and criminal action taken against legal professionals helps to identify areas of vulnerability and provides case studies of both witting and unwitting involvement. The FATF questionnaire specifically looked at disciplinary and criminal action within the preceding five years.

SRBs from ten countries provided advice about disciplinary action taken, however the number of disciplinary cases reported exceeded double figures only in the Netherlands, the United Kingdom and the United States.

Criminal prosecutions were started in sixteen countries, with Austria, Spain, Italy, and Poland joining the Netherlands, the United Kingdom and the United States reaching double figures of prosecutions in the last five years.

For both disciplinary and criminal actions only a small number were substantiated to the relevant standard of proof and resulted in sanctions. The United Kingdom and the United States provided the most examples of successful disciplinary and criminal prosecutions.

The individual case studies provided have been included in both Chapter 4 and Annex 6 of this report and the red flag indicators and other lessons to be learnt from those cases are considered in more detail in those sections. Some also contain details on sanctions imposed, which range from fines to removal from practice to imprisonment.

The case studies clearly demonstrate that criminals still seeking to exploit the vulnerabilities that caused the FATF to call for extending AML/CFT obligations to legal professionals. However, the case studies also show that, at least in some instances, it is now the legal professional who becomes aware of the attempted misuse of their services and submits an STR that then prompts an investigation.

TAKING ENFORCEMENT ACTION AGAINST LEGAL PROFESSIONALS

Within the literature and other typology research, law enforcement often cites “challenges” in successfully prosecuting legal professionals for money laundering as a basis for legal professionals posing a greater risk of ML/TF.

While the actual ML/TF offences are the same for legal professionals as they are for ordinary citizens, a number of potential hurdles to prosecuting legal professionals have been identified.

EVIDENCE GATHERING

Most of the practical issues concerning the investigation of ML/TF by or through legal professionals relate to legal professional privilege or professional secrecy and the process of gathering evidence. FATF Recommendation 31 is relevant as it stipulates that the powers of law enforcement agencies and investigative authorities should include evidence-gathering methods and compulsory measures for the production of records held by DNFBPs. Whether any evidence gathered or created in the course of an investigation is subject to legal professional privilege or professional secrecy is a legal issue that cannot be predicted with certainty. Some of the practical challenges identified in investigating ML/TF by or through legal professionals include: uncertainty about the scope of privilege, the difficult and time-consuming processes for seizing legal professional's documents, and the lack of access to client account information.

DIFFERENCES IN SCOPE OF PRIVILEGE

As outlined in Chapter 2 of this report, legal professional privilege and professional secrecy are considered fundamental human rights and the legal professional is obliged to take steps to protect that privilege. However, the remit of confidentiality, legal professional privilege and professional secrecy varies from one country to another, and the practical basis on which this protection can be overridden is not always clear or easily understood. In some countries, the FIU may have greater powers to access underlying information on which an STR is based, while in other countries it is also possible for law enforcement to have access to such material.

In some countries financial and banking records may be accessed just as easily for legal professionals as for any other individual, while tax information may be accessed easily by some law enforcement agencies. But in other countries this kind of information is also subject to privilege. In some countries, both law enforcement agencies and the private sector have said that they find the lack of clarity on the extent of the reporting duty under the AML/CFT legislation challenging.

DOCUMENTS

Regulatory officials, police, and prosecutors must be careful to respect solicitor-client privilege during the course of their work. This can result in an increase in time and resources required to build a case against a legal professional when compared to other persons or professionals. A number of the questionnaire responses highlighted this point, especially in relation to the seizure of documents from a legal professional's office – whether provided by the client or created by the legal professional.

Claims of legal professional privilege or professional secrecy could impede and delay the criminal investigation. Once a claim of privilege is made over a document obtained pursuant to a search warrant, for example, the document is essentially removed from consideration in the investigation until the claim for legal professional privilege is resolved.

This delay may still occur were the claim is made correctly and in accordance with the law, or if made with the genuine but mistaken belief by the legal professional that privilege or secrecy applies. This may be particularly relevant if there is misunderstanding of the extent of privilege or secrecy in particular circumstances by either the legal professional or law enforcement, or if there is a dispute

as to whether any of the grounds for removing the privilege or secrecy (such as the crime fraud exemption) apply. However, some of the case studies do evidence extremely wide claims of privilege or secrecy being occasionally made which exceed the generally understood provisions of the protections within the relevant country, an experience which was reflected in some of the responses to the questionnaire.

Law enforcement agencies are required by law to have strong evidence from the outset to demonstrate that privilege or secrecy should be removed. In many instances this means that the claim of legal professional privilege or professional secrecy will need to be resolved by a court, which can delay the investigation process for a substantial period of time. As time is a critical factor in pursuing the proceeds of crime, this may influence the decision of investigators of whether to investigate the possible involvement of the legal professional or to seek evidence of their client's activities from alternative sources. .

CLIENT ACCOUNTS

Several countries stated that tax authorities, police and prosecutors do not have the right to investigate transactions that touch legal professionals' client accounts, as these are covered by confidentiality requirements. Sight of such accounts can of course be given voluntarily by those under investigation, but this is a practical solution only where the investigating agency is willing to reveal the fact that they are conducting the investigation.

OTHER CHALLENGES

The use of certain investigative techniques such as intercepting the telephone or electronic communications may be virtually forbidden when those communications involve legal professionals. In some countries, prior consent to the recording by a party to the communication or the subsequent removal of sections of the recorded conversations covered by legal professional privilege or professional secrecy may permit some limited use of this technique.

Some countries noted the special position of the legal professional within a legal community as presenting a challenge in being permitted to investigate legal professionals. Legal professionals and judges will often be well-known to each other and the question has been raised of whether a court is obliged to find a judge who is not known by a defendant or suspect legal professional, and who is therefore demonstrably impartial.

PROSECUTING LEGAL PROFESSIONALS

Legal professionals have professional training, and even if they do not "know" the AML laws, they will generally be sufficiently aware to avoid crossing the line between questionable behaviour and criminality, making it more difficult to prove the relevant mental element in a money laundering prosecution. More importantly, if they do cross that line knowingly and willingly, legal professionals, especially in law firms, have access to employees who can establish companies or accounts (thus, further insulating the legal professional). Legal professionals who cross the line may also have access to other professionals (in both the legal and financial sectors) who can help them layer and conceal the proceeds of crime involved in money laundering transactions. Lastly, being a member of

the bar, affords a certain standing and prestige in society. This may cause others with whom the legal professional interacts, to favour or trust him/her, merely due to his/her status, when they would otherwise look suspiciously upon certain behaviour.

Responses to the questionnaire showed that in some cases, legal professionals were not charged with the criminal offence of money laundering although it was clear to the investigating officers that they were involved in the ML/TF activity. Two main reasons were provided as to why this may be the case:

- Firstly, because of the inability to secure sufficient evidence to prove their complicit involvement in the money laundering schemes. Domestically, access to evidence may have been refused because claims to legal professional privilege or professional secrecy were upheld; or investigators decided not to pursue that evidence because of the more complicated processes involved in seeking access to such evidence and demonstrating that it is appropriate to be released. In the case of an international investigation, the evidence-gathering process can be hindered by the fact that privilege and secrecy varies across the countries that are trying to co-operate.
- Secondly, because they are likely to make useful co-operators, informants, and/or cooperating witnesses. A legal professional has every incentive to co-operate with law enforcement once his/her illegal activity is discovered to avoid reputational harm, loss of license (livelihood), and censure by the bar.

CHAPTER 4

MONEY LAUNDERING TYPOLOGIES

This section of the report looks at case studies which illustrate the ML/TF methods and techniques which involve the services of a legal professional.

FATF recognises that the vast majority of legal professionals seek to comply with the law and their ethical obligations, and will not deliberately seek to assist clients with money laundering or terrorist financing. This report has identified case studies where legal professionals have stopped acting for clients and/or made an STR; although comprehensive information about the extent to which this occurs is not available, especially in the absence of a reporting obligation being imposed at a country level. [36]

However, as identified in Chapter 3, there are a range of legal services which are of interest to criminals because they assist in laundering money and may assist in terrorist financing.

The criminal may seek out the use of a legal professional, because they need expert advice to devise complicated schemes to launder vast amounts of money, and they will either corrupt the legal professional or find one who is already willing to wilfully assist them.

However in many other cases, the criminal will use the legal professional because:

- either by virtue of a legal requirement or custom, a legal professional is used to undertake the otherwise legitimate transaction, which in that instance involves the proceeds of crime;
- the involvement of a legal professional provides an impression of respectability sought in order to dissuade questioning or suspicion from professionals and/or financial institutions; or
- the involvement of a legal professional provides a further step in the chain to frustrate investigation by law enforcement.

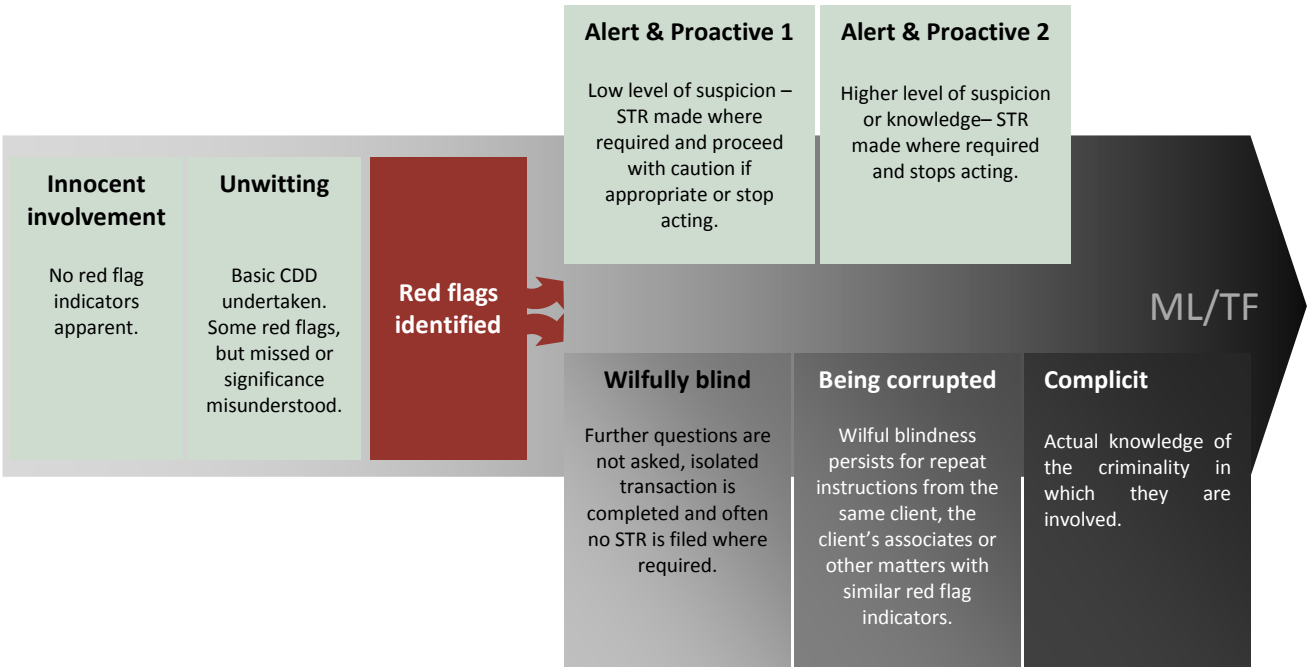
At the outset of this typology exercise, the objective was to identify examples of complicit involvement by legal professionals on the one hand and unknowing involvement on the other. A more detailed review of the case studies has indicated that such a stark distinction is not really appropriate.

The involvement of a legal professional in money laundering may more appropriately be described as a continuum:

[36] It should be noted that legal professionals may cease to act but not make an STR when legal professional privilege or professional secrecy applies.

- Depending on the extent to which the proceeds of crime have already been laundered previously, there may realistically be no red flag indicators apparent to the legal professional during the transaction or the client is able to provide convincing explanations to any generic red flag indicators identified.
- In other cases, red flag indicators may be present, but due to lack of awareness or proper systems, the legal professional genuinely does not see the red flag indicators or appreciate their significance.
- Where the red flag indicators are present and identified by the legal profession, two separate approaches may be taken.
    - In some cases the legal professional, for a variety of reasons may turn a blind eye to the red flag indicators, become more deeply involved in the criminal activity and may in a minority of cases become a future willing accomplice for one or more criminals. Law enforcement has reported that in some cases they may still receive an STR from such a legal professional after the police investigation has commenced.
    - Alternatively, the legal professional may make a STR (where required) and depending on the level of information they have causing the suspicion and their professional obligations in the given circumstances, either proceed with the transaction with caution, or cease acting for the client.

Figure 1. **Involvement of Legal Professionals in money laundering and terrorist financing (ML/TF)**



APPROACH TO CASE STUDIES IN THIS REPORT

For each method and technique identified, this report considers the attractiveness of the method for criminals and a relevant ethical or professional obligation of the legal professional.

Case studies are identified which demonstrate each technique and where possible, case studies have been sourced from both civil and common law countries and show different types of involvement from the legal professionals.

Under each case study, attention is drawn to the red flag indicators which *may* have been apparent to the legal professional and/or to the SRB or law enforcement investigating the transaction. These red flag indicators are drawn from a comprehensive list contained in Chapter 5.

Red flag indicators should always be considered in the context of the specific case. Individual red flag indicators may not be a basis on their own for having a suspicion of money laundering, but they will be a basis to ask questions of a client.[37] The answers to these questions may remove concerns about the source of funds being used in the transaction. Alternatively, the answers or lack of answers may cause a legal professional to be suspicious that his/her services are being misused, especially where there is more than one red flag indicator present.

A table of all case studies, with key methods and techniques is in Annex 5, as individual cases may demonstrate more than one method.

Additional case studies are contained in Annex 6.

[37] This is consistent with the FATF requirements to identify the client, the beneficial owners, understand the source of funds and the nature and the purpose of the business relationship.

METHOD 1: MISUSE OF CLIENT ACCOUNT

While the use of the client account is part of many legitimate transactions undertaken by legal professionals, it may be attractive to criminals as it can:

- be used as part of the first step in converting the cash proceeds of crime into other less suspicious assets;
- permit access to the financial system when the criminal may be otherwise suspicious or undesirable to a financial institution as a customer;
- serve to help hide ownership of criminally derived funds or other assets; and
- be used as an essential link between different money laundering techniques, such as purchasing real estate, setting up shell companies and transferring the proceeds of crime.[38]

[38] Australia, Canada and the United States – although the Canadian FIU is the AML/CFT supervisor for the Notaries in British Columbia.

TECHNIQUE: TRANSFERRING FUNDS WITHOUT PROVIDING LEGAL SERVICES

The majority of legal professionals are required to meet strict obligations when handling client money, including the requirement that they deal with client money only in connection with the provision of legal services and do not simply act as a bank or deposit-taking institution. Failure to comply with these obligations will generally be grounds for disciplinary action.

However, law enforcement and SRBs are still finding cases where legal professionals are simply transferring funds through their client account without providing an underlying legal service. In some cases this could raise questions as to whether a law firm had appropriate procedures or was supervising staff members or junior lawyers appropriately. In discussion with SRBs during the workshops, it was suggested that if legal services are not provided, there may not be a lawyer-client relationship and privilege or secrecy may not apply.

Case 1: **Use of client account without underlying legal services provided – common law country**

An employee working in a very small law firm in Australia received an email from a web-based account referring to a previous telephone conversation confirming that the law firm would act on the person's behalf.

The 'client' asked the employee to accept a deposit of AUD 260 000 for the purchase of machinery in London. The 'client' requested details of the firm's account, provided the surname of two customers of a bank in London, and confirmed the costs could be deducted from the deposit amount.

The details were provided, the funds arrived and the 'client' asked that the money be transferred as soon as possible to the London bank account (details provided) after costs and transfer fees were deducted. The funds were transferred, but no actual legal work was undertaken in relation to the purchase of the machinery. The transfer of the funds to the law firm was an unauthorised withdrawal from a third party's account.

This specific case was brought to the attention of the Office of the Legal Services Commissioner (OLSC) in Australia, which took the view that the law firm had failed to ensure that the identity and contact details of the individual were adequately established. This was particularly important given the individual was not a previous client of the law firm. The employee – proceeding on the basis of instructions received solely via email and telephone without this further verification of identity – was criticised. The OLSC also found that the law firm failed to take reasonable steps to establish the purpose of the transaction and failed to enquire into the basis for the use of the client account. The law firm was reprimanded for their conduct in this case.

Source: Australia (2012) questionnaire response.

Case 1 **Red flag indicators:**	• The client is actively avoiding personal contact without good reason. • Client is willing to pay fees without the requirement for legal work to be undertaken. • Client asks for unexplained speed.

Case 2: **Deliberate misuse of client account without underlying legal transaction – hybrid civil and common law country**

A Quebec lawyer received approximately USD 3 million in American currency from a Montreal businessman, which he deposited into the bank account of his law practice.

The lawyer then had the bank transfer the funds to accounts in Switzerland, the United States, and Panama.

In Switzerland, another lawyer, who was used as part of the laundering process, transferred on one occasion USD 1 760 000 to an account in Panama on the same day he received it from the Canadian lawyer.

When depositing the funds in Canada, the Quebec lawyer completed the large transaction reports as required by the bank, fraudulently indicating that that the funds came from the sale of real estate.

A police investigation into the Quebec lawyer established that these funds were transferred to a reputed Colombian drug trafficker linked to the Cali Cartel. In their attempts to gather further information about the suspicious transactions, bank officials contacted the lawyer about the funds. The lawyer refused to provide any further information, claiming solicitor-client confidentiality.

The bank subsequently informed the lawyer that it could no longer accept his business.

Source: Schneider, S. (2004)

Case 2 **Red flag indicators:**	• Use of a disproportionate amount of cash • Use of client account with no underlying legal work • Funds sent to one or more countries with high levels of secrecy • Client known to have connections with criminals

Case 3: **Disciplinary action taken for use of client account without underlying transaction – common law country**

The Kentucky Supreme Court ordered Attorney Charley Green Dixon be publicly reprimanded for misconduct relating to Dixon's attorney escrow account. Although the trial commissioner of the state bar disciplinary committee found Dixon not guilty on charges of violating two ethics rules, the court elected to review the case despite the fact that no appeal was filed by the committee.

The court found Dixon in violation of: an ethics rule relating to the safekeeping of client property; for his failure to notify corporations that he received funds in which corporations had an interest; and for distributing those funds to a third party. At the time of the misconduct, Dixon was the elected Knox County Attorney. Dixon represented his family friend, a Knox County judge, on and off for 15 years, and the judge asked him to cash cheques, leaving them on Dixon's desk each time and following up with phone calls.

In total, Dixon deposited 11 cheques payable to one of two construction companies into his attorney escrow account and subsequently wrote cheques in corresponding amounts to the judge's brother or sister-in-law. The court noted: "*An FBI investigation uncovered a money laundering scheme perpetrated by [Judge] Raymond Smith and [his brother] Matt Smith. Raymond Smith used his position as Knox County Judge–Executive to create false bids and invoices for county construction projects. He laundered the money through various accounts, including Dixon's attorney escrow account. Raymond*

and Matt Smith pled guilty to federal charges. Evidence before the trial commissioner included an affidavit from the FBI agent on the case, stating that Dixon was not charged with a crime because prosecution of Dixon required Raymond Smith's assistance, which was unlikely."

Despite the absence of a current attorney-client relationship between Dixon and the judge, the Court found that the relevant ethics rule prohibited an attorney from engaging in any conduct involving dishonesty, fraud, deceit, or misrepresentation, even outside of an attorney-client relationship. The Court ordered Dixon to be publicly reprimanded for his violation of the spirit of the ethics rules, the "global appearance of impropriety by Dixon," and his conduct which was deemed serious enough to "bring the Bar into disrepute." The Court held that even though he was not prosecuted for a money laundering offence, Dixon should have known better than to use his "escrow account for 'banking services' for individuals."

Source: United States (2012) questionnaire response Kentucky Bar Ass'n v. Dixon, 373 S.W.3d 444 (Ky. 2012)

Case 3 **Red flag indicators:**	• Use of client account without an underlying legal transaction. • Requests for payments to third parties without substantiating reason or corresponding transaction.

TECHNIQUE: STRUCTURING PAYMENTS

For countries where there are threshold reporting obligations, criminals may seek the advice and assistance of a legal practitioner to structure the payments to avoid those reporting obligations. Such involvement by a legal practitioner would be complicit. Even where threshold reporting is not required, criminals may still seek to structure payments in such a way as to avoid raising the suspicion of the financial institution.

Some of the case studies below show that advice on structuring may also include putting transactions in the names of third parties and getting involved in other financial transactions.

Under professional requirements, a legal professional would need to establish clearly who their client was, ensure they were acting in that person's best interest and that the person providing instructions had clear authority to do so. The failure to establish those factors would at least suggest a breach of professional obligations which warrant disciplinary action. It may also show that the legal professional knew or suspected that he or she was assisting with inappropriate conduct and so deliberately chose not to ask more questions.

Where the legal professional is involved in providing advice on share purchases and handling the funds to facilitate the purchase or is involved in other sorts financial transactions, consideration would need to be given as to whether the legal professional was acting as a financial advisor and/or investment broker rather than as a legal professional. Depending on the country, such conduct may be outside the scope of the legal professional's role and may require separate licensing. This may also mean that privilege/secrecy would not cover that transaction.

Case 4: **Legal professional deliberately structures transactions to avoid reporting threshold in property case – common law country**

An investigation into an individual revealed that an Australian solicitor acting on his behalf was heavily involved in money laundering through property and other transactions. The solicitor

organised conveyancing for the purchase of residential property and carried out structured transactions in an attempt to avoid detection. The solicitor established trust accounts for the individual under investigation and ensured that structured payments were used to purchase properties and pay off mortgages. Some properties were ostensibly purchased for the individual relatives, though the solicitor had no dealings with them. The solicitor also advised the individual on shares he should buy and received structured payments into his trust account for payment

Source: FATF (2007)

Case 4 **Red flag indicators:**	• Purchase of properties for family members where there is a lack of personal contact without good reason gives raises doubts as to the real nature of the transaction. • Third party funding warranting further consideration. • Significant private funding and the transfers are structured so as to avoid the threshold reporting requirements.

Case 5: **Legal professional convicted following structuring and purported stock purchases – common law country**

Criminal defence attorney Jerry Jarrett was convicted for money laundering and illegally structuring financial transactions to avoid reporting requirements. In one instance, Jarrett laundered USD 67 000 in drug proceeds by depositing money through small transactions into the bank account of a dormant business he controlled. He then prepared a backdated stock purchase agreement representing that the drug dealer had invested USD 15 000 in the company. He then wrote a series of cheques to the client for "return on investment." Jarrett organised a series of similar transactions with another drug dealer to launder USD 25 000 in drug proceeds. Both clients testified at trial that Jarrett knew that the cash was drug proceeds. See 447 F.3d 520 (7th Cir. 2006) (reversing district court's post-verdict dismissal of indictment).

Source: United States (2012) questionnaire response United States v. Jarrett, No. 03-cr-87 (N.D. Ind.)

Case 5 **Red flag indicators:**	• Significant private funding and the transfers are structured so as to avoid the threshold reporting requirements. • Client was known to have convictions for acquisitive crime.[1] • Unusual level of investment in a dormant company.

1. Acquisitive crime is any crime which produces proceeds of crime.

Case 6: **Legal professional files STR after noticing structuring and back to back sales by client – civil law country**

Person A purchases two real estate properties in 2007, for a combined price of EUR 150 000. The same properties are sold again in 2010 for a combined price of EUR 413 600 to Person B. The notary asked to see details of the payments between the vendor and the purchaser, before notarising the sale. They were provided with evidence that the funds had been deposited over the previous two months with all of the deposits under the reporting threshold amount of EUR 100 000. There was public information that Person B was associated with frauds in the automobile sector. The notary filed a STR.

Source: Spain (2012) questionnaire response

Case 6 **Red flag indicators:**	• The transaction was unusual in that the price increase was significant by comparison to the normal market changes over the same period. • One of the parties is known to be currently under investigation for acquisitive crime or to have known connections with criminals.

In this case, direct payment between the parties was not a red flag indicator, as this is quite common in Spain.

TECHNIQUE: ABORTED TRANSACTIONS

Some criminals will be aware of the restrictions on the ability of legal professionals to handle client funds without an underlying transaction. Therefore, they will appear to be conducting a legitimate transaction which, for one reason or another, collapses before completion. The client then asks for the money to be returned or paid to multiple recipients, sometimes according to the direction of a third party. [39]

During an economic downturn, the aborting of transactions is not an infrequent occurrence and legal practitioners may find it more difficult to distinguish between legitimate situations and those which were always intended to launder the proceeds of crime.

Third party funding is not unusual in aborted transactions. Under professional obligations, a legal professional must act in the best interests of the client. This means that they need to know who the client is and to understand if the funds they were using were being given to them as a gift or a loan, so that the arrangement and any subsequent ownership interests were properly documented. The failure to do so may suggest a breach of professional requirements or possibly complicity in the scheme.

Case 7: **Legal professional disciplined for sending funds to a third party after an aborted transaction – common law country**

In 2010 a solicitor was fined GBP 3 000 for their involvement in a purported company acquisition which was in fact an investment fraud. In 2005, the solicitor had accepted unsolicited funds directly from investors, but then the purchase of the company did not occur. A third party to the transaction asked for the funds to be paid into an account in Eastern Europe. The solicitor made an STR and received permission to send the funds back to the original source. For reasons which are unclear, the funds were instead transferred to another account controlled by a third party, allowing the proceeds of the fraud to be laundered. The Solicitors Disciplinary Tribunal found that the solicitor was naive rather than reckless.

Source: United Kingdom (2012) questionnaire response

Case 7 **Red flag indicators:**	• The person actually directing the operation is not one of the formal parties to the transaction or their representative • Transaction is aborted after receipt of funds and there is a request to send the funds on to a third party.

[39] This technique was specifically noted in the Australian questionnaire response to this project.

Case 8: **Legal professional removed from practice after ignoring red flag indicators on an aborted transaction – common law country**

In 2011 a solicitor was struck off the roll for acting in a number of property purchases which had all the hallmarks of money laundering. In 2008 the solicitor received instructions from an individual to purchase property on behalf of other clients, who provided funds for the purchase prior to the solicitor indicating the need for the funds to be deposited. The solicitor did not meet the clients, undertake due diligence checks or obtain instructions in writing. The funds came into the client account, the transaction was cancelled and there was a request to provide the funds to a third party – all on the same day.

Source: United Kingdom (2012) questionnaire response

Case 8 **Red flag indicators:**	• Transaction is aborted after receipt of funds and there is a request to send the funds to a third party • The client is acting through an intermediary and avoiding personal contact without good reason • Unusual speed requested.

METHOD 2: PROPERTY PURCHASES

Criminals, like those with legitimate incomes, require a place to live and premises from which to conduct their business activities. Irrespective of economic conditions, real estate investment often remains attractive for criminals and non-criminals alike. Consequently, the purchase of real estate is a common outlet for criminal proceeds. Real estate is generally an appreciating asset and the subsequent sale of the asset can provide a legitimate reason for the appearance of the funds

In many countries a legal professional is either required by law to undertake the transfer of property or their involvement is a matter of custom and practice.

However the specific role of the legal professional in real estate transactions varies significantly from country to country, or even within countries. In some countries, the legal professional will customarily hold and transfer the relevant funds for the purchase. In other countries this will be done by other parties, such as a title insurance agent.

Even if the legal professional is not handling the money, they will be aware of the financial details and in many cases will be in a position to ask further questions about the purchase or sale.

Therefore, real estate transactions are a key area of potential ML/TF vulnerability for legal professionals.

TECHNIQUE: INVESTMENT OF PROCEEDS OF CRIME IN PROPERTY

From the cases obtained, it is clear that some criminals will seek to invest the proceeds of their crime in real estate without attempting to obscure their ownership.

Despite many countries introducing reporting requirements on cash payments, and many professional bodies restricting the amount of cash which legal professionals may receive, some criminals will still seek to use the purchase of real property as a means of placing cash obtained from criminal activity. Increasingly, this is seen as part of the layering process, where the funds have been accumulated in one or more bank accounts and the property purchase is wholly or predominantly funded through private means rather than a mortgage or loan.

There has been extensive publicity about the money laundering risks posed by large amounts of cash or unexplained levels of private funding in relation to property purchases. Where legal professionals are involved and an STR is not made, it is more likely that the legal professional is either complicit in the money laundering, or is being wilfully blind by failing to ask more questions when warning signs are present.

Case 9: **Legal professional files STR after noticing red flag indicators on property transaction – civil law country**

The CTIF-CFI (the Belgium FIU) received a notification from a notary on a person from Eastern Europe, who resided in Belgium and had bought a property there.

The purchase happened by depositing the total purchase price in cash before the document authenticating the purchase was signed. The person claimed that he could not open a bank account

and so had to pay cash for the property.

After the notification of the notary, the FIU learned that the person did have an account at a Belgian bank and that the size of the transaction was not in proportion with his financial situation as he was receiving state benefits. Police sources revealed the person was known for illicit trafficking in goods and merchandise

Source: Cellule de traitement des informations Financières, (2005)

Case 9 **Red flag indicators:**	• Transaction involves a disproportionate amount of private funding/cash, which is inconsistent with the socio-economic profile of the individual • Transaction is unusual because of the manner of execution – in this case it was the depositing of the total purchase price so early in the transaction which was different to normal custom.

Case 10: **Legal professional acts as prosecution witness after failing to notice warning signs relating to a property purchase – common law country**

In 2009 a client approached a United Kingdom solicitor to purchase land for the client's family.

The client deposited GBP 35 000 with the solicitor which they said was from family members as the family were pooling the money together to buy land on which all the family could live.

Further cash amounts were deposited with the solicitor from numerous third parties to fund the rest of the purchase.

The solicitor only spoke with the client, who said they were the only literate member of the family and so was conducting business on the family's behalf.

While the solicitor did not submit an STR, the solicitor was not prosecuted but acted as a witness for the police.

Source: United Kingdom (2012) questionnaire response

Case 10 **Red flag indicators:**	• Significant levels of private funding/cash which is inconsistent with the socio-economic profile of the individual • Funding from third parties requiring further consideration • Request to act for multiple parties without meeting them

Case 11: **Legal professional convicted of money laundering through property purchase involving cash and significant funding from multiple parties – common law country**

Shadab Kahn, a solicitor, assisted in the purchase of a number of properties for a client using the proceeds of crime. The client owned a luxury car business, but was also involved in drug dealing.

The funds for the property purchases were generally provided in cash from the client or from third parties. Almost GBP 600 000 was provided by the client, which was a significant level of private funding despite the client's apparent legitimate business activities.

Mr Khan was convicted in 2009 of money laundering and failing to make an STR, jailed for four years, and struck off the roll by the Solicitors Disciplinary Tribunal in 2011. The court criticised Mr Khan for accepting explanations about the source of funds at face value and not looking behind the claimed cultural customs about the funding arrangements.

Source: United Kingdom (2012) questionnaire response

Case 11 **Red flag indicators:**	• Significant amount of private funding/cash from an individual who was running a cash intensive business. • Involvement of third parties funding without apparent connection or legitimate explanation.

TECHNIQUE: TRANSFERRING VALUE – BACK TO BACK OR ABC SALES

The frequent movement of investments in immovable assets such as property is not common. Quick successive sales of property, either with or without a mortgage, enable criminals to inflate the value of the property, thereby justifying the injection of further criminal funds into the purchase chain and enabling value to be either transferred to other parts of an organised crime group or reinvested within the group. While the frequent changes in ownership may also make it more difficult for law enforcement to follow the funds and link the assets back to the predicate offence.

Case 12: **Legal professional facilitates multiple back to back sales of properties within a group of mortgage fraudsters – civil law country**

An individual in his early 20's who worked as a gardener approached a notary to purchase several real estate properties. The client advised that he was funding the purchases from previous sales of other properties and provided a bank cheque to pay the purchase price.

The client then instructed a different set of notaries to re-sell the properties at a higher price very quickly after the first purchase. The properties were sold to other people that the client knew who were also in their early 20's and had similar low paying jobs.

The client had in fact obtained mortgages using false documents for these properties, generating the proceeds of crime. The multiple sales helped to launder those funds.

Source: France (2012) questionnaire response

Case 12 **Red flag indicators:**	• Disproportionate amount of private funding which is inconsistent with the socio-economic profile of the individual • Transactions are unusual because they are inconsistent with the age and profile of the parties • Multiple appearances of the same parties in transactions over a short period of time. • Back to back (or ABC) property transaction, with rapidly increasing value • Client changes legal advisor a number of times in a short space of time without legitimate reason. • Client provides false documentation.

TECHNIQUE: TRANSFERRING VALUE – SALES WITHIN AN ORGANISED CRIME GROUP

Case 13: **Legal professional facilitates multiple back to back property sales within an organised crime group – civil law country**

The attention of Tracfin was drawn to atypical financial flows relating to real estate purchases undertaken in the regions of Midi-Pyrénées, Languedoc-Roussillon and Provence-Alpes-Côte d'Azur.

The analysis brought to light a possible network of organised criminality involving people who were either current or former members of the Foreign Legion. The individuals were mostly of the same foreign nationality and involved a real estate civil society (property investment scheme).

Between April 2009 and March 2011 the office of a notary public registered 28 deeds of real estate transfer for this group. All the sales, bar one, were officialised by the same notary in the office.

Twelve individuals and six different real estate civil societies (non-trading companies) were listed as the purchaser, while seven individuals and five societies were sellers of the properties.

Of these 28 deeds, 16 were paid in full for EUR 1.925 million; six were financed through loans of EUR 841 149 in total, and the source of financing was not able to be determined for five properties which had a value of EUR 308 200.

Nine of the transactions were paid in full by individuals in the amount of EUR 1.152 million, which was a significant amount given the profession of the clients.

The properties were also resold within relatively short timeframes. For example, one of the properties in Castres was resold every year since 2009 with occasionally significant increases in the sale price. All these sales were registered by the same notary. The real estate civil society thereby multiplied by six the purchase price of this property.

In some instances the sellers claimed the property had increased in value because they had done work on those properties (they hadn't).

The notary registered two further transactions in 2011 which were paid for in cash and were at a significant distance from the notary's office.

Source: France (2012) questionnaire response

Case 13 **Red flag indicators:**	• Disproportionate amount of private funding/cash which is inconsistent with the socio-economic profile of the individual. • Significant increases in value / sale price sometimes realised within a relatively short timescale. • Parties to the transaction are connected without an apparent business reason. • Multiple appearances of the same parties in transactions over a short period of time.

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE WITH A FALSE NAME

Criminals who seek to retain the benefit of the proceeds of their crime may seek to obscure the ownership of real property by using false identities. Legal professionals may be complicit in these transactions, but are more likely to be involved unwittingly, especially if the criminal has forged identity documentation of a high quality or if the legal professional is not required in their country to undertake CDD.

The use of false or counterfeited documents should always be a red flag to the legitimacy of the individual and the action they wish to take. While legal professionals are not expected to be forgery experts, with the increased ability of criminals to access such materials through the internet, having some familiarity with identity documents at least within their country, may help them avoid being taken in by obvious forgeries.

Case 14: **Legal Professional facilitates property purchase in a false name – common law country**

Law enforcement investigated a matter involving a drug offender actively growing a large crop of cannabis on a property. When the person of interest (POI) was arrested for this offence, it was established that the person had purchased the block of land under a false name.

Under provisions of Chapter 3 of the Criminal Proceeds Confiscation Act 2002, if the POI had effective control of the land, and used that land to produce dangerous drugs, then the property was liable for forfeiture. Initial inquiries revealed the property was registered as being owned by a different person. Further enquiries made with another government department revealed the person had the same first names as the POI, but a different surname. The date of birth recorded at this department was very similar to the POI with the year and month identical, but the day slightly different.

It was alleged the POI had purchased the property under a false name, as no identification was required by the real estate agent to sign the contract. It is further suspected the POI took the contract to a solicitor for conveyance and had the solicitor sign the transfer documents on the POI's behalf. The sale was executed in 2002, but the final payment (made via a solicitor) was not made until 2004. This payment method was written into the contract.

Source: Australia (2012) questionnaire response

Case 14 **Red flag indicators:**	• Client provides false or counterfeited documentation • There are attempts to disguise the real owner or parties to the transaction • Transaction is unusual because of the manner of execution in terms of the delay in payment well after the contact was executed.

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE THROUGH INTERMEDIARIES

The creation of convincing false identities involves time and expenditure by criminals and there is a risk that the fake identity will be discovered. Another option for obscuring ownership while retaining control is placing the property in the names of family, friends or business associates.

While the purchase of real property for family members may be quite legitimate and a regular occurrence in many cultures, such transactions will usually require detailed documentation to ensure that ownership, inheritance and taxation matters are properly dealt with.

Legal professionals also need to carefully consider who they are acting for, especially where there are a number of parties involved in a purchase. They will need to ensure that they are not in a conflict situation and that they are able to act in the best interests of their client. Failure to ask such questions may be indicative that the legal professional is either complicit or wilfully blind to the money laundering risks.

Case 15: **Family members used as a front for purchasing property – common law country**

A Canadian career criminal, with a record including drug trafficking, fraud, auto theft, and telecommunications theft, deposited cash into a bank account in his parents' name.

The accused purchased a home with the assistance of a lawyer, the title of which was registered to his parents. He financed the home through a mortgage, also registered to his parents. The CAD 320 000 mortgage was paid off in less than six months.

Source: Schneider (2004)

Case 15 **Red flag indicators:**	• Disproportionate amount of private funding/cash which is inconsistent with the known legitimate income of the individual • Client is known to have convictions for acquisitive crime • There are attempts to disguise the real owner or parties to the transaction. • Mortgages repaid significantly prior to the initial agreed maturity date with no logical explanation.

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE THROUGH A COMPANY OR TRUST

The purchasing of real estate through a company or a trust has been identified previously[40] as a technique used to both obscure ownership and frustrate law enforcement activity to pursue the proceeds of crime.

Case 16: **PEP involved in financial wrongdoing purchases expensive properties in foreign country through a corporate vehicle – civil law country**

A foreign client approached a legal professional to buy two properties, one in Alpes-Maritimes (South of France), and the other in Paris, for EUR 11 million.

The purchase price was completely funded by the purchaser (there was no mortgage) and the funds were sent through a bank in an off-shore jurisdiction.

As the contract was about to be signed, there was a change in instructions, and a property investment company was replaced as the purchaser. The two minor children of the client were the shareholders of the company.

The foreign client held an important political function in his country and there was publicly available information about his involvement in financial wrongdoing.

Source: France (2012) questionnaire response

Case 16 **Red flag indicators:**	• The legal professional was located at a distance from the client / transaction, and there was no legitimate or economic reason for using this legal professional over one who was located closer. [1] • Disproportionate amount of private funding which is inconsistent with the socio-economic profile of the individual • Client is using bank accounts from a high risk country

40 FATF (2007) and Schneider (2004).

	• Unexplained changes in instructions, especially last minute • The transaction is unusual in the manner of its execution – in France it is quite unusual for residential property to be purchased via a corporate vehicle or for minors to be shareholders. It should be noted that this approach would be considered normal and prudent estate planning in other countries. • Use of a complicated structure without legitimate reason • Shareholders of the executing party are under legal age • Client holds a public position and is engaged in unusual private business given the characteristics involved.

1. In some jurisdictions it is becoming more frequent for legal services relating to property purchases to be sourced online which may mean that the legal professional is located at a distance from the client or the transaction. However in many civil law countries, where notaries are required to be involved with the purchase, notaries are appointed to a specific location. While non-face to face transactions are no longer listed as automatically requiring enhanced due diligence under the FATF Recommendations, the desire to avoid personal contact without good reason is still an indicator of money laundering or terrorist financing risk

Case 17: **Legal professionals assist with opening bank accounts and investing in property via complex corporate structures – civil law country**

A foreigner residing in Belgium was introduced to a bank by a law firm with a view to him opening an account. This account was credited with large sums by foreign transfers ordered by an unknown counterpart. A civil-law notary wrote bank order cheques from the account, which was then invested in real estate projects in Belgium. In one of these projects the person under suspicion was assisted by other foreign investors in setting up a particularly complex scheme.

The FIU learned from questioning the civil law notary, that he had been engaged by four foreign companies to help set up two holding companies. These two companies had in their turn set up two other Belgian real estate companies. The latter two had then invested in real estate.

The people representing these companies – a lawyer and diamond merchant – acted as intermediaries for the person under suspicion. It turned out the lawyer who had introduced this person to the bank was also involved in other schemes of a similar nature. The address of the registered office of the Belgian companies was also the address of his lawyer's office.

This information showed the important role played by the lawyer in setting up a financial and corporate structure designed to enable funds from unknown foreign principals to be invested in real estate projects in Belgium. On the basis of all these elements the FIU decided to report the file for laundering of the proceeds of organised crime.

Source: Belgium (2012) questionnaire response

Case 17 **Red flag indicators:**	• Creation of complicated ownership structures where there is no legitimate or economic reason. • Client is using an agent or intermediary without good reason. • Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason. • The source of funds is unusual as there is third party funding with no apparent connection or legitimate explanation and the funds are received from a foreign country where there is no apparent connection between the country and the client.

Case 18: **Legal professional files STR when companies are used to purchase properties to facilitate laundering of drug proceeds and/or terrorist financing – civil law country**

A Spanish married couple of Moroccan origins, who own three properties, incorporate a limited company. They own 100% of the shares between them, the value of which is EUR 12 000 euro.

Within the first five months, the company has undertaken investments of over EUR 260 000, without apparent recourse to external financing. This includes purchasing five properties for over EUR 193 000 in cash. One of the property purchases is from an Islamic community in the south of Spain, the vice-president of which was arrested in 2009 within the context of a Civil Guard anti-drugs trafficking operation.

The couple are found to be associated with other companies which do not file accounts as required under law or receive official gazette notifications. The notary involved in some of the property purchases makes an STR.

According to subsequent information obtained by the Spanish Executive Service of the Commission for Monitoring Exchange Control Offences (SEPBLAC), the transactions could be connected with people possibly related to drug trafficking or terrorist financing.

Source: Spain (2012) questionnaire response

Case 18 **Red flag indicators:**	• The size of the client company was inconsistent with the volume or value of the investments made by the company • The professional profiles of a company's shareholders make it unlikely that the company possessed a lawful source of funds for the scope of investments made • The sum paid out in cash for the properties acquired by the company seems unusual and the company had no corresponding business or operations to justify such a cash outlay • Morocco is geographically located on a route used to introduce drugs into Europe, and this, in connection with the considerable sums of cash being moved from the country to Spain, suggests that the territory should receive particular attention. • One of the persons associated with the operation had been arrested within the context of an anti-drugs trafficking operation.

TECHNIQUE: MORTGAGE FRAUD WITH ANTECEDENT LAUNDERING

While this is a typology on money laundering and terrorist financing – not a report on the involvement of legal professionals in predicate offences – it is relevant to highlight a few cases involving mortgage fraud.

Many of the red flag indicators which would demonstrate money laundering are also present in mortgage frauds, and depending on the specific elements of the money laundering offence, possession of the mortgage funds in the legal professional's client account and subsequent transfer will amount to money laundering.

Case 19: **Legal professional disciplined for failing to notice warning signs of mortgage fraud and handling the proceeds of crime – common law country**

In 2008 a law firm employee was approached by three individuals who were accompanied by a friend to seek a quote to purchase three separate properties. They returned later that day with passports and utility bills and instructed the law firm to act for them in the purchases.

The clients asked for the purchases to be processed quickly and did not want the normal searches undertaken. They did not provide any money to the solicitors for expenses (such funds would normally be provided) but said the seller's solicitors would be covering all fees and expenses. The clients said they had paid the deposit directly to the seller. The mortgages were paid to the law firm, which retained their fees and then sent the funds to a bank account which the law firm employee thought belonged to solicitors acting for the sellers. No due diligence was undertaken.

In fact the actual owners of the property were not selling the properties and had no knowledge of the transaction or the mortgages taken out over their properties. The mortgage funds were paid away to the fraudsters, not to another solicitors firm.

In 2010, the supervising solicitor was fined GBP 10 000 for not properly supervising the employee who allowed the fraud to take place and the proceeds of the funds to be laundered. The solicitor's advanced age was taken into account as a mitigating factor in deciding the penalty.

Source: United Kingdom (2012) questionnaire response

Case 19 **Red flag indicators:**	• Transaction was unusual in terms of all three purchasers attending together with an intermediary to undertake separate transactions; failure to provide any funds for expense in accordance with normal processes; and part of the funds being sent directly between the parties. • Client showed an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory client identification. • Clients asked for short-cuts and unexplained speed in completing a transaction.

Case 20: **Legal professional removed from practice after facilitating multiple mortgage frauds for a number of property developers – common law country**

In 2006 a solicitor was approached by three developers wanting him to act in a number of property transactions. The developers were selling the properties to various companies and investment networks, who were then quickly selling the properties on at significantly inflated prices to other individuals. The solicitor was acting for these individuals, and was introduced to the clients by the other parties to the transaction with the 'deal' already completed.

In 2011 the solicitor was struck off the roll by the Solicitors Disciplinary Tribunal because they had failed to provide full information to the lender (enabling mortgage fraud), had not checked the source of funds for the original transactions or deposits (enabling money laundering) and had not taken notes of their instructions at the time of the transactions, fabricating them during the investigation.

Source: United Kingdom (2012) questionnaire response

Case 20 **Red flag indicators:**	• Back to back (or ABC) property transaction with rapidly increasing purchase price • Transaction is unusual in that there is limited legal work to be undertaken by the legal professional • Unnecessary complexity in the structures and parties involved in the transaction.

METHOD 3: CREATION OF COMPANIES AND TRUSTS

Criminals will often seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and trusts are seen by criminals as potentially useful vehicles to achieve this outcome.

TECHNIQUE: CREATION OF TRUSTS TO OBSCURE OWNERSHIP AND RETAIN CONTROL

Disguising the real owners and parties to the transaction is a necessary requirement for money laundering to be successful and therefore, although there may be legitimate reasons for obscuring ownership it should be considered as a red flag.

Case 21: **Trust established to receive proceeds of tax crime and invest in criminal property**

Two trusts were established in an offshore centre by a law firm. The law firm requested the trustee to accept two payment orders in favour of a bank in order to buy real estate. It appeared that the trust had been used to conceal the identity of the beneficial owners.

Information obtained by the Belgian FIU revealed that the beneficiaries of the trusts were individuals A and B, who were managers of two companies, established in Belgium that were the subject of a judicial investigation regarding serious tax fraud. Part of the funds in these trusts could have originated from criminal activity of the companies.

Source: FATF (2010)

Case 21 **Red flag indicators:**	• Use of an intermediary without good reason. • Attempts to disguise the real owner or parties to the transaction. • Involvement of structures in multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason. • Client is known to be currently under investigation for acquisitive crimes.

Case 22: **Trust established to enable a criminal to act as a trustee and retain control of property obtained with criminal proceeds – common law country**

A criminal involved in smuggling into the United Kingdom set up a Trust in order to launder the proceeds of his crime, with the assistance of a collusive Independent Financial Adviser (IFA) and a Solicitor, who also appeared to be acting in the knowledge that the individual was a criminal. The Trust was discretionary and therefore power over the management of the fund was vested in the Trustees, namely the criminal, his wife and the IFA.

The criminal purchased a garage, which he transferred directly to his daughter (who also happened to be a beneficiary of the Trust). She in turn leased the garage to a company. The garage was eventually sold to this company, with the purchase funded by a loan provided by the Trust. The company subsequently made repayments of several thousand pounds a month, ostensibly to the Trust, but in practice to the criminal.

Thus the criminal who had originally owned the garage probably maintained control despite his

daughter's ownership. Through controlling the Trust he was able to funnel funds back to himself through loaning funds from the Trust and receive payments on that loan.

Source: FATF (2010)

Case 22 **Red flag indicators:**	• Creation of a complicated ownership structure when there is no legitimate or economic reason. • The ties between the parties of a family nature generate doubt as to the real nature or reason for the transaction. • Client is known to be currently under investigation for acquisitive crimes.

TECHNIQUE: CREATION OF SHELL COMPANIES TO PLACE OR LAYER

In some countries, a legal professional (usually a notary) must be involved in the creation of a company, so there is an increased risk of unintentional involvement in this laundering method. However, in a number of countries, members of the public are able to register a company themselves directly with the company register. In those countries, if a client simply wants a legal professional to undertake the mechanical aspects of setting up the company, without seeking legal advice on the appropriateness of the company structure and related matters, it may be an indication that the client is seeking to add respectability to the creation of a shell company.

A shell company is a business or corporate entity that does not have any business activities or recognisable assets itself. Shell companies may be used of legitimate purposes such as serving as a transaction vehicle (*e.g.*, an acquiring company sets up a shell company subsidiary that is then merged with a target company, thus making the target company the subsidiary of the acquiring company) or protecting the corporate name from being used by a third party because the incorporation of the shell company under that name blocks any other company from being incorporated with the same name. But criminals often seek to set up shell companies to help obscure beneficial ownership.

Shell companies should be distinguished from shelf companies that are often set up by legal professionals for the purpose of facilitating legitimate transactions. Such companies will be used when it becomes apparent during a transaction that there is a need for a corporate vehicle to be used and there is a legitimate need for speed in the transaction. They will usually be created with the legal professional or their employees as the directors and/or shareholders and are held "on the shelf" until they are needed in the course of a transaction. The legal firm will only have a few of these companies at any one time; in many cases they will only be in existence for a short amount of time and they are sold to the clients in full, with the legal professionals having no further involvement in the management of the company after it is taken down off the shelf. Criminals may seek to misuse shelf companies by seeking access to companies which have been 'sitting on the shelf' for a long time in an attempt to create the impression that the company is reputable and trading well because it has been in existence for many years.

In terms of professional obligations, if a client fails to provide adequate information about the purpose for which the company was set up, this may give rise to concerns as to whether the legal professional would be able to adequately provide advice in the best interests of the client. The

failure to ask such questions may be an indicator that the legal professional is complicit in the scheme.

Case 23: **Legal professional approached over internet to set up multiple companies without information on identity, source of funds or purpose – hybrid common law / civil law country**

A legal professional was approached over the internet to set up companies with limited or no details about the future uses of the company.

Over three years they were asked to set up at least 1 000 such companies in this way.

The people they were asked to list as directors included individuals known to be involved with high level organised crime in that country.

They never met the clients and did not undertake any due diligence.

The companies were used to facilitate money laundering from loan sharking.

Source: Japan (2012) questionnaire response

Case 23 **Red flag indicators:**	• Client is actively avoiding personal contact without good reason. • Transactions are unusual in terms of volume. • Client is overly secretive about the purpose of the transaction. • Parties involved in the transaction have known connections with criminals.

Case 24: **Legal professional sets up multiple international company structures for existing clients – civil law country**

A legal professional in Spain was asked to set up a series of companies for clients for the purpose of purchasing real estate.

Some companies were incorporated in Spain but they were owned by companies which the legal professional also incorporated in an American State.

The legal professional and others in the law firm would constitute the board of directors of the companies incorporated in America. They would later sell these companies to their clients.

The legal professional set up over 300 such companies for clients of the law firm, and continued to administer those companies for the clients.

Many of the clients were known to be involved in international criminal organisations.

Source: FATF (2010)

Case 24 **Red flag indicators:**	• Involvement of structures with multiple countries where there is no apparent link to the client or transaction or no other legitimate or economic reason. • Involvement of high risk countries. • Client is known to have convictions for acquisitive crime, to be currently under investigation for acquisitive crime or have known connections with criminals.

TECHNIQUE: USE OF BEARER SHARES TO OBSCURE OWNERSHIP

Bearer shares are an equity security that is wholly-owned by whoever holds the physical stock certificate. The issuing firm neither registers the owner of the stock, nor does it track transfers of ownership.

Quite a number of countries have banned the use of bearer shares by legal entities, while in other countries; these types of securities are quite common, even for companies acting legally.

Case 25: **Creation of company with bearer shares to obscure ownership in a property transaction – civil law country**

A Spanish lawyer created several companies for a client on the same day (with ownership through bearer shares, thus hiding the identity of the true owners). One of these companies acquired a property that was an area of undeveloped land. A few weeks later, the area was re-classified by the local authorities where it was located so it could be urbanised.

The lawyer came to the Property Registry and in successive operations, transferred the ownership of the property by means of the transfer of mortgage loans constituted in entities located in offshore jurisdictions. With each succeeding transfer of the property the price of the land was increased.

The participants in the individual transfers were shell companies controlled by the lawyer. Finally the mortgage was cancelled with a cheque issued by a correspondent account. The cheque was received by a company different from the one that appeared as the acquirer on the deed (cheque endorsement). Since the company used a correspondent account exclusively, it can be inferred that this company was a front set up merely for the purpose of carrying out the property transactions.

After investigation it was learned that the purchaser and seller were the same person: the leader of a criminal organisation. Money used in the transaction was of illegal origin (drug trafficking). Additionally, in the process of reclassification, administrative anomalies and bribes were detected.

Source: FATF (2007)

Case 25 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime, or have known connections with criminals. • Back to back (or ABC) property transactions, with rapidly increasing value / purchase price. • Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.

Case 26: **Creation of complex company structures in multiple countries to launder proceeds of drug trafficking**

A legal professional in Country A was approached to assist in setting up companies for a client.

The legal professional approached a management company in Country B, who in turn approached a trust and company service provider in Country C to incorporate a number of bearer share companies.

Only the details of the trust and company service provider were included in the incorporation

documents as nominee directors and administrators.

The articles of incorporation and the bearer shares were forwarded to the lawyer, via the management company, who provided them to the client.

The client was involved in drug importation. Approximately USD 1.73 million was restrained in combined assets from residential property and bank accounts in relation to those companies

Source: FATF 2010

Case 26 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason. • Disproportionate private funding which is inconsistent with the socio-economic profile of the individual.

METHOD 4: MANAGEMENT OF COMPANIES AND TRUSTS

While the creation of companies and trusts is a key area of vulnerability for legal professionals, criminals will also often seek to have legal professionals involved in the management of those companies and trusts in order to provide greater respectability and legitimacy to the entity and its activities.

In some countries professional rules preclude a legal professional from acting as a trustee or as a company director. In countries where this is permitted, there are differing rules as to whether that legal professional can also provide external legal advice or otherwise act for the company or trust. This will affect whether any funds relating to activities by the company or trust can go through the client account.

TECHNIQUE: ACTING AS TRUSTEE – RECEIVING THE PROCEEDS OF CRIME

Where a settlor creates a trust using the proceeds of crime or deposits further assets into the trust which are the proceeds of crime, a legal professional acting as trustee will be facilitating the laundering of those proceeds by managing the trust. Under common law there is an obligation on the trustee to acquaint themselves with all trust property and the FATF standards require that those providing trust services in a business capacity undertake CDD, including ascertaining the source of funds. Such enquiries would assist in minimising the risks of legal professionals who are acting as trustees inadvertently becoming involved in money laundering.

Case 27: **Legal professional uses client account to transfer proceeds of crime into a trust he managed – common law country**

Defendant Paul Monea was convicted of various money laundering counts in connection with his attempt to accept payment for the sale of a large diamond by requiring the purchasers to wire funds, which he knew to be drug proceeds, to his attorney's IOLTA (attorney trust) account and onward to his family trust account, which was managed by the same attorney. It does not appear as if the attorney was prosecuted. *See* 376 F. App'x 531 (6th Cir. 2010), *cert. denied* 131 S. Ct. 356 (2010).

Monea's Family Trust was in possession of a 43-carat flawless yellow diamond that Monea was looking to sell for a profit. Monea was introduced to an undercover federal agent who used the name "Rizzo," and Rizzo volunteered that he knew someone (a drug dealer) who would be interested in purchasing the diamond. Monea explained that he did not want to conduct the sale in cash because of apprehension that he was being "watched" by the government. The court noted that the pair discussed at a meeting: "the best way to conduct the transaction, the problem of receiving cash, Monea's conversations with his attorney about his responsibilities concerning knowledge of the money's source, and whether Monea could use the [Attorney Trust Account] of the attorney representing the Monea Family Trust." On meeting with another undercover agent posing as the buyer's representative, Monea told the man (who he believed to be the associate of the drug dealer-purchaser) that USD19.5 million should be wired into his Attorney's Trust Account. Funds were wired in the amount of USD 100 000 in three instalments when the deal was supposed to close at the attorney's office with a gemmologist present to certify the authenticity of the stone. Rizzo pretended to make a call to have the remainder of the purchase price wired into the Attorney Trust

Account, but instead, he called other law enforcement agents and the scheme was disrupted.

The court held that Monea's "intent to conceal" the nature of the drug dealer's proceeds used to buy the diamond was shown by his desire to use the Attorney Trust Account to funnel the funds to the Monea Family Trust account, which the attorney also managed. Routing the transaction through the Attorney Trust Account was an extra and unnecessary step, not integral to the sale, which should have raised red flags with the attorney.

Furthermore, according to recorded conversations, Monea discussed with the attorney that he did not want the wire transfers "looked at." The attorney allegedly stated that he represented his Attorney Trust Account and Monea's trust, so there was no problem as long as the diamond was sold for fair market value. Monea paraphrased the attorney speaking to him, in a recorded conversation: "you [Monea] don't really have the responsibility or obligation to interview people to find out how they got the money [for the diamond] . . . it's not your responsibility." Monea later stated: "I'll tell you why I want [the money] going into my [Attorney's Trust Account]. Because my attorney represents the [Monea Family Trust]. And my attorney can legitimately represent the [Monea Family Trust] . . . and we're conducting the sale on behalf of the trust. And it keeps me clean." Monea used his attorney and his trust account as intermediaries, and then further used his trust account that was managed by the attorney to conceal drug proceeds and insulate himself by virtue of the attorney-client relationship. *See* 376 F. App'x 531 (6th Cir. 2010), *cert. denied* 131 S. Ct. 356 (2010).

Source: United States (2012) questionnaire response United States v. Monea, No. 07-cr-30 (N.D. Ohio)

Case 27 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • The retainer involves using the client account were this is not required for the provision of legal services

TECHNIQUE: MANAGEMENT OF A COMPANY OR TRUST –APPEARANCE OF LEGITIMACY AND PROVISION OF LEGAL SERVICES

Case 28: **Legal practitioner incorporates companies and acts as front man to launder proceeds of embezzlement**

A money laundering operation involved a massive purchase of derivatives by companies which paid hefty fees to fake intermediaries, then surreptitiously transferred to the bank directors either in cash or on foreign banks accounts.

In this scheme the notary participated by incorporating some of the fake intermediaries, whilst the lawyer appeared as the beneficial owner of such companies and actively participated in a complex scheme of bank transactions put in place to embezzle the funds illicitly obtained. Several bank accounts at different institutions were used, with the involvement of figureheads and shell companies, so as to transfer funds from one account to another by mainly making use of cheques and cash.

Source: Italy (2012) questionnaire response

Case 28 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Creation of complicated ownership structures when there is no legitimate or economic reason.

Case 29: **Legal professional manages trusts used to perpetrate an advanced fraud scheme and launder the proceeds – common law country**

An entity, Euro-American Money Fund Trust, was used to perpetrate an advance-fee scheme. John Voigt created a genealogy for the Trust, claiming it was a long-standing European trust associated with the Catholic Church. He then solicited investments for phony loans. Ralph Anderskow was a partner at a large Chicago firm who managed the Trust and whose credentials were publicised as legitimising the Trust. Although he may not have known that the Trust was fraudulent at first, it was apparent shortly thereafter. Anderskow provided guarantees to borrowers, maintained a client escrow account into which advance fees were deposited, and distributed the deposited fees to Voigt and his associates, which violated the terms of the contracts entered into with the loan applicants and investors. *See* 88 F.3d 245 (3d Cir. 1996) (affirming conviction and 78-month sentence).

Source: United States (2012) questionnaire response United States v. Anderskow, No. 3:93-cr-300 (D.N.J.)

Case 29 **Red flag indicators:**	• Client is using false or fraudulent identity documents for the business entity • Requests to make payments to third parties contrary to contractual obligations

TECHNIQUE: HOLDING SHARES AS AN UNDISCLOSED NOMINEE

Individuals may sometimes have legal professionals or others hold their shares as a nominee, where there is legitimate privacy, safety or commercial concerns. Criminals may also use nominee shareholders to further obscure their ownership of assets. In some countries legal professionals are not permitted to hold shares in entities for whom they provide advice, while in other countries legal

professionals regularly act as nominees. Where a legal professional is asked to act as a nominee, they should understand the reason for this request.

Case 30: **Legal professionals acting as undisclosed nominees in companies suspected as vehicles for organised crime – civil law country**

A lawyer was reported by an Italian banking institution in connection with some banking transactions performed on behalf of companies operating in the wind power sector in which he held a stake. The reporting entities suspected the stake was in fact held on behalf of some clients of his rather than for himself.

The report concerned a company owned by the lawyer who sold his minority stake (acquired two years earlier for a much lower price) to another company authorised to build a wind farm. The majority stake belonged to a firm owned by another lawyer specialising in the renewable energy sector and involved in several law enforcement investigations concerning the infiltration of organised criminal organisations in the sector.

The whole company was purchased by a major corporation operating in the energy sector. Financial flows showed that the parent firm of the company being sold received €59million from the corporation. Although most of the funds were either used in instalments to repay lines of financing previously obtained both from Italian and foreign lenders or transferred to other companies belonging to the same financial group, some funds were credited to the account held in the name of the law firm of which the reported lawyer was a partner. Transfers to other legal professional were also observed.

Source: Italy (2012) questionnaire response

Case 30 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Client is known to have connections with criminals • There is an excessively high price attached to the securities transferred, with regards to circumstances indicating such an excess or with regard to the sum declared in another operation.

METHOD 5: MANAGING CLIENT AFFAIRS AND MAKING INTRODUCTIONS

Because of their ethical and professional obligations, the involvement of legal professionals in a transaction or their referral of a client to other professionals or businesses often provides the activities of the criminal with a veneer of legitimacy.

TECHNIQUE: OPENING BANK ACCOUNTS ON BEHALF OF CLIENTS

Financial institutions who are complying with their AML/CFT obligations may choose not to provide bank accounts to certain individuals who pose a high risk of money laundering or terrorist financing. In the questionnaire responses and literature reviewed, there were cases where legal professionals have either encouraged financial institutions to open accounts (despite being aware of the money laundering risks) or have opened accounts specifically for the use of clients, in such a way as to avoid disclosing to the financial institution the true beneficial owner of the account.

The lack of alleged access to a bank account may be a red flag indicator that the individual is subject to sanctions or a court freezing or restraint order.

Case 31: **Legal professional assisting client to obtain banking services despite warning signs of money laundering by a politically exposed person – common law country**

From 2000 to 2008, Jennifer Douglas, a U.S. citizen and the fourth wife of Atiku Abubakar, former Vice President and former candidate for President of Nigeria, helped her husband bring over USD 40 million in suspect funds into the United States through wire transfers sent by offshore corporations to U.S. bank accounts. In a 2008 civil complaint, the U.S. Securities and Exchange Commission alleged that Ms. Douglas received over USD 2 million in bribe payments in 2001 and 2002 from Siemens AG, a major German corporation.

While Ms. Douglas denies wrongdoing, Siemens has already pled guilty to U.S. criminal charges and settled civil charges related to bribery. Siemens told the Senate Permanent Subcommittee on Investigations that it sent the payments to one of Ms. Douglas' U.S. accounts. In 2007, Mr. Abubakar was the subject of corruption allegations in Nigeria related to the Petroleum Technology Development Fund.

Of the USD 40 million in suspect funds, USD 25 million was wire transferred by offshore corporations into more than 30 U.S. bank accounts opened by Ms. Douglas, primarily by Guernsey Trust Company Nigeria Ltd., LetsGo Ltd. Inc. and Sima Holding Ltd.

The U.S. banks maintaining those accounts were, at times, unaware of her Politically Exposed Person (PEP) status, and they allowed multiple, large offshore wire transfers into her accounts. As each bank began to question the offshore wire transfers, Ms. Douglas indicated that all of the funds came from her husband and professed little familiarity with the offshore corporations actually sending her money. When one bank closed her account due to the offshore wire transfers, her lawyer helped convince other banks to provide a new account.

Source: United States Senate Permanente Subcommittee on Investigations (2010)

Case 31 **Red flag indicators:**	• Client requires introduction to financial institutions to help secure banking facilities • Client has family ties to an individual who held a public position and is engaged in unusual private business given the frequency or

	characteristics involved. • Involvement of structures with multiple countries where there is no apparent link to the client or transaction or no other legitimate or economic reason. • Private expenditure is being funded by a company, business or government.

Case 32: **Legal professionals create shell companies and permit transfers through their client account without underlying transactions to help a PEP suspected of corruption to access financial services – common law country**

Teodoro Nguema Obiang Mangue is the son of the President of Equatorial Guinea and the current Minister of Agriculture of that country. He used two attorneys in the U.S. to form shell corporations and launder millions of dollars through accounts held by those corporations to fund real property, living expenses, and other purchases in the U.S.

The shell corporations hid the identity of Obiang as a PEP, and, particularly, a PEP whose family had a reputation for corruption and contributed to the dismemberment and sale of an entire U.S. financial institution, Riggs Bank. Obiang's further use of his attorney's trust accounts to receive wire transfers from Equatorial Guinea, helped to provide an apparently legitimate reason for transfers from a high-risk country

As banks became aware of Obiang's connection to the shell companies and shut down their accounts, the attorneys would open new accounts and new institutions, concealing Obiang's beneficial ownership once again.

The Department of Justice has filed civil forfeiture actions in two district courts in Los Angeles and Washington to forfeit the proceeds of foreign corruption and other domestic offenses laundered through the U.S. *See* U.S. Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Keeping Foreign Corruption out of the United States: Four Case Histories* (Feb. 4, 2010).

Source: United States questionnaire response 2012: United States v. One White Crystal Covered Bad Tour Glove No.11-cv-3582 (C.D. Cal.), and United States v. One Gulfstream G-V Jet Aircraft, No. 11-cv-1874 (D.D.C.)

Case 32 **Red flag indicators:**	• Client required introduction to financial institutions to help secure banking facilities. • Client is a public official and has family ties to a head of state and is engaged in unusual private business given the frequency or characteristics involved • Involvement of structures with multiple countries where there is no apparent link to the client or transaction or no other legitimate or economic reason. • Private expenditure is being funded by a company, business or government. • There is an attempt to disguise the real owner or parties to the transaction.

Case 33: **Legal professional coordinates banking activities and sets up companies to assist with laundering – civil law country**

An individual in the Netherlands set up three companies. For one of the companies he held bearer shares. To hide his involvement in the companies he used a front man and a trust and company service provider as legal representatives.

For each of the companies, the legal representatives opened bank accounts with three different banks in different countries. The individual used the three companies to set up a loan-back scheme in order to transfer, layer and integrate his criminal money. He then co-mingled the criminal funds with the funds that originated from the legal activities of one of his companies. Next the front man bought real estate. To finance that transaction he arranged for a loan between the two companies.

Source: FATF (2007)

Case 33 **Red flag indicators:**	• There is an attempt to disguise the real owner or parties to the transaction. • Client required introduction to financial institutions to help secure banking facilities. • The transactions are unusual in that there is unexplained complexity in the structures and the funding arrangements. • Finance is being provided by a lender, other than a credit institution with no logical explanation or economic justification.

TECHNIQUE: INTRODUCTION TO OTHER PROFESSIONALS FOR PARTS OF A TRANSACTION

Other professionals, including other legal professionals, may not ask detailed CDD questions, where a client is referred to them by a legal professional. While making referrals or seeking additional expertise in another field to ensure the client obtains full advice is normal, receiving payment for such referrals may or may not be legal depending on the country.

Case 34: **Legal professional provides cover story for client when providing funds to a notary for a property purchase – civil law country**

Upon executing a deed of sale of a property, a notary received a cheque from the buyer‘s lawyer, Mr. M.

The lawyer pointed out to the notary that the money originated from the sale of a property that belonged to Mr. M‘s family. The cheque was first endorsed in favour of Mr. M‘s family before being endorsed to the notary. The cheque was issued from the lawyer‘s personal account rather than his client account.

Mr M’s bank account was credited by cash deposits, and thereafter, was mainly debited by mortgage repayments. Mr. M was known to the police for organised crime and armed robbery, for which he had already been convicted.

Source: Deloitte (2011)

Case 34 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime • The transaction is unusual as while there is a requirement in law for

	the notary to be involved in the transaction, there was no legitimate reason for the funds to be passed through the lawyer, and it would be against client account rules for the lawyer to put client's money into his personal account.

Case 35: **Criminal defence legal professional introduces clients to other professionals to assist with laundering the proceeds of their crime – common law country**

A prominent criminal defence attorney in Boston, Robert A. George helped a former client launder USD 200 000 in proceeds from various crimes, including wire fraud and cocaine distribution. George connected his former client to "his guy" who owned a mortgage company in Massachusetts and who accepted currency in duffel bags from the former client. George's associate then cut cheques to the former client to make the illicit funds appear to be a loan.

George was paid a fee for his part in the laundering scheme and also arranged a fee-splitting agreement with the former client to refer other criminals to him so that George could represent them in federal cases and launder their drug proceeds. Furthermore, George structured a USD 25 000 cash "retainer fee" from an undercover agent posing as a drug dealer into a bank account held in the name of his law firm, and issued a cheque to the apparent drug dealer with a memorandum note meant to conceal the purpose of the transaction. A notice of appeal has been filed in this case.

George was sentenced on October 31, 2012, to three and a half years for money laundering and related crimes following his jury trial in June 2012. George was convicted of money laundering conspiracy, aiding and abetting money laundering, money laundering, and structuring transactions to avoid reporting requirements.

Source: United States (2012) questionnaire response - United States v. George, No. 11-cr-10201-NMG (D. Mass.)

Case 35 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime. • Disproportionate amounts of cash and private funding in terms of the client's known legitimate income. • Legal professional's referral to non-legal professional constitutes professional ethics rule violations

TECHNIQUE: MANAGEMENT OF A CLIENT'S GENERAL AFFAIRS

Another feature of the highlighted cases involves the legal professional undertaking a range of 'management' activities for clients. In some jurisdictions this is referred to as 'man of affairs work' which is permitted in limited circumstances by some professional rules.

Situations where a legal professional may be undertaking these activities legitimately may involve a client who has limited capacity to manage their own affairs, or in other circumstances where the client has limited other options or a clear legitimate rational for seeking the continuing assistance from his/her legal professional. The legal professional, whether acting pursuant to a court order or a power of attorney, may use his/her client account to undertake transactions, but would more typically use accounts held by the client for whom the legal professional is acting.

In reported cases where illicit proceeds were involved, clients have had full capacity to manage their affairs and there is limited justification requiring specialist skills of the legal professional or use of their client account.

From the cases considered during this typology, it is apparent that the legal professional is more likely to be either complicit or wilfully blind to the red flag indicators of money laundering when this technique is employed In order to act in the client's best interests in such situations it is imperative they fully understand the financial and business affairs they are being asked to manage.

Other management activities may raise the question as to whether the legal professional is really acting as a financial advisor and mortgage broker. Such conduct especially when provided without connection to other legal services, may not be within the scope of the activities of a legal professional; may require separate licensing depending on the country; and may not attract professional secrecy/ legal professional privilege.

Case 36: **Criminal defence legal professional introduces clients to other professionals to assist with laundering the proceeds of their crime – common law country**

A lawyer was instructed by his client, a drug trafficker, to deposit cash into the lawyer's trust account and then make routine payments to mortgages on properties beneficially owned by the drug trafficker.

The lawyer received commissions from the sale of these properties and brokering the mortgages.

While he later admitted to receiving the cash from the trafficker, depositing it into his trust account and administering payments to the trafficker's mortgages, the lawyer denied knowledge of the source of funds.

Source: FATF (2004)

Case 36 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime • Disproportionate amounts of cash and private funding in terms of the client's known legitimate income. • Client is using an agent or intermediary without good reason.

Case 37: **Legal professional undertakes financial transaction unrelated to the provision of legal services to hide funds from a bankruptcy**

A trading company, operated by the client's spouse, was declared bankrupt.

Shortly afterwards the client deposited cash (from the bankrupt company) in an account opened in the name of a family member.

The money was immediately paid by cheque to the account of a legal professional.

The legal professional deposited part of the funds back into the family member's account and used the rest to purchase a life assurance policy, via a bank transfer. The policy was immediately cashed in by the family member.

Source: Belgium (2012) questionnaire response

Case 37 **Red flag indicators:**	• Private expenditure is being funded by a company • The transaction is unusual in terms of funding arrangements, who the client is, and the reason for the involvement of the legal professional. • The use of "U-turn" transactions where money is transferred to a legal professional or other entity and then sent back to the originating account in a short timeframe • Insurance policies cashed in shortly after purchase or loans and mortgages paid quickly, in full

METHOD 6: LITIGATION

Litigation is not an activity covered by the FATF Recommendations and, as outlined above, the courts to date have held that its exclusion is important for the protection of the fundamental human right of access to justice. However, in the case of Bowman v Fels[41] – the only case to specifically consider the question in the context of a real case involving clients[42] – the English Court of Appeal held that while genuine litigation should be exempt from the reporting requirements, sham litigation would not as such litigation is an abuse of the court's processes.

Litigation could constitute *sham litigation* if the subject of the dispute was fabricated (for example if there is no actual debt and the funds being transferred are simply the proceeds of crime being passed from one entity to another) or if the subject of the litigation was a contract relating to criminal activity which a court would not enforce.[43]

Case 38: **Legal professionals pursue debts relating to criminal activity – civil law country**

In 2005, two lawyers unsuccessfully defended two clients who were prosecuted for criminal offences. They then assisted those clients to recover debts of over 5 million NOK from other known criminals. Both lawyers were convicted of money laundering.

Source: Norway (2012) questionnaire response

Case 38 **Red flag indicators:**	• Client with known convictions for acquisitive crime • Debts relate to contract based on criminal activity

Case 39: **Legal professional files STR on debt recovery transaction without economic rationale – civil law country**

In 2011, a notary submitted an STR on the unusual movement of funds between companies as a purported debt recovery action. A lawyer acting for Company A created two further limited liability companies in Spain – Company B and Company C.

Within a month, four significant transactions take place on the same day which all required involvement of notary:

1. Mr X (an Italian national, whom the press reported was linked to the Mafia) acknowledges to a notary, a debt of around EUR 440 000 they owned to Company B, but it is not clear on what basis this debt exists.
2. Mr X sells a number of real estate properties to Company B for approximately EUR 460 000, which is paid through an electronic transfer, a bankers draft and a credit agreement.
3. Company A sells the shares for Company B to Company C.
4. The shares in Company C are bought by a Swiss company.

41 [2005] EWCA Civ 226.

42 All of the other cases were constitutional challenges on the legitimacy of legislation in principle.

43 Corbin A.L 1962 Corbin on Contracts West Publishing Co.

Later that year, Company B acknowledges to a notary a debt of around EUR 600 000 to the Swiss Company, who bought Company C. The agreement the notary is asked to confirm involves quarterly payments of EUR 7 500 with the Swiss company obtaining stock options for Company C. The basis of this debt was also unclear.

Source: Spain (2012) questionnaire response

Case 39 **Red flag indicators:**	• There are multiple appearances of the same parties in transactions over a short period of time. • Large financial transactions requested by recently set up companies, not justified by the activity of the client. • Creation of complicated ownership structures where there is no legitimate or economic reason There was no legitimate economic reason to create two companies, where the intention was to sell one to the other in such a short space of time, especially when control over both was passed to a company domiciled in another country at the same time. The creation of the purported debts and significant real estate purchase were designed to give the appearance of commercial business relationships to justify the transfer of value between Italy and Switzerland, via Spain. • A party to the transaction has known links to organised crime.

Case 40: **Legal practitioners receive requests for use of client account to recover debts with little or no legal services to be provided – common law country**

Australian legal practitioners have advised AUSTRAC of receiving unusual requests from prospective clients, particularly targeted at passing funds through solicitors' trust accounts. This included a foreign company requesting legal services involving debt recovery, with the legal firm receiving substantial payments into its trust account from purported debtors (both in Australia and overseas) with little debt recovery work actually being required to be undertaken by the firm.

These types of approaches to legal professionals have been noted by FIUs and SRBs in a number of countries, although no detailed case studies were provided.

Source: AUSTRAC (2011)

Case 40 **Red flag indicators:**	• Client and/or debtor are located at a distance from the legal professional • The type of debt recovery is unusual work for the legal professional • The client has written a pre-action letter to the debtor naming the legal professional and providing the legal professional's client account details • The litigation is settled very quickly, sometimes before the legal professional has actually written to the debtor • Client is unconcerned about the level of fees • There is a request for the funds received from the debtor to be paid out very quickly, sometimes to third parties.

METHOD 7: OTHER METHODS

TECHNIQUE: USE OF SPECIALISED LEGAL SKILLS

Legal professionals possess a range of specialised legal skills which may be of interest to criminals, in order to enable them to transfer value obtained from criminal activity between parties and obscure ownership.

These specialised skills include the creation of financial instruments, advice on and drafting of contractual arrangements, and the creation of powers of attorney.

In other areas of legal specialisation, such as probate (succession) and insolvency or bankruptcy work, the legal professional may simply come across information giving rise to a suspicion that the deceased or insolvent individual previously engaged in criminal activity or that parties may be hiding assets to avoid payment to legitimate creditors. Countries differ on how unexpected sums of cash are treated in relation to probate or insolvency cases, in some a threshold report will be made and the government becomes a super-creditor able to recover the money before any other beneficiary; in other countries this would give rise to a suspicion of money laundering, requiring a STR to be filed and possibly putting the executor or the legal professional at risk of money laundering.

Depending on the complexity of the arrangement, a legal professional could be unwittingly involved in the money laundering, complicit or wilfully blind through failing to ask further questions about suspicious instructions.

Case 41: **Legal professional prepares a power of attorney to dispose of all assets belonging to a client facing drug trafficking charges**

A legal professional was asked to prepare a power of attorney for a client to give control of all of his assets to his girlfriend, including power to dispose of those assets.

The legal professional then prepared a deed of conveyance under which the girlfriend transferred all of the property to the client's brother and sister.

The legal professional had just secured bail for the client in relation to a drug trafficking charge.

The legal professional was acquitted of money laundering.

Source: Trinidad & Tobago (2012) questionnaire response

Case 41 **Red flag indicators:**	• A power of attorney is sought for the disposal of assets under conditions which are unusual and where there is no logical explanation – it would have to be very exceptional circumstances for it to be in the client's best interests to allow them to make themselves impecunious. • Unexplained speed and complexity in the transaction. • Client is known to be under investigation for acquisitive crime.

Case 42: **Legal professional submits STR on commercial arrangement which has not economic rationale – civil law country**

In 2008 a Spanish citizen (Mr A) and a citizen from a Middle East country (Mr B) attended a notary office to formalise a contract which provided:

1. Mr A is the holder of a Gold Import Licence from an African Republic.
2. Mr B will fund the gold importation by making a payment of EUR 8 000, through a promissory note of EUR 6 000 maturing later that year and the remaining EUR 2 000 in cash three days after the promissory note matures.
3. Mr A will make payments of EUR 4 000 per month to Mr B, on the 22nd of each month for an indefinite period to represent the profits of the gold import activity.
4. Either party may terminate the agreement, with Mr A refunding the EUR 8 000 to Mr B and an agreement that the termination will be accepted without question.

These are new clients for the notary, Mr A refuses to provide certain identification information requested by the notary and no records supporting any business activity of any kind by either party are provided. The notary submitted an STR.

Source: Spain (2012) questionnaire response

Case 42 **Red flag indicators:**	• The client is reluctant to provide information usually required in order to enable the execution of the transaction. • There are a number of high risk countries involved in the transaction • The transaction makes no economic sense given the evident imbalance suffered by Mr A. • The transaction was unusual for this notary, given their unfamiliarity with the parties, the gold import business and the international elements of the transaction.

Case 43: **Legal professionals uncover funds tainted by criminal activity during administration of an estate – common law country**

A firm of solicitors was instructed to act in the administration of a deceased person's estate.

When attending the deceased's property a large amount of cash was found.

In addition, the individual had a savings account holding GBP 20 000.

As part of the administration of the estate the solicitor subsequently identified that the individual was receiving state benefits, to which they would not have been entitled if the hidden assets had been known, thus meaning that the entire estate of the client was now tainted by this criminality

The solicitor filed an STR.

Source: United Kingdom (2012) presentation at typologies workshop

Case 43 **Red flag indicators:**	• Disproportionate levels of private funding and cash which is inconsistent with the socio-economic profile of the individual. • Information suggesting involvement in acquisitive criminal activity.

Case 44: **Legal professional's attention drawn to unusual purchases of assets during the administration of a bankruptcy – civil law country**

In a bankruptcy case where A and B were guarantors, a notary was appointed by the court to proceed with the public sale of different goods of the parties concerned. In the context of the public sale. The attention of the notary was drawn to the fact that several of the goods were purchased by X, the daughter of A and B. Additionally, the total amount of the purchases was significant and was not commensurate with the socio-economic status of X, who was unemployed.

The purchased goods were partially funded by a cheque of a mortgage loan that a bank granted to X. The balance came from an account which was opened in the name of a third person, C.

This account had received several deposits in cash and transfers from a company of which both C and B were partners. B had been a partner in different companies that were declared bankrupt and for which he was known to the judicial authorities. Further, the daughter who had purchased the goods was not a director of this company, was not subject to VAT in Belgium and her official income consisted only of unemployment benefits.

With this information the FIU research indicated that the funds that were deposited on the accounts of C in cash may have come from funds that B had taken without permission to help his daughter to buy a part of his own real estate. C and B knew each other as they were partners in the same company.

In this case, the account of C was used as inadvertent account to conceal the illegal origin of the funds. Taking the above elements the various purchases of X can therefore be associated with a crime relating to the bankruptcy. A law enforcement investigation started.

Source: Cellule de traitement des informations Financières (2006)

Case 44 **Red flag indicators:**	• The ties between the parties are of a family nature, which generate doubts as to the real nature or reason for the transaction. • Disproportionate private funding which was inconsistent with the socio-economic profile of the individual. • Third party funding with no apparent connection or legitimate explanation

TECHNIQUE: PAYMENT OF LEGAL FEES AND ASSOCIATED EXPENSES

In some countries there are specific exemptions to enable legal practitioners to be paid with the proceeds of crime for defence purposes, provided that the defence fees are reasonable to the services rendered and that any remaining funds are not returned to the client or to third parties. In other countries this would still constitute money laundering and the fees paid would be amenable to confiscation proceedings.

Case 45: **Legal practitioner uses known criminal funds to pay for expenses of client who was in prison – common law country**

Miguel Rodriguez-Orejuela was a leader of the Cali Cartel who required and enforced a vow of silence from his associates and employees. In return for this vow of silence regarding his association

with drug trafficking, Rodriguez-Orejuela agreed to pay the defence expenses of any of his associates and to compensate their families while they were in prison.

Through his law firm, Michael Abbell facilitated the payments to family and prison commissary accounts on behalf Rodriguez-Orejuela. The funds Abbell accepted to reimburse these payments came from Rodriguez-Orejuela, who had no legitimate form of income (all his businesses were in fact funded by narco-trafficking). Abbell would make the payments, often using money orders paid for by the law firm, and then bill Rodriguez-Orejuela for reimbursement and fees. The transactions were designed to conceal the fact that Rodriguez-Orejuela was funding the payments and was associated with drug activity.

After two trials, a jury convicted Abbell of money laundering and racketeering charges. *See* 271 F.3d 1286 (11th Cir. 2001) (affirming convictions and reversing district court's grant of judgment of acquittal on racketeering-related counts). Abbell was sentenced to 97 months' incarceration.

Source: United States (2012) questionnaire response United States v. Abbell, No. 93-cr-470(17) (S.D. Fla.)

Case 45 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals. • Disproportionate private funding or cash (potentially from a third party) which is inconsistent with known legitimate income. • There is an attempt to disguise the real owner or parties to the transactions.

Case 46: **Legal practitioner accepted large amounts of cash from a known criminal to pay for legal fees – common law country**

Defense attorney Donald Ferguson was indicted on four counts of money laundering, and one count of conspiring to launder money. Ferguson accepted four large sums of cash totalling USD 566 400 from Salvador Magluta. Ferguson deposited the cash payments into his attorney trust accounts, supposedly as payment for the defence of an associate of Magluta. Ferguson ultimately pleaded guilty to one count of money laundering and consented to the forfeiture of the full amount of the payments. He was sentenced to five years' probation. *See* 142 F. Supp. 2d 1350 (S.D. Fla. 2000) (declining to dismiss indictment).

Source: United States (2012) questionnaire response United States v. Ferguson, No. 99-cr-116 (S.D. Fla.)

Case 46 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals. • Disproportionate private funding or cash (potentially from a third party) which is inconsistent with known legitimate income.

Case 47: **Legal practitioner paid 'salary' by organised criminals to be available to represent their needs, irrespective of whether legal services were provided – civil law country**

In July 1999 La Stampa reported a criminal lawyer and accountant arrested by DIA,17 (Anti-mafia Investigation Department), who were charged with facilitating funds from illicit sources on the French Riviera. The arrests were the consequence of investigations and electronic surveillance

(phone and environmental wiretapping), corroborated by the lawyer's confession. The lawyer's office was the operational base for the criminal activities of two high-profile mafia bosses. According to the indictment, the lawyer was paid a monthly salary of about EUR 6 000 to be always available for the needs of the mafia family.

Source: Di Nicola, A. and Zoffi, P. (2004)

Case 47 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals. • Disproportionate private funding or cash (potentially from a third party) which is inconsistent with known legitimate income. • Payment of a general retainer rather than fees for specific services, where professional rules require the provision of itemised bills.

TECHNIQUE: PROVIDING LEGAL SERVICES FOR CHARITIES

Legal professionals may be involved in setting up charities or other non-profit entities, acting as a trustee, and providing advice on legal matters pertaining to the charity, including advising on internal investigations.

Like many other businesses, charities can be victims of fraud from trustees, employees and volunteers or be set up as vehicles for fraud, which will involve the proceeds of crime and subsequent money laundering. FATF typologies have also identified a particular vulnerability for charities in the financing of terrorism. [44]

Case 48: **Legal professional sets up charity to provide funding to individuals convicted of terrorist activities – civil law country**

This case has been brought to the attention of the Dutch Bureau for Supervision. A Foundation was established by a person related to a member of an organization whose purpose is committing terrorist offences. This person was herself not designated on international sanctions. The goal for the foundation was to provide help to persons convicted of terrorist activities. A first notary refused to establish the foundation, while a second notary agreed to do so.

Providing this form of financial assistance to a person convicted of terrorist activities, given the specific circumstances of the case, did not constitute an offence of financing terrorism, so no prosecutions were brought.

Source: Netherlands (2012) questionnaire response

Case 48 **Red flag indicators:**	• Client is related to a person listed as having involvement with a known terrorist organisation • Funding is to be provided to a person convicted of terrorist activities

44 FATF (2008b); FATF typology 2002-2003.

Case 49: **Legal professional sets up charities to undertake criminal activity and deal with the proceeds of that crime – common law country**

Attorney and lobbyist Jack Abramoff pleaded guilty in 2006 to three counts including conspiracy to defraud the United States, tax evasion, and "honest services" fraud (a corruption offense), upon the filing of a criminal information in the U.S. District Court for the District of Columbia. While working for two law and lobbying firms between 1999 and 2004, Abramoff solicited and lobbied for various groups and businesses, including Native American tribal governments operating or interested in operating casinos.

Abramoff conspired with former Congressional staff member Michael Scanlon to: defraud his lobbying clients by pocketing approximately USD 50 million; misuse his charitable organization by using it to finance a lavish golf trip to Scotland for public officials and others; and to provide numerous "things of value" to public officials in exchange for benefits to his clients.

In one set of schemes, Abramoff employed a non-profit that he founded called Capital Athletic Foundation. The Foundation was intended to fundraise for a non-profit school and it was granted tax-exempt status from the Internal Revenue Service, however, Abramoff used it as a personal slush fund. One congressional staffer solicited a contribution from a Russian distilled beverage company and Abramoff client on behalf of the Foundation. Abramoff used the Russian client's donation for personal and professional benefit, namely, to finance a trip to Scotland attended by members of Congress that cost the Foundation approximately USD 166 000.

Another Abramoff client, a wireless company, was solicited to make a contribution of at least USD 50 000 to the Foundation, in exchange for Abramoff securing a license for the company without charging his firm's usual lobbying fee or even informing his firm of the arrangement. According to the criminal information, Abramoff also concealed assets and sources of income from the Internal Revenue Service through the use of nominees, some of which were tax-exempt organizations.

Although not detailed in the court filings in this case, it was widely reported at the time that a congressional staff member's spouse received USD 50 000 from another non-profit affiliated with Abramoff, which in turn, received money from Abramoff clients interested in internet gambling and postal rate issues before Congress. Further, the Capital Athletic Foundation allegedly donated USD 25 000 to Representative and House Majority Leader Tom DeLay's Foundation for Kids. These are just a few examples of Abramoff's misuse of non-profits, some of which were founded by him and some of which existed previously and accepted contributions from Abramoff, Scanlon, or their clients, often due to Abramoff's personal relationships with the heads of such charities.

Abramoff was also indicted in 2005 in the Southern District of Florida in connection with a massive fraud that he conducted involving his purchase of a casino and cruise company. Abramoff pleaded guilty to two more counts of conspiracy and wire fraud in the Florida case, which did not involve the misuse of tax-exempt entities. He was never charged with money laundering.

Source: United States (2012) questionnaire response - United States v. Abramoff, No. 06-cr-00001 (D.D.C.)

Case 49 **Red flag indicators:**	• Non-profit organisation engages in transactions not compatible with those declared and not typical for that body • There are attempts to disguise the real owner or parties to the transactions

CHAPTER 5

RED FLAG INDICATORS

As outlined in Chapter 4 the methods and techniques used by criminals to launder money may also be used by clients with legitimate means for legitimate purposes.

Because of this, red flag indicators should always be considered in context. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, as a client may be able to provide a legitimate explanation.

These red flag indicators should assist legal professionals in applying a risk-based approach to their CDD requirements of knowing who their client and the beneficial owners are, understanding the nature and the purpose of the business relationship, and understanding the source of funds being used in a retainer. Where there are a number of red flag indicators, it is more likely that a legal professional should have a suspicion that ML or TF is occurring.

SRBs and law enforcement may also find these red flag indicators to be useful when monitoring the professional conduct of or investigating legal professionals or their clients. Where a legal professional has information about a red flag indicator and has failed to ask questions of the client, this may be relevant in assessing whether their conduct was complicit or unwitting.

This chapter contains a collection of red flag indicators identified through the case studies, literature reviewed, and existing advice published by FIUs and SRBs which were provided in response to the questionnaire.

RED FLAGS ABOUT THE CLIENT

- Red flag 1: The client is overly secret or evasive about:
  - who the client is
  - who the beneficial owner is
  - where the money is coming from
  - why they are doing this transaction this way
  - what the big picture is.
- Red flag 2: The client:
  - is using an agent or intermediary without good reason.
  - is actively avoiding personal contact without good reason.

- is reluctant to provide or refuses to provide information, data and documents usually required in order to enable the transaction's execution
- holds or has previously held a public position (political or high-level professional appointment) or has professional or family ties to such an individual and is engaged in unusual private business given the frequency or characteristics involved.
- provides false or counterfeited documentation
- is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain part such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact.
- is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals
- is or is related to or is a known associate of a person listed as being involved or suspected of involvement with terrorist or terrorist financing related activities.
- shows an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory customer identification, data entries and suspicious transaction reports – that is – asks repeated questions on the procedures for applying the ordinary standards.

- Red flag 3: The parties:
  - The parties or their representatives (and, where applicable, the real owners or intermediary companies in the chain of ownership of legal entities), are native to, resident in or incorporated in a high-risk country
  - The parties to the transaction are connected without an apparent business reason.
  - The ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature or reason for the transaction.
  - There are multiple appearances of the same parties in transactions over a short period of time.
  - The age of the executing parties is unusual for the transaction, especially if they are under legal age, or the executing parties

are incapacitated, and there is no logical explanation for their involvement.

- There are attempts to disguise the real owner or parties to the transaction.
- The person actually directing the operation is not one of the formal parties to the transaction or their representative.
- The natural person acting as a director or representative does not appear a suitable representative.

RED FLAGS IN THE SOURCE OF FUNDS

- Red Flag 4: The transaction involves a disproportional amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.
- Red flag 5: The client or third party is contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly, without logical explanation.
- Red flag 6: The source of funds is unusual:
  - third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation
  - funds received from or sent to a foreign country when there is no apparent connection between the country and the client
  - funds received from or sent to high-risk countries.
- Red flag 7: The client is using multiple bank accounts or foreign accounts without good reason.
- Red flag 8: Private expenditure is funded by a company, business or government.
- Red flag 9: Selecting the method of payment has been deferred to a date very close to the time of notarisation, in a jurisdiction where the method of payment is usually included in the contract, particularly if no guarantee securing the payment is established, without a logical explanation.
- Red flag 10: An unusually short repayment period has been set without logical explanation.
- Red flag 11: Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.
- Red flag 12: The asset is purchased with cash and then rapidly used as collateral for a loan.

- Red flag 13: There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested which are not appropriate for the common practice used for the ordered transaction.
- Red Flag 14: Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification.
- Red Flag 15: The collateral being provided for the transaction is currently located in a high-risk country.
- Red flag 16: There has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation.
- Red flag 17: There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk.
- Red flag 18: The company receives an injection of capital or assets in kind which is notably high in comparison with the business, size or market value of the company performing, with no logical explanation.
- Red flag 19: There is an excessively high or low price attached to the securities transferred, with regard to any circumstance indicating such an excess (*e.g.* volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation.

- Red flag 20: Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the client or the possible group of companies to which it belongs or other justifiable reasons.

RED FLAGS IN THE CHOICE OF LAWYER

- Red flag 21: Instruction of a legal professional at a distance from the client or transaction without legitimate or economic reason.
- Red flag 22: Instruction of a legal professional without experience in a particular specialty or without experience in providing services in complicated or especially large transactions..
- Red flag 23: The client is prepared to pay substantially higher fees than usual, without legitimate reason.
- Red flag 24: The client has changed advisor a number of times in a short space of time or engaged multiple legal advisers without legitimate reason

- Red flag 25: The required service was refused by another professional or the relationship with another professional was terminated.

RED FLAGS IN THE NATURE OF THE RETAINER

- Red flag 26: The transaction is unusual, *e.g.*:
    - the type of operation being notarised is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting
    - the transactions are unusual because of their size, nature, frequency, or manner of execution
    - there are remarkable and highly significant differences between the declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional
    - a non-profit organisation requests services for purposes or transactions not compatible with those declared or not typical for that body.
- Red flag 27: The client:
    - is involved in transactions which do not correspond to his normal professional or business activities
    - shows he does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested
    - wishes to establish or take over a legal person or entity with a dubious description of the aim, or a description of the aim which is not related to his normal professional or commercial activities or his other activities, or with a description of the aim for which a license is required, while the customer does not have the intention to obtain such a licence
    - frequently changes legal structures and/or managers of legal persons
    - asks for short-cuts or unexplained speed in completing a transaction
    - appears very disinterested in the outcome of the retainer
    - requires introduction to financial institutions to help secure banking facilities

- Red flag 28: Creation of complicated ownership structures when there is no legitimate or economic reason.
- Red flag 29: Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason.
- Red flag 30: Incorporation and/or purchase of stock or securities of several companies, enterprises or legal entities within a short period of time with elements in common (one or several partners or shareholders, director, registered company office, corporate purpose etc.) with no logical explanation.
- Red flag 31: There is an absence of documentation to support the client's story, previous transactions, or company activities.
- Red flag 32: There are several elements in common between a number of transactions in a short period of time without logical explanations.
- Red flag 33: Back to back (or ABC) property transactions, with rapidly increasing value or purchase price.
- Red flag 34: Abandoned transactions with no concern for the fee level or after receipt of funds.
- Red flag 35: There are unexplained changes in instructions, especially at the last minute.
- Red flag 36: The retainer exclusively relates to keeping documents or other goods, holding large deposits of money or otherwise using the client account without the provision of legal services.
- Red flag 37 There is a lack of sensible commercial/financial/tax or legal reason for the transaction.
- Red flag 38 There is increased complexity in the transaction or the structures used for the transaction which results in higher taxes and fees than apparently necessary.
- Red flag 39: A power of attorney is sought for the administration or disposal of assets under conditions which are unusual, where there is no logical explanation.
- Red flag 40: Investment in immovable property, in the absence of any links with the place where the property is located and/ or of any financial advantage from the investment.
- Red flag 41: Litigation is settled too easily or quickly, with little/no involvement by the legal professional retained.
- Red flag 42: Requests for payments to third parties without substantiating reason or corresponding transaction.

CHAPTER 6

CONCLUSIONS

KEY FINDINGS

This typology has found evidence that criminals seek out the involvement of legal professionals in their money laundering schemes, sometimes because the involvement of a legal professional is required to carry out certain types of activities, and sometimes because access to specialised legal and notarial skills and services may assist the laundering of the proceeds of crime and the funding of terrorism.

Case studies, STRs and literature point to the following legal services being vulnerable to misuse for the purpose of ML/TF:

- client accounts (administered by the legal professional)
- purchase of real property
- creation of trusts and companies
- management of trusts and companies
- setting up and managing charities
- administration of deceased estates
- providing insolvency services
- providing tax advice
- preparing powers of attorney
- engaging in litigation – where the underlying dispute is a sham or the debt involves the proceeds of crime.

Not all legal professionals are involved in providing these types of legitimate legal services that criminals may seek to abuse, but in some cases a legal professional may need to be involved. This makes the use of legal professionals carrying out these activities uniquely exposed to criminality, irrespective of the attitude of the legal professional to the criminality.

It is accepted that the vast majority of legal professionals seek to comply with the law and their professional requirements, and they have no desire to be involved in ML/TF activity. The legal profession is highly regulated. Furthermore, ethical obligations, professional rules and guidance on ML/TF provided by SRBs and professional bodies should cause legal professionals to refuse to act for clients who seek to misuse legal services for ML/TF purposes.

To keep legal professionals from becoming involved in ML/TF however, the above factors rely on the legal professionals:

- being alert to red flags indicating that the client is seeking to involve them in criminal activity
- choosing to abide by their ethical obligations and applicable professional rules; and
- discerning legitimate client wishes from transactions and structures intended to conceal or promote criminal activity or thwart law enforcement.

Equally, the application of FATF Recommendations to legal professionals over the last decade should provide the legal sector with tools to better identify situations where criminals are seeking to misuse legal services.

Some SRBs and professional bodies are quite active in educating their members on the ML/TF vulnerabilities they face and the red flag indicators which could alert them to a suspicious transaction. STRs from legal professionals have also assisted law enforcement in detecting and prosecuting criminals engaged in ML/TF activity.

However, not all legal professionals are undertaking the CDD measures required by the FATF Recommendations, and not all SRBs and professional bodies have a clear understanding of information on ML/TF vulnerabilities specific to the legal sector to provide to their members.

A lack of awareness and/or lack of education of ML/TF vulnerabilities and red flag indicators reduces the likelihood that legal professionals would be in a position prevent the misuse of their services and avoid a breach of their professional obligations.

This typology research recognises that investigating a legal professional presents more practical challenges than investigating other professionals, due to the important protections for fundamental human rights which attach to the discharge of a legal professional's activities. However, the research has also confirmed that neither legal professional privilege nor professional secrecy would ever permit a legal professional to continue to act for a client who was engaging in criminal activity.

The scope of legal professional privilege/professional secrecy depends on the constitutional and legal framework of each country, and in some federal systems, in each state within the country. Practically, this diversity and differing interpretations by legal professionals and law enforcement on what information is actually covered by legal professional privilege / professional secrecy has, at times provided a disincentive for law enforcement to take action against legal professionals suspected of being complicit in or wilfully blind to ML/TF activity.

OPPORTUNITIES FOR FUTURE ACTION

This typology study should be used to increase awareness of the red flag indicators for potential misuse of legal professionals for ML/TF purposes and in particular for:

- **Legal professionals –** as this would assist in reducing their unwitting involvement in ML/TF activities undertaken by their clients and promote the filing of STRs where appropriate;
- **Financial institutions and other DFNBPs** – as this may alert them to situations where legal professionals are complicit in their client's ML/TF activity or are not aware of the red flag indicators to promote the filing of STRs where appropriate;
- **SRBs and professional bodies** – as this will assist in developing training programmes and guidance which focus not just on the law but the practical application of the law to everyday legal practice and assist in identifying both witting and unwitting involvement in ML/TF activities as part of their monitoring of professional conduct; and
- **Competent authorities and partner law enforcement agencies –** to assist in their investigation of ML/TF where legal services are a method used and to inform the assessment of whether it is likely that the legal professional is involved wittingly or unwittingly, so that appropriate action can be taken.

Potentially, the increased education of legal professionals on ML/TF vulnerabilities may include a discussion of AML/CFT risks and obligations in the course of the legal education or licensing of legal new professionals. Initially, this education can take place in the context of ethics and professionalism in courses and law schools, and later, through continuing education curricula.

Competent authorities, SRBs and professional bodies should review the case examples in this typology study and fit them to the specific roles and vulnerabilities of their members.

Increased interaction between competent authorities, supervisors and professional bodies in terms of sharing information on trends and vulnerabilities, as well as notifying each other of instances where legal professionals are failing to meet their ethical and legal obligations in an AML/CFT context, may also assist in reducing misuse of legal professionals. SRBs and professional bodies may find the red flag indicators in this report useful when monitoring their members' conduct against professional and client account rules.

There will be many factors taken into consideration when deciding whether to criminally prosecute a legal professional for money laundering of failing to submit an STR where required. In some instances, it will be more appropriate and effective for the SRB or professional body to take disciplinary or remedial action where the legal professional's conduct falls short of professional requirements and permits money laundering to occur, but was not intended to aid in money laundering. This shared approach to enforcement not only helps to combat ML / TF, but also helps to ensure that legal professionals uphold the rule of law and do not bring the wider profession into disrepute.

Competent authorities, SRBs and professional bodies should work to ensure that there is a clear and shared understanding of the remit of confidentiality, legal professional privilege and/or professional secrecy in their own country. A clear understanding of the remit of these principles and the procedures for investigating a legal professional will assist in reducing mistrust from both

parties during this process and may help to dispel the perception that privilege or secrecy is designed to protect criminals. It may also assist in more prompt investigation and prosecution of those who would misuse the services of legal professionals or abuse their role as a legal professional, while reducing the concern of legal professionals that they may be sanctioned for breaching privilege or secrecy when complying with their AML/CFT obligations.

Finally, this typology found that the analysis of STRs made about legal professionals and the types of assets being confiscated provided useful information on the AML/CFT risks posed by the legal sector. Member states may wish to consider using these sources of information when assessing risks for the purpose of completing the national risk assessment in line with FATF Recommendation 1. FATF can also consider this work, in consultation with the legal sector, when updating its RBA Guidance for Legal Professionals and other DNFBPs.

ANNEX 1
BIBLIOGRAPHY

FATF (2004), Report on Money Laundering Typologies 2003-2004, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/2003_2004_ML_Typologies_ENG.pdf

FATF (2006), *Misuse of Corporate Vehicles Including Trust and Company Service Providers*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Misuse%20of%20Corporate%20Vehicles%20including%20Trusts%20and%20Company%20Services%20Providers.pdf

FATF (2007), *Money Laundering and Terrorist Financing through the Real Estate Sector,* FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf

FATF (2008a) *Risk Based Approach Guidance for the Legal Sector, FATF, Paris,* www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf

FATF (2008b) *Terrorist Financing and Typologies Report,* FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

FATF (2010), *Money Laundering Using Trust and Company Service Providers*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf

FATF (2011), *Laundering the Proceeds of Corruption*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Laundering%20the%20Proceeds%20of%20Corruption.pdf

FATF (2012) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations, FATF, Paris,* www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

AUSTRAC (2011) *Money laundering in Australia 2011*, Austrac, Australia, http://www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf

Cellule de traitement des information Financieres (2005), *Doorgemelde dossiers in verband met corruptie, typologische aspecten* (*files reported in connection with corruption, typological aspects*), Cellule de traitement des information Financieres, Belgium

Cellule de traitement des information Financieres (2006), *Notarissen en witwasbestrijding* (*Notaries and combating money laundering*), Cellule de traitement des information Financieres, Brussels

Cellule de traitement des information Financieres (2007), *Jaarverslag 2007* (annual report 2007) Cellule de traitement des information Financieres, Brussels

Cellule de traitement des information Financieres (2008), *Jaarverslag 2008* (annual report 2008) Cellule de traitement des information Financieres, Brussels

Cellule de traitement des information Financieres (2009), *Jaarverslag 2009* (annual report 2009) Cellule de traitement des information Financieres, Brussels

Cummings, L. and Stepnowsky, P.T. (2011), *My Brother's Keeper: An Empirical Study of Attorney Facilitation of Money Laundering through Commercial Transactions*, University of Maryland Legal Studies Research Paper No. 2010-32, University of Maryland, College Park

Deloitte (2011), *Final Study on the Application of the Anti-Money Laundering Directive: Commissioned by the European Commission*, Deloitte DG Internal Market and Services – Budget, European Commission, Brussels

Dodek, A. (2011), *Solicitor-Client Privilege in Canada: Challenges for the 21st Century,* The Canadian Bar Association, Ottawa

Does, van der, E. et al. (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It, Stolen Asset Recovery Initiative (StAR)*, World Bank/UNODC, Washington, D.C.

European Commission (2006), *The application to the legal profession of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering*, European Commission, Brussels

Gallant, M. (2010), *Uncertainties Collide: Lawyers and Money Laundering, Terrorist Finance Regulation*, Journal of Financial Crime, Vol. 16, University of Manitoba, Winnipeg

Global Witness (2009), *The Secret Life of a Shopaholic: How an African Dictator's Playboy Son Went on a Multi-million Dollar Shopping Spree in the US*, Global Witness, London, www.globalwitness.org/sites/default/files/pdfs/gw_obiang_low.pdf

IBA, OECD and UNODC (2010), *Risks and Threats of Corruption and the Legal Profession Survey*, IBA, OECD and UNODC, at www.oecd.org/investment/anti-bribery/46137847.pdf

International Bar Association (2011), *IBA International Principles on Conduct for the Legal Profession (IBA International Principles)*, London www.ibanet.org/Article/Detail.aspx?ArticleUid=BC99FD2C-D253-4BFE-A3B9-C13F196D9E60

International Union of Notaries (2004), *Principles of Notarial Ethics*, Rome http://uinl.net/presentacion.asp?idioma=ing&submenu=DEONTOLOGIA

Journal of Crime, Law & Social Change (2004), Vol. 42, Springer, Boston

- Levi, M. *et al.* (2004), "Lawyers as crime facilitators in Europe: An introduction and overview"

- Middleton, D.J. (2004), "The legal and regulatory response to solicitors involved in serious fraud"

- Middleton D.J. and Levi, M. (2004), "The role of solicitors in facilitating organised crime: situational crime opportunities and their regulation"

- Lankhorst, F. and Nelen, H. (2004), "Professional services and organised crime in the Netherlands"

- Chevrier, E., "The French government's will to fight organised crime and clean up the legal professions: the awkward compromise between professional secrecy and mandatory reporting"

- Di Nicola, A. and Zoffi, P. (2004), "Italian lawyers and criminal clients: Risks and countermeasures"

Parlementaire enquête-commissie opsporings-methoden (*parliamentary hearing regarding methods of investigation*) (1996), *Inzake Opsporing* ("Regarding investigation"), The Hague

Schneider, S. (2004), *Money Laundering in Canada: An analysis of RCMP cases*, Nathan Centre for the Study of Organized Crime and Corruption, Toronto, https://www.ncjrs.gov/App/publications/Abstract.aspx?id=232379

Tavares, C., et al. (2010), *Money Laundering in Europe: Report of Work Carried Out by Eurostat and DG Home Affairs*, Eurostat, Brussels

United States Senate Permanent Subcommittee on Investigations (2010), *Keeping Foreign Corruption Out of the United States: Four Case Histories*, United States Senate, Washington, D.C. http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=2de71520-5901-4a31-98ad-5138aebc49c2

Van Dijken, A. (2009), *Verdachte transacties bij advocaten en juridisch adviseurs, een analyse van verdachte transacties uit 2009 gemeld door advocaten en juridisch adviseurs* (*Suspicious transactions at lawyers and legal advisers, an analysis of suspicious transactions reported by lawyers and legal advisers from 2009*), FIU-Netherlands, The Hague

Van Duyne, P.C., et al. Eds., (2007), *Crime business and crime money in Europe: the dirty linen of illicit enterprise,* Wolf Legal Publishers, Nijmegen

World Economic Forum (2012), *Organised Crime Enablers*, World Economic Forum, Geneva, www3.weforum.org/docs/WEF_GAC_OrganizedCrimeEnablers_Report_2012.pdf

Other Resources:

American Bar Association (2010), *Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing, American Bar Association, Washington, D.C.,* www.americanbar.org/content/dam/aba/publishing/criminal_justice_section_newsletter/crimjust_taskforce_gtfgoodpracticesguidance.authcheckdam.pdf

IBA Anti-Money Laundering Forum www.anti-moneylaundering.org/

Law Society of England and Wales (2012) Anti-Money Laundering Practice Note, Law Society, London www.lawsociety.org.uk/advice/anti-money-laundering/

Federation of Law Societies Canada Model Rules to Fighting Money Laundering and Terrorist Financing www.lawsociety.org.uk/advice/anti-money-laundering/

Law Council of Australia (2009) Anti-Money Laundering Guide for legal practitioners, Law Council, Canberra, www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=8FCE74BF-1E4F-17FA-D2A2-C549BD6656B4&siteName=lca

ANNEX 2
RESPONDENTS TO THE QUESTIONNAIRE

RESPONSES RECEIVED FROM MEMBER STATES AND ASSOCIATE MEMBER STATES:

Australia	Austria	Belgium
Canada	Denmark	Finland
France	Japan	Ireland
Italy	Japan	Netherlands
Norway	Portugal	Spain
Sweden	Switzerland	Turkey
United Kingdom	United States	Bermuda
Curacao	St Vincent & the Grenadines	Trinidad & Tobago
Gibraltar	Jordan	Liechtenstein
Montenegro		

RESPONSES RECEIVED FROM SRBS OR PROFESSIONAL BODIES IN THE FOLLOWING COUNTRIES:

Australia	Austria	Belgium
Canada	Denmark	France
Germany	Ireland	Italy
Japan	Luxembourg	Netherlands
Norway	Portugal	South Africa
Spain	Sweden	Switzerland
United Kingdom	United States	Bermuda
Curacao	Namibia	Saint Vincent & the Grenadines
Trinidad & Tobago	Malawi	Cyprus
Czech Republic	Estonia	Hungary
Montenegro	Poland	Slovakia
Slovenia	Swaziland	

ANNEX 3
DEFINITIONS

Mechanism: An ML/TF mechanism is a system or element that carries out part of the ML/TF process. Examples of ML/TF mechanisms include financial institutions, legal professionals, legal entities and legal arrangements.

Method: In the ML/TF context, a method is a discrete procedure or process used to carry out ML/TF activities. It may combine various techniques, mechanisms and instruments, and it may or may not represent a typology in and of its self.

Scheme: An ML/TF scheme is a specific operation or case of money laundering or terrorist financing that combines various methods (techniques, mechanisms and instruments) into a single structure.

Technique: An ML/TF technique is a particular action or practice for carrying out ML/TF activity. Examples of ML/TF techniques include structuring financial transactions, co-mingling of legal and illegal funds, over and under valuing merchandise, transmission of funds by wire transfer, etc.

Typology: An ML/TF typology is a pattern or series of similar types of money laundering or terrorist financing schemes or methods.

Legal professional: Lawyers, notaries and other independent legal professionals – this refers to sole practitioners, partners, or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.

Legal professionals are covered by the FATF Recommendations when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate
- managing of client money, securities or other assets
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation, or management of companies
- creation, operation or management of legal persons or arrangements, and the buying and selling of business entities.

SRB: Self-regulatory body – is a body that represents a profession (*e.g.* lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practicing in the profession.

ANNEX 4
TYPES OF LEGAL PROFESSIONALS

The Risk Based Approach Guidance for Legal Professionals, produced by FATF, in consultation with the legal sector in 2008, provided high level definitions of the legal professionals in terms of Lawyers and Notaries.[45]

In summary these definitions highlighted the regulated nature of these professions, their important role in promoting adherence to the rule of law, providing impartial and independent legal advice on complex rights and obligations, and/or authenticating documents.

For this typology research, greater focus was on the actual areas of law and specific tasks in which different types of legal professionals provided services, to obtain a clearer understanding of which vulnerabilities may be more relevant to which legal professionals.

The questionnaire sent to SRBs specifically asked for information on whether their members:

- engaged in activities covered by the FATF Recommendations;
- only provided legal and advice and representation;
- held exclusive licences for a particular legal services; and
- held client money

From the many responses received a number of trends were identifiable:

1. Lawyers

   Legal professionals who would fall within the RBA Guidance category of lawyer may actually be referred to in their home country as: Advocate, Advogardo, Attorney, Barrister, Lawyer, Legal Practitioner, Rechtsanwalt, Solicitor, Trial Attorney, etc.[46]

   Between countries however, the exact legal services provided by legal practitioners with the same title and restrictions on their activities also differed.

   In some countries legal professionals within this category were predominantly listed as providing legal advice and representing their clients, often in court, sometimes in negotiations. While in other countries they provided legal advice and assisted their

45 www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf

46 For example the European Directive to facilitate practice of the profession of a lawyer on a permanent basis in a member state other than that in which the qualification was obtained provides a useful overview of lawyers in the European union. See the CCBE website for more information www.ccbe.eu/index.php?id=94&id_comite=8&L=0

clients with the preparation of documents and carrying out of transactions, as well as representing those clients in court and negotiations.

In many countries legal professionals in this category held an exclusive licence for representation in court, but generally they did not hold an exclusive licence for legal services covered by the FATF Recommendations.[47]

In most countries all legal professionals in this category were able to receive clients directly[48] and were able to hold client money, either in specified accounts or accounts held by their professional body.

Both confidentiality and either legal professional privilege or professional secrecy reportedly applied to many or all of the activities of legal professionals within this category.

2. Notaries[49]

There is a distinction between civil law notaries and common law 'notaries public', with the latter certifying signatures and documents and the former having the status of a qualified legal professional and of public office holders in terms of establishing authentic instruments in the area of preventative justice.[50]

Civil law notaries often have an exclusive licence in relation to their role in the following areas:

1. the law relating to real property, such as the preparation and registering of contracts and/or deeds transferring real property from one party to another.

2. the law relating to legal persons, such as incorporating companies, issuing shares and registering their transfer.

3. the law relating to persons and families, such as the preparation of prenuptial agreements, property agreements following a divorce and drafting wills.

In some countries the notary is appointed to a specific geographical area and it would be atypical of them to undertake notarial work for transactions relating to other geographic areas.

---

47 There are exceptions to this, for example in Bermuda barristers have an exclusive licence in relation to legal work involving the transfer of real property and in Hungary attorneys are the only legal professionals able to undertake legal work relating to real property and the formation of companies

48 An exception to this was found in some common law countries, where a barrister will usually only act for a client who has been referred to them by a solicitor. The barrister is also precluded from holding client funds.

49 In Japan the category of notary is not known, although similar activities are undertaken by Judicial Scriveners and Certified Administrative Procedures Specialists.

50 In addition to the information about the role of civil and common law notaries in the FATF RBA guidance, the Council of Notariats of the European Union provide information on the role of notaries on their website: www.notaries-of-europe.eu/notary-s-role/overview

These legal professionals would occasionally hold client money or facilitate the transfer of a monetary instrument such as a cheque between parties, always in a traceable and recorded way. They would deal with the clients (or an authorised representative) directly, but sometimes on referral from another legal professional.

Confidentiality generally applied to these legal professionals. Some SRBS advised that legal professional privilege or professional secrecy also applied to these legal professionals, but others said that it would not.

ANNEX 5
SCHEDULE OF CASES

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
1	**Australia**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Financial Institution	Disciplinary sanction imposed	2, 23, 27
2	**Canada**	Misuse of Client Account	Transferring funds without providing legal services	Illicit Drug Trafficking	Financial Institution	No information	2, 3, 4, 36
3	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Corruption	Financial Institution	Disciplinary sanction imposed	36, 42
4	**Australia**	Misuse of Client Account	Structuring payments	Unspecified	Financial Institution, Real Estate	No information	2, 4, 5
5	**United States**	Misuse of Client Account	Structuring payments	Illicit Drug Trafficking	Financial Institution	Criminal conviction	2, 4, 18
6	**Spain**	Misuse of Client Account	Structuring payments	Fraud	Real Estate	STR filed by legal professional	2, 26
7	**United Kingdom**	Misuse of Client Account	Aborted transactions	Fraud	Company	Disciplinary sanction imposed	3, 34
8	**United Kingdom**	Misuse of Client Account	Aborted transactions	Unspecified	Real Estate	Removed from practice	2, 27, 34
9	**Belgium**	Property Purchases	Investment of proceeds of crime in property	Illicit trafficking in goods and merchandise	Real Estate	STR filed by legal professional	4, 26
10	**United Kingdom**	Property Purchases	Investment of proceeds of crime in property	Unspecified	Real Estate	Legal professional acted as prosecution witness	2, 4, 5

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
11	**United Kingdom**	Property Purchases	Investment of proceeds of crime in property	Illicit Drug Trafficking	Real Estate	Criminal conviction	4, 5
12	**France**	Property Purchases	Transferring value - back to back or ABC sales	Unspecified	Financial Institution, Real Estate	No information	2, 3, 4, 24, 33
13	**France**	Property Purchases	Transferring value - sales within an organised crime group	Organised Crime	Real Estate	No information	3, 4, 26
14	**Australia**	Property Purchases	Obscuring ownership - purchase with false name / counterfeit documents	Illicit Drug Trafficking	Real Estate	No information	2, 26
15	**Canada**	Property Purchases	Obscuring ownership - purchasing [purchase] through intermediaries	Illicit Drug Trafficking, Fraud or Theft	Financial Institution, Real Estate	No information	2, 4, 11
16	**France**	Property Purchases	Obscuring ownership - purchase through a company or trust	Corruption (?)	Company, Financial Institution, Real Estate	No information	2, 3, 4, 21, 26, 28, 35
17	**Belgium**	Property Purchases	Obscuring ownership - purchase through a company or trust	Organised Crime (?)	Company, Financial Institution, Real Estate	Investigation commenced	2, 6, 28, 29
18	**Spain**	Property Purchases	Obscuring ownership - purchase through a company or trust	Illicit Drug Trafficking	Company, Real Estate	STR filed by legal professional	2, 3, 4, 19,20
19	**United Kingdom**	Property Purchases	Mortgage fraud with antecedent laundering	Fraud	Financial Institution, Real Estate	Disciplinary sanction imposed	2, 26, 27
20	**United Kingdom**	Property Purchases	Mortgage fraud with antecedent laundering	Unspecified	Financial Institution, Real Estate	Removed from practice	26, 28, 33

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
21	**Belgium**	Creation of Companies and Trusts	Creation of trusts to obscure ownership and retain control	Tax Fraud (?)	Company, Financial Institution, Real Estate, Trust	No information	2, 29
22	**FATF**	Creation of Companies and Trusts, Misuse of Client Account	Creation of trusts to obscure ownership and retain control	Smuggling	Company, Financial Institution, Trust, Real Estate	No information	2, 3, 28
23	**Japan**	Creation of Companies and Trusts	Creation of shell companies to place or layer	Loan Sharking	Company	No information	1, 2, 26
24	**Spain**	Creation of Companies and Trusts	Creation of shell companies to place or layer, Management of a company or trust - creation of legitimacy and provision of legal services	Organised Crime	Company	No information	2, 3, 29
25	**Spain**	Creation of Companies and Trusts, Management of Companies and Trusts	Use of bearer shares to obscure ownership, Creation of shell companies to place or layer	Unspecified	Company, Financial Institution, Real Estate	No information	2, 11, 33
26	**Jersey**	Creation of Companies and Trusts	Use of bearer shares to obscure ownership	Illicit Drug Trafficking	Company, Financial Institution	No information	2, 4, 29
27	**United States**	Management of Companies and Trusts	Acting as trustee - receiving the proceeds of crime	Illicit Drug Trafficking	Trust	Decision not to prosecute legal practitioner	3, 36
28	**Italy**	Management of Companies and Trusts	Management of a company or trust - appearance of legitimacy and provision of legal services	Money laundering operation	Company, Financial Institution	No information	2, 19
29	**United States**	Management of Companies and Trusts	Management of a company or trust - appearance of legitimacy and provision of legal services	Advance-fee scheme	Company, Financial Institution	Criminal conviction	2, 42

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
30	**Italy**	Management of Companies and Trusts	Holding shares as an undisclosed nominee	Organised Crime (?)	Company, Financial Institution	No information	2, 19
31	**United States**	Management of Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Corruption	Company, Financial Institution	No information	2, 8, 27, 29
32	**United States**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Corruption	Company, Financial Institution Real Estate	No information	2, 8, 27
33	**Netherlands**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Unspecified	Company, Financial Institution	No information	2, 14, 26, 27
34	**Egmont**	Managing Client Affairs and Making Introductions	Introduction of other professionals for parts of a transaction	Organised Crime	Financial Institution, Real Estate	No information	2, 26
35	**United States**	Managing Client Affairs and Making Introductions	Introduction of other professionals for parts of a transaction	Illicit Drug Trafficking	Company, Financial Institution	Criminal conviction	2, 4, 26
36	**FATF**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of a client's general affairs	Illicit Drug Trafficking	Financial Institution, Real Estate	No information	2, 4
37	**Belgium**	Managing Client Affairs and Making Introductions	Management of a client's general affairs	Fraud	Financial Institution, Insurance	No information	8, 11, 26
38	**Norway**	Litigation	Sham litigation	Unspecified	Unspecified	Criminal conviction	2, 41
39	**Spain**	Litigation	Sham litigation	Organised Crime (?)	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 3, 20
40	**Australia**	Litigation	Sham litigation	Unspecified	Company	STR filed by legal professional	21, 22, 27, 38, 41

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
41	**Trinidad & Tobago**	Other Methods	Use of specialised legal skills	Illicit Drug Trafficking	Real Estate	Legal professional acquitted	2, 27, 39
42	**Spain**	Other Methods	Use of specialised legal skills	Unspecified	Unspecified	STR filed by legal professional	2, 3, 22, 37
43	**United Kingdom**	Other Methods	Use of specialised legal skills	Fraud	Unspecified	STR filed by legal professional	2, 4
44	**Belgium**	Other Methods	Use of specialised legal skills	Fraud	Company, Financial Institution	Investigation commenced	3, 4, 5
45	**United States**	Other Methods	Payment of legal fees and associated expenses	Illicit Drug Trafficking	Financial Institution / Money or value transfer service	Criminal conviction	2, 4
46	**United States**	Other Methods	Payment of legal fees and associated expenses	Illicit Drug Trafficking	Unspecified	Criminal conviction	2, 4
47	**Italy**	Other Methods	Payment of legal fees and associated expenses	Organised Crime	Unspecified	Legal professional charged	2, 4, 26
48	**Netherlands**	Other Methods	Providing legal services for charities	Terrorism	Company (Foundation)	Decision not to prosecute legal practitioner	2, 25
49	**United States**	Other Methods	Providing legal services for charities	Fraud	Company (Foundation)	Criminal conviction (for predicate offences)	2, 26
50	**Australia**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Company, Financial Institution	No information	7, 26, 28
51	**Australia**	Misuse of Client Account	Transferring funds without providing legal services	Fraud	Financial Institution	No information	4, 8, 36
52	**Belgium**	Misuse of Client Account	Transferring funds without providing legal services	Tax Evasion	Company, Financial Institution	No information	29, 36

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
53	**Belgium**	Misuse of Client Account	Transferring funds without providing legal services	Fraud	Company, Financial Institution	Investigation commenced	2, 29, 36
54	**Canada**	Misuse of Client Account	Transferring funds without providing legal services	Illicit Drug Trafficking	Financial Institution	No information	2, 4, 26, 36
55	**South Africa**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Company, Financial Institution	No information	3, 4, 36
56	**United Kingdom**	Misuse of Client Account	Transferring funds without providing legal services	Tax Fraud	Unspecified	Criminal conviction	3, 36
57	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Sale of Stolen Goods	Unspecified	Criminal conviction, new trial granted on appeal which is currently being appealed	3, 36
58	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Fraud	Company, Financial Institution	Criminal conviction	36
59	**United States**	Misuse of Client Account	Transferring funds without providing legal services	Unspecified	Company, Financial Institution	Criminal conviction	29, 36
60	**United States**	Misuse of Client Account	Structuring payments	Illicit Drug Trafficking	Company	Criminal conviction	3, 4, 26
61	**United States**	Misuse of Client Account	Structuring payments	Fraud	Financial Institution, Real Estate	Criminal conviction	4, 26
62	**United States**	Misuse of Client Account	Structuring payments	Illicit Drug Trafficking (Undercover Operation)	Real Estate (Undercover Operation)	Criminal conviction	2, 3, 26, 28
63	**United Kingdom**	Misuse of Client Account	Aborted transactions	Fraud (?)	Real Estate	Removed from practice	26, 34, 36
64	**FATF**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Company, Financial Institution, Real Estate, Trust	No information	4, 26, 28, 29

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
65	**Belgium**	Purchase of Real Property	Investment of proceeds of crime in property	Unspecified	Financial Institution, Real Estate	No information	4, 5
66	**Belgium**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 4
67	**Canada**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Real Estate	No information	4, 26
68	**Canada**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Financial Institution, Real Estate	No information	2, 4, 7, 26
69	**United Kingdom**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Financial Institution, Real Estate	Criminal conviction	2, 4
70	**United Kingdom**	Purchase of Real Property	Investment of proceeds of crime in property	Illicit Drug Trafficking	Financial Institution, Real Estate	Legal professional acted as prosecution witness	4
71	**United Kingdom**	Purchase of Real Property	Investment of proceeds of crime in property	Fraud	Real Estate	One legal professional removed from practice and two received disciplinary sanctions	2, 3, 26, 36
72	**France**	Purchase of Real Property	Obscuring ownership - purchasing through intermediaries	Illicit Drug Trafficking	Financial Institution, Real Estate	Criminal conviction	2, 4, 7
73	**United States**	Purchase of Real Property	Obscuring ownership - purchasing through intermediaries	Illicit Drug Trafficking	Real Estate	Criminal conviction	2, 4
74	**FATF**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Embezzlement	Company, Financial Institution, Real Estate	No information	28, 29

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
75	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Fraud	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 4, 29
76	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Fraud	Company, Financial Institution, Real Estate	Investigation commenced	2, 4, 28, 29
77	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Unspecified	Company, Financial Institution, Real Estate	Investigation commenced	28, 29
78	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Organised Crime	Company, Financial Institution, Real Estate	No information	4, 28, 29
79	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Organised crime	Company, Financial Institution, Real Estate	No information	17, 26, 37
80	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Fraud	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 5, 26
81	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 4, 26
82	**Belgium**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	No information	2, 3, 26, 36

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
83	**Spain**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Unspecified	Company, Financial Institution, Real Estate	No information	2, 8, 20, 26, 37
84	**Switzerland**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Corruption (?)	Company ["yet to be established"], Financial Institution, Real Estate	No information	2, 4, 26
85	**United Kingdom**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Unspecified	Real Estate	Decision not to prosecute legal practitioner	26
86	**United Kingdom**	Purchase of Real Property	Obscuring ownership - purchasing through a company or trust	Housing illegal immigrants	Company, Real Estate	Criminal conviction	29
87	**France**	Purchase of Real Property	Mortgage fraud with antecedent laundering	Fraud	Financial Institution, Real Estate	Prosecution commenced	3, 8, 26
88	**United Kingdom**	Purchase of Real Property	Mortgage fraud with antecedent laundering	Fraud, Organised Crime	Real Estate	Criminal conviction	2
89	**United Kingdom**	Purchase of Real Property	Mortgage fraud with antecedent laundering	Fraud	Real Estate	Disciplinary sanction imposed	2, 26, 35
90	**FATF**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution	Decision not to prosecute legal practitioner	2, 29, 36
91	**Belgium**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Tax Fraud (?)	Company, Financial Institution	Investigation commenced	17, 28, 29, 30
92	**Belgium**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Organised Crime	Company	Investigation commenced	29, 30

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
93	**Belgium**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Unspecified	Company	No information	26, 30
94	**Canada**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution	No information	2, 29, 30
95	**Canada**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution, Real Estate	No information	4, 24
96	**Canada**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company	No information	2, 30
97	**Spain**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Unspecified	Company	No information	3, 19, 27
98	**Spain**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Unspecified	Company	No information	18, 29, 30
99	**Netherlands**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Fraud	Company, Financial Institution	No information	2, 4, 26, 29
100	**Netherlands**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Fraud	Company	No information	24, 28
101	**United Kingdom**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Fraud, Tax Fraud	Company, Financial Institution	Criminal conviction	2, 4, 29, 36
102	**United Kingdom**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Corruption	Company, Financial Institution, Real Estate	STR filed by legal professional	2, 3, 8

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
103	**United Kingdom**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Corruption, Fraud	Company, Financial Institution, Real Estate	Criminal conviction (currently under appeal)	2, 3, 4, 8
104	**United States**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking	Company, Financial Institution	Prosecution commenced	2, 7, 29, 36
105	**United States**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Illicit Drug Trafficking (Undercover Operation)	Company, Financial Institution	Criminal conviction	27, 29, 36
106	**United States**	Creation of Companies and Trusts, Misuse of Client Account	Creation of shell companies to place or layer	Corruption	Company	Criminal conviction	2, 4, 26
107	**Austria**	Management of Companies and Trusts	Management of a company or trust - appearance of legitimacy and provision of legal services	Fraud, Breach of Trust	Company, Financial Institution	Criminal conviction	7, 26, 29
108	**Canada**	Management of Companies and Trusts	Management of a company or trust - creation of legitimacy and provision of legal services	Smuggling	Company, Financial Institution	No information	2, 4, 24, 30, 36
109	**Belgium**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Organised Crime	Financial Institution	No information	27
110	**Belgium**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Corruption	Company / Trust, Financial Institution	No information	2, 8, 27
111	**Belgium**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Fraud	Company, Financial Institution	No information	2, 27, 29
112	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Opening bank accounts on behalf of clients	Fraud	Company, Financial Institution	Criminal conviction	26, 29

Case.	Country / Source	Method	Technique	Source of Illicit Proceeds	Economic Sector(s)	Action by or against legal professional	Red Flags
113	**United States**	Managing Client Affairs and Making Introductions	Opening bank accounts on behalf of clients	Unspecified	Company, Financial Institution	Criminal conviction	7, 26, 27, 30
114	**Australia**	Managing Client Affairs and Making Introductions	Management of client's general affairs through client account	Unspecified	Financial Institution, Insurance	No information	5, 26, 36
115	**Belgium**	Managing Client Affairs and Making Introductions	Management of client's general affairs through client account	Illicit Drug Trafficking, Organised Crime	Company, Financial Institution	No information	5, 14, 21, 40
116	**Canada**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Illicit Drug Trafficking	Company, Financial Institution	No information	4, 24, 30, 36
117	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Fraud	Company, Financial Institution	Removed from practice	2, 26, 27, 36
118	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Illicit Drug Trafficking	Financial Institution	Criminal conviction	2, 4, 5, 36
119	**United States**	Managing Client Affairs and Making Introductions, Misuse of Client Account	Management of client's general affairs through client account	Illicit Drug Trafficking	Financial Institution	Criminal conviction	2, 4, 26, 36
120	**Netherlands**	Use of Specialised Legal Skills		Illicit Drug Trafficking	Financial Institution	Legal professional arrested	2, 7, 39
121	**Trinidad & Tobago**	Use of Specialised Legal Skills, Misuse of Client Account		Fraud	Company, Financial Institution	Prosecution commenced	7, 27, 30
122	**United Kingdom**	Use of Specialised Legal Skills		Fraud	(Art)	Criminal conviction	2, 4, 36
123	**United States**	Use of Specialised Legal Skills		Illicit Drug Trafficking	Company, Financial Institution	Criminal conviction	2, 4, 26, 27

ANNEX 6
ADDITIONAL CASE STUDIES

METHOD: MISUSE OF CLIENT ACCOUNT

TECHNIQUE: TRANSFERRING FUNDS WITHOUT PROVIDING LEGAL SERVICES

Case 50: **Legal professional acts as cash courier and makes international transfers without underlying legal transaction – common law country**

An Australian-based solicitor structured funds to an offshore account in Hong Kong. At times it was believed he actually carried cash to Hong Kong. His colleague, a Hong Kong-based solicitor, arranged for the creation of offshore companies in the British Virgin Islands and bank accounts in Hong Kong to receive structured funds from Australia. These funds were then transferred to other countries by the Hong Kong-based solicitor to hide from authorities or returned to Australia in order to appear legitimate.

Source: Australia (2012) questionnaire response

Case 50 **Red flag indicators:**	• Creation of complicated ownership structures without legitimate or economic reason • U-turn transactions • Use of multiple foreign accounts without good reason

Case 51: **Legal professional participates in u-turn payments to cover up fraud – common law country**

A person in control of a corporation's financial affairs abused this position of trust by defrauding the company. The person authorised and instructed staff to make electronic funds transfers from the company to his bookmakers' accounts. He then instructed the bookmakers to direct excess funds and winnings from their accounts to his account or third party accounts, and instructed bank officers to transfer funds from his accounts internationally.

In order to layer and disguise the fraud, he instructed his lawyer to contact the beneficiary of the original international transfers to return the payments via wire transfers into the lawyer's trust account. Approximately AUD 450 000 was returned in one international transfer to the lawyer's trust account. The lawyer then transferred AUD 350 000 to a church fund in an attempt to further hide the assets. To access these funds the person made structured withdrawals of AUD 9 000 each within a nine day period.

The suspect was charged with fraud-related offences for stealing more than AUD 22 million from the

company. He was sentenced to 14 years imprisonment, with a nine-and-a-half-year non-parole period.

Source: Australia (2012) questionnaire response

Case 51 **Red flag indicators:**	• Use of corporate funds for private expenditure • Use of the client account without an underlying transaction • Structuring of payments

Case 52: **Legal professional processes transfers between companies through client account without provision of legal services – civil law jurisdiction**

A bank disclosed suspicious international transfers to the Belgian FIU. Substantial sums from investment companies from Country A were credited on the third party account of a Belgian law firm to the benefit of the Belgian company X. The third party account was subsequently debited by means of money transfers to a company established in Country B. The total sum of these transactions amounted to several million euros.

The FIU's analysis revealed that the third party account clearly served as a transit account to make the construction less transparent. There was no justification to pass these funds through this third party account given that the Belgian company X already owned several accounts with Belgian banks. Furthermore, the majority of the managing directors of company X resided in Asia and were in no way connected to Belgium, whereas the shares of the company were owned by the investment company in Country A. Company X acted as a front company to cover up the relation between the origin and the destination of the funds.

Tax intelligence obtained by the FIU showed that, because of the intervention of company X, the investment companies from Country A (the clients of the international transfers) could relieve the tax burden for important investments in Country B.

Source: Belgium (2012) questionnaire response

Case 52 **Red flag indicators:**	• Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason • Use of the client account without an underlying transaction

Case 53: **Legal professional transfers the proceeds of a fraud through client account and attempts to purchase foreign currency to further disguise the origin of the funds – civil law country**

An exchange office disclosed the purchase of a considerable amount of GBP by a foreigner for the account of company X established in Belgium. The funds for this purchase had been transferred to the exchange office's account at the request of a lawyer with a Belgian bank account. The Unit questioned the bank where the lawyer/client held his account. This revealed that the funds on the account of the exchange office had been transferred to the lawyer's account in order of company Y established abroad. The funds that had been transferred by company Y were used to issue a cheque

to the order of company X.

The Unit was informed by the bank that the transfer order was false. Based on this information the bank countermanded the cheque issued by the lawyer, and further investigation by the Unit showed that company X was managed by a foreign national who had performed the exchange transaction. This transaction for company X's account did not have any known economic justification. Information by the tax administration indicated the company had not made its tax returns for quite some time.

Police intelligence revealed that company X, its managing director and its lawyer were on record for fraud. Part of the proceeds of this fraud was used to finance the purchase of GBP by a foreign national on behalf of company X. The Unit reported this file for financial fraud related money laundering.

Source: Belgium (2012) questionnaire response

Case 53 **Red flag indicators:**	• Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason • Use of the client account with no underlying transaction • Use of false documents • The client is known to have convictions for acquisitive crime

Case 54: **Legal professional accepts transfers into client account and acts as cash courier – common law country**

An Ontario-based drug trafficker admitted to police that he purposely used legal trust accounts to help block access to information about the true ownership of the funds in the account. He confessed that he would provide cash to his lawyer, who would then deposit the funds into the law firm's trust account. Every few days, the lawyer would withdraw the money from the trust account and deposit the funds into the various bank accounts controlled by the drug trafficker. This was often done by issuing cheques against the trust account, which would be payable to a company associated with the trafficker. Most cheques were in the amount of CAD 2 000 to avoid suspicion.

The small deposits and withdrawals, combined with the use of cheques issued from his lawyer's trust account, helped to circumvent cash or suspicious transaction declarations at financial institutions.

Source: Schneider, S. (2004)

Case 54 **Red flag indicators:**	• Cash payments not consistent with the client's known legitimate income • Use of the client account with no underlying transaction • Structuring of payments • The client is known to have convictions for acquisitive crime or to be currently under investigation for acquisitive crime

Case 55: **Legal professional uses client account as a banking facility for clients and applies their funds to his personal credit card – common law country**

The South African FIU received several STRs about an attorney who appeared to be abusing his attorney trust facility. The suspicious transactions in the reports pointed out the following:

i) Multiple large sums of money were being deposited into the trust account by different people and companies over a period exceeding two years

ii) These funds were used to make payments to other depositors in South Africa and abroad

iii) Funds from this account were being remitted to foreign countries deemed to be tax havens

iv) Money was transferred to the attorney's personal credit card; his practice expenses were also paid directly from the trust account.

Source: Deloitte (2011)

Case 55 **Red flag indicators:**	• Use of the client account without an underlying transaction • Payment of funds to a high risk country • Possibly disproportionate private funding and/or payments from third parties

Case 56: **Legal professional convicted after transferring funds to a criminal client's mistress – common law country**

In 2008, Mr Krestin, a solicitor was convicted of entering into an arrangement to facilitate money laundering after making a payment of EUR 14 000 euro to his client's mistress. There was no underlying transaction supporting the payment. The solicitor had received a production order relating to the client which outlined allegations of Tax (MTIC) fraud against the client. The first jury had not been able to reach a verdict, and the judge concluded that the second jury must have convicted the solicitor on the basis that he suspected that the funds were the proceeds of crime, rather than that he knew they were. The solicitor was fined GBP 5 000. When his conduct was considered by the Solicitors Disciplinary Tribunal, in light of the sentencing judge's comments he was reprimanded, but allowed to keep practicing as a lawyer, subject to restrictions.

Source: United Kingdom (2012) questionnaire response

Case 56 **Red flag indicators:**	• No underlying transaction for use of the client account • The is known to be currently under investigation of acquisitive crime

Case 57: **Legal professional disperses funds to criminal client's family members and keeps fee – common law country**

Attorney Jamie Harmon accepted the proceeds of the sale of stolen goods from her client, Christian Pantages. Harmon deposited the funds into her attorney trust account and then dispersed the funds

to Pantages and his wife, keeping a fee for herself.

Pantages pleaded guilty to all counts against him and testified against Harmon at trial. Following a guilty verdict on five counts of money laundering, the district court granted Harmon a new trial based on an improper jury instruction. In so doing, the judge expressed concern regarding the difficulties defence counsel face when accepting fees from clients that may be criminal proceeds.

See 2011 WL 7937876, at *5 n.12 (N.D. Cal. Aug. 18, 2011) (denying motion for judgment of acquittal but granting motion for a new trial based on improper jury instruction). The government's appeal of the grant of a new trial is pending.

Source: United States (2012) questionnaire response – United States v Harmon, No. 08-cr-938 (ND Cal)

Case 57 **Red flag indicators:**	• Use of client account without an underlying transaction

Case 58: **Legal professional convicted for creating secret client accounts to transfer the proceeds of fraud – common law country**

Attorney Jonathan Bristol pleaded guilty to conspiracy to commit money laundering for his role in laundering more than $18m in fraud proceeds through two attorney escrow accounts on behalf of Kenneth Starr and his fraudulent investment enterprises. At the time, Bristol was an attorney at a large, international law firm in New York.

Bristol created two attorney escrow accounts, without informing his law firm, into which Starr's investment advisory clients deposited their investment funds. Bristol then transferred the funds to Starr, members of his family, and his entities. Bristol also used the clandestine attorney escrow accounts to pay his law firm on behalf of Starr.

Bristol is currently awaiting sentencing. Following disciplinary action, the Court accepted his resignation for reasons of judicial economy and ordered Bristol's name be immediately struck from the roll of attorneys.

Source: United States (2012) questionnaire response United States v. Bristol, No. 10-cr-1239 (S.D.N.Y.)

Case 58 **Red flag indicators:**	• Use of client account without an underlying transaction • Payment of funds intended for corporate purposes to private accounts • Payments to third parties with no legitimate explanation

Case 59: **Legal professional creates complicated foreign structures and transfers funds through client account while claiming privilege would prevent discovery – common law country**

Attorney David Foster was indicted on charges of money laundering and ultimately pleaded guilty to one count of causing a financial institution to fail to file a currency transaction report. Foster assured undercover agents that their money laundering transactions through his client trust account would be protected by attorney-client privilege. After the funds were deposited in the trust

account, he transferred the money to a corporation and bank accounts in Liechtenstein that he had established. See 868 F. Supp. 213 (E.D. Mich. 1994) (holding that Foster's sentence calculation should be increased because of an enhancement for use of "special skills").

Source: United States (2012) questionnaire response United States v Foster No 93-cr-80141 (Ed Mich)

Case 59 **Red flag indicators:**	• Use of client account without an underlying transaction • Involvement of structures and countries where there is no legitimate reason

TECHNIQUE: STRUCTURING PAYMENTS

Case 60: **Legal professional creates companies, false legal documentation and advises on structuring payments to avoid reporting requirements – common law country**

Attorney George Rorrer was convicted by a jury of conspiracy to commit money laundering. Rorrer helped to invest the drug proceeds of client John Caporale by forming a corporation in the name of the client's wife and arranging a loan from the corporation to another (non-criminal) client, Robin Hawkins. Rorrer then drafted a phony construction-work contract, making the repayment of the loan appear to be payment for construction work performed by the Caporales. Rorrer instructed Hawkins to give the construction receipts to the Caporales to legitimise the payment.

Rorrer also drew up a promissory note, which the wife signed, but did not provide copies of the note to either party. Rorrer advised Hawkins how to deposit the cash loan without triggering reporting requirements. The appeals court upheld Rorrer's conviction but remanded him for resentencing after finding that the district court abused its discretion by not applying a sentencing enhancement based on Rorrer's use of "special skills" (legal skills) in committing the offenses of conviction. See United States v. Robertson, 67 F. App'x 257 (6th Cir. 2003).

Source: United States (2012) questionnaire response United States v. Rorrer, No. 99-cr-139(7) (W.D. Ky.)

Case 60 **Red flag indicators:**	• Significant private funding and the transfers are structured so as to avoid the threshold requirements • The ties between the parties are of a family, employment, corporate or other nature such as to generate doubts as to the real nature or reason for the transaction • Structuring of payments

Case 61: **Legal professional structures payments for property to avoid threshold reporting requirements – common law country**

Attorney Michael Sinko was convicted of conspiracy to commit money laundering and aiding and abetting money laundering. Sinko owned a condominium project that was financed by NOVA Bank, of which Sinko was the outside counsel. John Palmer, who had fraudulently obtained funds from his employer, wished to launder money by buying a condominium from Sinko. Sinko structured the purchase agreement in a way that avoided disclosure of cash payments. See 394 F. App'x 843 (3d

Cir. 2010) (affirming sentence).

Source: United States (2012) questionnaire response United States v. Sinko, No. 07-cr-703 (E.D. Pa.)

Case 61 **Red flag indicators:**	• Structuring of payments • Significant private funding / cash payments disproportionate to known legitimate income

Case 62: **Legal professional structures payments on property purchase and creates false documentation to launder proceeds of crime – common law country**

Defence attorney Victor Arditti advised an undercover agent posing as a cocaine dealer on how to structure cash in order to purchase real estate. Later, Arditti told the agent he would draft documents memorialising a sham loan to legitimise cash drug proceeds and then establish an escrow account to receive the proceeds and then invest it in an Oklahoma oil deal. When the escrow account idea failed to work, Arditti set up a trust account to funnel the drug proceeds to the oil deal, keeping the undercover agent's alias off all bank records.

No trust agreement was prepared, and Arditti had sole signature authority on the account. Subsequent deposits were made to the trust account using cashier's cheques from a Mexican money exchanger. A grand jury indicted Arditti on charges of conspiracy to launder money and to avoid currency reporting requirements. A jury found Arditti guilty on all counts, and the district court denied judgment of acquittal.

Source: United States (2012) questionnaire response United States v. Arditti, 955 F.2d 331 (5th Cir.), cert. denied, 506 U.S. 998 (1992)

Case 62 **Red flag indicators:**	• Structuring of payments • Client with purported convictions for acquisitive crime • Use of complicated structures for no legitimate reasons • Funds received from high risk countries

TECHNIQUE: ABORTED TRANSACTIONS

Case 63: **Legal professional facilitates laundering of the proceeds of mortgage fraud following aborted property transactions – common law country**

In 2010 a solicitor was stuck off after having allowed a large property company to use the client account as a banking facility, when the transactions were suddenly aborted They had also dissipated the funds received from a number of properties, rather than paying out the mortgage on the property.

Source: United Kingdom (2012) questionnaire response

Case 63 **Red flag indicators:**	• Large payments to the client account without an underlying legal transaction • Transaction unexpectedly aborted after funds had been received

	• Transaction were large for the particular practice

METHOD: PURCHASE OF REAL PROPERTY

TECHNIQUE: INVESTMENT OF PROCEEDS OF CRIME IN PROPERTY

Case 64: **Legal professional creates complex structures to purchase property with drug proceeds - common law country**

Suspicious flows of more than USD 2 million were identified being sent in small amounts by different individuals who ordered wire transfers and bank drafts on behalf of a drug trafficking syndicate who were importing 24kg of heroin into Country Z. Bank drafts purchased from different financial institutions in country Y (the drug source country) were then used to purchase real estate in Country Z. A firm of solicitors was also used by the syndicate to purchase the property using the bank drafts that had been purchased overseas after they had first been processed through the solicitor's trust account. Family trusts and companies were also set up by the solicitors.

Source: FATF (2004)

Case 64 **Red flag indicators:**	• Possible structuring of payments • Significant funding disproportionate to the known legitimate income of the client • Involvement of structures and accounts in multiple countries with no legitimate reasons • Use of complicated ownership structures for no legitimate reason

Case 65: **Legal professional instructed in property purchase by a foreign national with multiple third parties contributing to funding – civil law country**

A bank's suspicions were raised after a bank cheque was issued to the order of a notary upon request of an Asian national for purchasing real estate. Analysis of the account transactions showed that the account received several transfers from Asians residing abroad and was known through an investigation regarding a network of Asian immigrants. The analysis showed that the account had been used as a transit account by other Asian nationals for the purchase of real estate.

Source: FATF (2007)

Case 65 **Red flag indicators:**	• Third party funding with no legitimate explanation • Significant levels of private funding which may have been disproportionate to the socio-economic profile of the client

Case 66: **Legal professional makes STR after client attempts to purchase property with cash – civil law country**

A notary did a notification to the FIU on a company, represented by the Managing Director, who had

purchased a property in Belgium. The notary got suspicious when the buyer wished to pay the total price in cash. When the notary refused the Managing Director asked where the nearest bank Agency was. He came back to the Office of the notary with a cheque from the bank after he had run a deposit in cash. The suspicions of the notary were further enhanced when the company which he represented was the subject of a criminal investigation. Research by the FIU revealed that the person was already the subject of a dossier that was been sent by the FIU in connection with illicit drug trafficking. After the notification from the FIU a law enforcement investigation commenced.

Source: Cellule de traitement des information Financieres (2006)

Case 66 **Red flag indicators:**	• Significant amounts of cash not consistent with known legitimate income • The client is currently under investigation for acquisitive crimes

Case 67: **Legal professional acts as a depository institution and then purchases property for client with no known legitimate income – common law country**

A BC man used the proceeds from the sale of cocaine, marijuana and steroids to purchase several homes throughout British Columbia. The trafficker would regularly provide cash to his lawyer who would deposit the funds into his law firm's bank account in amounts averaging CAD 4 000 to CAD 5 000. When the balance of the amount reached a certain level the funds would be applied to the purchase of property (mostly homes used as marijuana grow-ups).

Source: Schneider, S. (2004)

Case 67 **Red flag indicators:**	• Significant private funding and cash not consistent with known legitimate income • Structuring of payments • Transactions not consistent with legitimate socio-economic profile of the client

Case 68: **Legal professional accepts over 130 transactions in 8 months to purchase property for drug trafficker – common law country**

Between January and August 1994, more than 130 transactions were conducted through a trust account of a law firm that represented a drug trafficker in the purchase of a $650,000 home in Toronto. The accused was convicted of drug trafficking and police were also able to prove that the funds used to purchase the property were derived from his illegal activities. During a two week period preceding his purchase of the real estate, the accused provided the law firm with numerous bank drafts obtained from a number of different financial institutions. The vast majority of these bank drafts were between CAD 3 000 and CAD 5 000 in value. The highest amount was CAD 9 000. Between March 17 and March 25, 1994, 76 bank drafts were deposited on behalf of the accused in the law firm's trust account. On March 17 alone, 18 different bank drafts were deposited into the account. The bank drafts were purchased from eight different deposit institutions.

Source: Schneider, S. (2004)

Case 68 **Red flag indicators:**	• Client known to have convictions for acquisitive crime • Structuring of payments • Significant private funding not consistent with known legitimate income • Use of multiple bank accounts and financial institutions for no legitimate reason

Case 69: **Legal professionals co-opted into laundering activity by his brother – common law country**

In 2009, Mr Farid a solicitor was convicted of failing to make a suspicious transaction report after acting in a number of property transactions on behalf of a drug dealer. Mr Farid was introduced to the client by the Mr Farid's brother and a mortgage broker. The mortgage broker had assisted in identity theft to facilitate fraudulent mortgage applications, with the transactions being processed by the solicitor, after large cash deposits were made. Mr Farid was sentenced to 9 months jail and in 2011 the Solicitors Disciplinary Tribunal ordered that he should not be re-employed within a law firm without permission from the regulator.

Source: United Kingdom (2012) questionnaire response

Case 69 **Red flag indicators:**	• Disproportionate amounts of cash • Use of false identities

Case 70: **Legal professional acts as prosecution witness after wrongly assuming funds were clean because they have come from a bank account – common law country**

In 2008/09 an international drug trafficker laundered over GBP 300 000 through bank accounts. This was then paid from the bank via cheque to a solicitor who acted as legal professional in a house purchase, where the house was bought for approximately GBP 450 000 with no mortgage. The solicitor had assumed because the money was transferred from a bank account, the funds had already been checked. The solicitor was not charged and acted as a witness for the police.

Source: United Kingdom (2012) questionnaire response

Case 70 **Red flag indicators:**	• Disproportionate level of private funding not consistent with the known legitimate income

Case 71: **Three legal professionals engage in money laundering through a property transaction for convicted fraudster husband of senior partner – common law jurisdiction**

In March 2006, a law firm acted for a small company in the purchase of a property for GBP 123 000. The director of the company was Mr A, the husband of one of the solicitors and a convicted fraudster. In September 2006, the law firm acted for Mr A who purchased the same property from the company for GBP 195 000. In February 2007, the firm then acted for Mr A's step son who

purchased the same property for GBP 230 000. In December 2006, the small company provided the firm with a payment of GBP 25 000 and GBP 20 000. The amount of GBP 25 000 was noted as covering a shortfall for the property, but there was no shortfall. The amount of £20,000 was said to be a loan to another client, but there were not documents to support the loan. The Solicitors Disciplinary Tribunal considered the conduct of three solicitors in relation to the matter. One was struck off, one was given an indefinite suspension from practice and the other was fined GBP 10 000.

Source: United Kingdom (2012) questionnaire response

Case 71 **Red flag indicators:**	• Director of client was known to have criminal convictions • Rapidly increasing value on the property that was not consistent with the market • Connection between the parties giving rise to questions about the underlying nature of the transaction • Use of client account without underlying transaction

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASING THROUGH INTERMEDIARIES

Case 72: **Legal professional turns a blind eye to false documents when helping partner of drug trafficker buy property with criminal proceeds – civil law country**

In 1995 a notary was found guilty of money laundering as he helped the sexual partner of a drug trafficker, who had been arrested to buy a property and advise her to pay the price with international wire transfers. The court decided that the notary could not have been ignorant of the fact that some documents had been falsified.

Source: Chevrier, E. (2005)

Case 72 **Red flag indicators:**	• Use of false documents • Client known to have close connections with a person under investigation for acquisitive crimes • Use of foreign accounts with no legitimate reason • Significant private funding possibly not consistent with known legitimate income

Case 73: **Legal professional convicted for creating property portfolio for drug trafficking friend – common law country**

Attorney James Nesser was convicted of conspiracy to distribute drugs, conspiracy to launder money, money laundering, and engaging in illegal monetary transactions. Nesser handled property transactions for a client and sometimes social acquaintance Ronald Whethers. Nesser laundered Whethers' drug proceeds through the purchase of a farm, the sham sale of a house, and the masked purchase of another real property. Nesser's conviction on drug conspiracy charges was upheld because the laundering promoted the drug conspiracy and prevented its discovery by concealing the

origin of the proceeds. See 939 F. Supp. 417 (W.D. Penn. 1996) (affirming conviction).

Source: United States (2012) questionnaire response - United States v. Nesser, No. 95-cr-36 (W.D. Penn.)

Case 73 **Red flag indicators:**	• Client known to be involved in criminal activity • There are attempts to disguise the real owner or parties to a transaction • Significant private funding not consistent with known legitimate income

TECHNIQUE: OBSCURING OWNERSHIP – PURCHASE THROUGH A COMPANY OR TRUST

Case 74: **Legal professional assists in creating property investment countries to hide millions derived from fraud**

A director of several industrial companies embezzled several million dollars using the bank accounts of offshore companies. Part of the embezzled funds were then invested in Country Y by means of non-trading real estate investment companies managed by associates of the person who committed the principal offence. The investigations conducted in Country Y, following a report from the FIU established that the creation and implementation of this money laundering channel had been facilitated by accounting and legal professionals – gatekeepers. The gatekeepers had helped organise a number of loans and helped set up the different legal arrangements made, in particular by creating the non-trading real estate investment companies used to purchase the real estate. The professionals also took part in managing the structures set up in Country Y.

Source: FATF (2004)

Case 74 **Red flag indicators:**	• Creation of complicated ownership structures with no legitimate reason • Involvement of structures with multiple countries with no legitimate reason

Case 75: **Legal professionals help obscure beneficial ownership through complicated international corporate structures – civil law country**

A notary disclosed a real estate purchase by the company RICH, established in an off-shore centre. For this purchase the company was represented by a Belgian lawyer. The payment for the property took place in two stages. Prior to drafting the deed a substantial advance was paid in cash. The balance was paid by means of an international transfer on the notary‘s account.

Analysis revealed the following.

The balance was paid on the notary‘s account with an international transfer from an account opened in name of a lawyer‘s office established in Asia. The principal of this transfer was not the company RICH but a Mr. Wall. Ms. Wall, ex-wife of Mr.Wall resided at the address of the property in question. Police sources revealed that Mr. Wall was known for fraud abroad.

These elements seemed to indicate that Mr. Wall wanted to remain in the background of the

transaction. That is why he used an off-shore company, represented by a lawyer in Belgium and channelled the money through a lawyer's office abroad to launder money from fraud by investing in real estate.

Source: Deloitte (2011)

Case 75 **Red flag indicators:**	• Use of multiple countries, including higher risk countries, without legitimate reason • There are attempts to disguise the real owner or parties to the transaction • Significant amounts of cash and private funding possibly not consistent with the known legitimate income of the client

Case 76: **Legal professional involved in unusual transfers of property without apparent economic or other legitimate justification – civil law country**

A bank reported a person whose account has remained inactive for a long time, but who suddenly was filled with several deposits in cash and international transfers. These funds were then used for the issuance of a cheque to order of a notary for the purchase of a property. Research by the FIU revealed that the ultimate purchaser of the property not was the person involved, but an offshore company. The person concerned had first bought the property in his own name and then left to the listed company by a command statement for the notary. Examination of the dossier revealed that the person who was connected to a bankrupt company, acted as hand to buy property with disadvantage of his creditors. The person concerned also practiced no known professional activity and received state benefits. On these grounds and police intelligence the FIU reported the dossier for money laundering in connection with fraudulent bankruptcy. A judicial inquiry is currently underway.

Source: Cellule de traitement des information Financieres (2006)

Case 76 **Red flag indicators:**	• Involvement of a complicated ownership structure without legitimate reason • Funding not consistent with known legitimate income • There are attempts to disguise the real owner or parties to the transaction • Involvement of foreign countries with no legitimate reason

Case 77: **Legal professional involved in creating complex foreign corporate structure to purchase properties to facilitate laundering – civil law country**

The bank account of a person was credited by substantial transfers from abroad. These funds were used as banking cheques to order of a notary to purchase real estate. The investigation of the FIU revealed that the person had set up a highly complex corporate structure for this investment. Interrogation of the notary and the Constitutive Act of the companies showed that the two holdings companies in Belgium were founded at this notary in Belgium by four foreign companies. Then

those two companies founded two other companies in the real estate sector. Then the intermediary of these two last companies made investments in real estate. This dossier is currently subject of a judicial inquiry.

Source: Cellule de traitement des information Financieres (2006)

Case 77 **Red flag indicators:**	• Use of a complicated ownership structure without legitimate reason • Involvement of multiple countries without legitimate reason

Case 78: **Legal professionals makes STR after unusually high money transfers received from foreign country with no connection to the parties or the transaction – civil law country**

A Russian couple, living in Belgium, controlled the company OIL that was located in Singapore and that was active in the oil and gas sector. A company in the British Virgin Islands was the only shareholder of OIL. On their accounts significant transfers were made regarding OIL. The money was then transferred to accounts on their name in Singapore or withdrawn in cash. The use of foreign accounts and the intervention of off shore companies attracted the attention of the banks. In addition, the couple invested several million euros in immovable property in Belgium. The notary found such substantial investments and that they were paid through transfers from Singapore suspicious. Police source revealed that these stakeholders were heads of a Russian crime syndicate. They practiced no commercial activities in Belgium that could justify the transactions on their accounts. The Belgian financial system was apparently only used for the purpose of money laundering.

Source: Cellule de traitement des information Financieres (2009)

Case 78 **Red flag indicators:**	• Involvement of multiple countries without legitimate reason, including high risk countries • Significant private funding not consistent with the company's economic profile • Complicated ownership structure without legitimate reason

Case 79: **Legal professional used in U-turn property transaction designed to legitimise funds from organised crime – civil law country**

An East European was acting under an alias as the director of a company for which he opened an account with a Belgian bank. Transfers were made to this account from abroad, including some on the instructions of "one of our clients".

The funds were then used to issue a cheque to a notary for the purchase of a property. The attention of the notary was drawn to the fact that some time after the purchase, the company went into voluntary liquidation, and the person concerned bought the property back from his company for an amount considerably above the original price. In this way the individual was able to insert money into the financial system for an amount corresponding to the initial sale price plus the capital gain. He was thus able to use a business account, front company customer, purchase of real estate, cross border transaction and wire transfers to launder money that, according to police sources, came

from activities related to organised crime.

It appeared that the company acted as a front set up merely for the purpose of carrying out the property transaction.

Source: FATF (2007)

Case 79 **Red flag indicators:**	• Sale of property in a non-arm's length transaction (i.e. a director selling to his company) • Resale back to the original seller at a reduced price • There has been an increase in capital from a foreign country, where there is no clear connection

Case 80: **Legal professional makes STR after unusual third party funding of a property purchase**

The FIU received a suspicious transaction report from notary A on one of his clients, person B, a foreigner without an address in Belgium, who in his office had set up a company for letting real estate. The sole manager and shareholder of this company was a family member of B, who also resided abroad. Shortly after its creation the company bought a property in Belgium. The formal property transfer was carried out at notary A's office. The property was paid for through the account of notary A by means of several transfers, not from company X, but from another foreign company about which individual B did not provide any details. The establishment of a company managed by a family member with the aim of offering real estate for let and paid by a foreign company disguised the link between the origin and the destination of the money. Police intelligence revealed that the individual was known for financial fraud. The investment in the property was apparently financed by the fraud.

Source: FATF (2007)

Case 80 **Red flag indicators:**	• Funds received from third parties, in a foreign country, with no legitimate reason • The client is evasive about the source of funds • The transaction is unusual – there is limited connection between the client and the country in which the transaction takes place and the client does not have ownership or formal control over the entity on whose behalf he is conducting the transaction. • The client has convictions for acquisitive crimes

Case 81: **Legal professional makes STR after unusual cash payments made in relation to a property purchase – civil law country**

The company ANDI, managed by Mr. Oxo, sold a property to the company BARA, managed by Mr. Rya, for a significant amount for which the deposit was paid in cash. A large part of the price was also paid in cash. When the notary who had executed the act noticed these transactions he sent a disclosure to the FIU based on article 10bis of the Law of 11 January 1993.

Analysis revealed the following elements:

• The notary deed showed that money for the cheque to the notary was put on the account of the company ANDI by a cash deposit two days before the cheque was issued.

• Information from the bank showed that the company ANDI and Mr. Oxo's personal account were credited by substantial cash deposits. This money was used for, among other things, reimbursing a mortgage loan, and was withdrawn in cash.

• Police sources revealed that Mr. Oxo and Mr. Rya were the subject of a judicial inquiry into money laundering with regard to trafficking in narcotics. They were suspected of having invested their money for purchasing several properties in Belgium through their companies.

All of these elements showed that the cash used for purchasing property probably originated from trafficking in narcotics for which they were on record.

Source: Deloitte (2011)

Case 81 **Red flag indicators:**	• Significant cash deposits • Sale of property in a non-arm's length transaction • Clients currently under investigation for acquisitive crimes

Case 82: **Legal professional receives multiple deposits from various sources for property transaction – civil law jurisdiction**

A company purchased property by using a notary's client account. Apart from a considerable number of cheques that were regularly cashed or issued, which were at first sight linked to the notary's professional activities, there were also various transfers from the company to his account. By using the company and the notary's client account, money was laundered by investing in real estate in Belgium, and the links between the individual and the company were concealed in order to avoid suspicions. Police sources revealed that the sole shareholder of this company was a known drug trafficker.

Source: FATF (2007)

Case 82 **Red flag indicators:**	• The funding appears unusual in terms of multiple deposits being made towards the property purchase over a period • Use of the client account without an underlying transaction • The company only has one shareholder • A beneficial owner has convictions for acquisitive crime

Case 83: **Legal professional assists PEPs to purchase expensive foreign property though a company with a later transfer to a family member without genuine payment – civil law country**

A company is incorporated with a capital stock of EUR 3 050 by a Spanish lawyer, who then creates a general power of attorney over the company for a relative of the Head of State of an African country. Half the stock in the company is then transferred to another national of the same African country, who claims to be a businessman.

The company purchases of a plot of land within an urban development in Spain on which a detached house has been built. The property is valued at EUR 5 700 000, the price being paid through transfers between accounts at the same Spanish credit institution.

The company transfers the recently purchased property, in the following deed, to the relative of the Head of State, specifying the same price as set for the first purchase, while deferring payment of the entire sum.

Source: Spain (2012) questionnaire response

Case 83 **Red flag indicators:**	• The client and beneficial owner have family and personal ties to an individual who holds a public position in a high risk country. • The company makes a significant purchase which is disproportionate to the initial capital in the company and its economic profile • Company funds are used to make a private purchase • The transaction does not make economic sense in that the company divests itself of its largest asset without making a profit and with payment being deferred, • The transfer of the property is a non-arm's length transaction (i.e. company sells to its director)

Case 84: **Legal professional accepts tens of millions of euros from a PEP as a gift to his children to purchase property despite warnings of the corruption risks – civil law country**

Following the payment of a sum of money to the account of a notary's office, a bank sent a STR to the FIU. The STR referred to the payment of several tens of millions credited to the account of the notary. As the transaction appeared unusual, in particular because of the amount, the financial intermediary requested its client to clarify matters. The notary explained that the payment was a gift from a high-ranking government official or president of a country on the African continent to his children residing in Switzerland. The funds were destined for the purchase, via the intermediary of a public limited company yet to be established, of an apartment in the town in question.

As the funds originated from a politically exposed person (PEP), the degree of corruption in the African country in question was assessed as high and the Swiss Federal Banking Commission (SFBC) had issued warnings regarding this country, the financial intermediary reported the case.

Following investigations carried out by the FIU, it became apparent that the extremely high price of the property in question was in no proportion to the normal price for this type of object. Furthermore, open sources revealed that a third country was already carrying out investigations

into corruption and money laundering by the government official in question and members of his family.

Source: Deloitte (2011)

Case 84 **Red flag indicators:**	• Disproportionate private funding given known legitimate income • There are attempts to disguise the real owner or parties to the transaction • The client holds a public position in a high risk country • There is a remarkable high and significant difference between the purchase price and the known value of properties in the area • The client is currently under investigation for acquisitive crimes

Case 85: **Legal professional unaware that funds used to purchase property through a trust were proceeds of crime – common law country**

Between 2004 and 2008 a legal professional who conducted property transactions, assisted the subject by drafting a Deed of Trust and the purchase of a property. The property was bought at a discounted rate by the client and then transferred to third party. No action was taken against the legal professional as the law enforcement agency was unable to prove that legal professional had known or suspected that they were dealing with the proceeds of crime.

Source: United Kingdom (2012) questionnaire response

Case 85 **Red flag indicators:**	• Unusual transaction involving transfer of property at significant undervalue. • Complex property transactions

Case 86: **Legal professional convicted after transferring hotels at undervalue to offshore company – common law country**

In 2010, Mr Wilcock, a solicitor was convicted of failing to make a suspicious transaction report and fined GBP 2 515. He was acting for a client who ran a chain of properties in Southport, England which housed illegal immigrants. He was asked to transfer the ownership of the hotels to an offshore company at a significant undervalue. It was not clear if Mr Wilcock knew his client was being investigated by police at the time of the transaction, but in pleading guilty he acknowledged that he should have been suspicious as to the source of the funds used to purchase the hotels in the first place.

Source: United Kingdom (2012) questionnaire response

Case 86 **Red flag indicators:**	• Significant undervalue • Involvement of complex ownership in a country with which there was limited connection

TECHNIQUE: MORTGAGE FRAUD WITH ANTECEDENT LAUNDERING

Case 87: **Legal professional investigated for acting in unusual property transactions - including selling maid's rooms for 8 times their original value – civil law country**

Judicial investigations are in progress into the facts surrounding credit frauds to the detriment of a bank: 6 fraudulent real estate files of financing were presented to the agency on the basis of the production of false pay slips and false bank statements, for a loss at first estimated esteemed at EUR 505 000.

The first investigations led by the police confirmed that the loan files were presented to the bank systematically by the same client adviser and systematically by the same real estate agent for six different borrowers. They confirmed also that the loss finally amounted to about EUR 5 million as more loans which had deceitfully been obtained by those 6 borrowers were uncovered.

Searches of the offenders' residences led to the discovery of numerous documents, and a lifestyle out of proportion to their legitimate income.

However, the destination of the lent funds could only be partially determined because 5 of the 6 involved borrowers had acquired real property in Luxembourg.

The investigation also identified the complicity of two agents of the defrauded bank and the assistant director of this bank who indicated they let pass at least 9 files which they knew were based on false documents and that the borrowers were involved in the fraud.

The lent funds stemming from frauds allowed the purchase of properties in France and in Luxembourg. All of the purchases involved a single solicitor and his clerk, who were complicit of the organised fraud.

Searches of the office of the notary revealed approximately sixty notarial acts drafted on the basis of falsified documents. The notary recognized that he had failed to make in-depth searches on the buyers. He explained that some requests of his customers were not clear, in particular when he was reselling four maid's rooms in Paris of less than 10 m^2 for EUR 250 000 each while they had been initially bought for EUR 30 000 euro each..

He admitted making two transfers on bank accounts in Luxembourg belonging to two of presumed fraudsters by knowing perfectly that these are French resident and are not supposed to hold of bank accounts in Luxembourg.

He finally confirmed having realised all the notarial acts by having knowledge that the properties were bought on the basis of loans obtained thanks to forgery documents and internal complicities of the bank.

Without the intervention of this notary, this vast swindle would not have been so extensive

The notary is at present being prosecuted for complicity of money laundering and complicity of organised fraud.

Source: France (2012) questionnaire response

Case 87 **Red flag indicators:**	• Use of false documents • There are multiple appearances of the same parties in transactions over a short period of time • There are remarkable and highly significant differences between he

	declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional • The client holds bank accounts in a foreign country when this is prohibited by law

Case 88: **Legal professional provides a wide range of legal services to three organised crime groups – common law country**

In 2008, Ms Shah a legal executive working within a law firm provided services to three separate Organised Crime Groups (OCGs) by:

facilitating false immigration applications using false or improperly obtained identity documents

securing criminal assets by creating and falsely dating a Deed of Trust on behalf of a subject (who had been sentenced to 14 years imprisonment for drug trafficking) to hide assets from confiscation proceedings

facilitating mortgage fraud and the subsequent disbursement of funds to multiple individuals and companies on behalf of the OCG.

Within a short timeframe, approximately GBP 1 million was paid into the client account from five different mortgage companies, which was then paid out to numerous third parties.

In 2011 Ms Shah was sentenced to five years imprisonment (four years for six counts of fraud and 11 counts of money laundering in relation to the mortgage frauds and subsequent disbursements of funds; and one year for one count of perverting the course of justice in relation to immigration applications).

Source: United Kingdom (2012) questionnaire response

Case 88 **Red flag indicators:**	• Client seeks false or counterfeited documentation • Client is known to have convictions for acquisitive crime

Case 89: **Legal professional facilitates significant property fraud and laundering of the proceeds by ignoring multiple warning signs of fraud and money laundering – common law country**

Between 2009 and 2010 a solicitor acted for sellers in the purchase of a number of properties. Sellers were all introduced to solicitor by a company – these people where engaging in fraud by attempting to sell properties they did not own. Some purchases aborted and funds where then sent to third parties, in other cases the purchaser changed part way through the transaction and the purchase price reduced for no reason. The solicitor did not meet the clients and the dates of birth on the due diligence material provided showed that the person could not have been the same person who owned the property (i.e. they would have been too young to have legally purchased the property). The solicitor received a fine of GBP 5 000 from the Solicitors Disciplinary Tribunal, who noted the fact that solicitor was seriously ill at the time of his failings and did not make a finding of dishonesty.

Source: United Kingdom (2012) questionnaire response

Case 89 **Red flag indicators:**	• Changes in instructions • False identification documents • Unusual reductions in the purchase price.

METHOD: CREATION OF COMPANIES AND TRUSTS

TECHNIQUE: CREATION OF SHELL COMPANIES TO PLACE OR LAYER

Case 90: **Legal professional creates complex multijurisdictional corporate structures to launder funds**

Mr S headed an organisation importing narcotics into country A, from country B. A lawyer was employed by Mr S to launder the proceeds of this operation.

To launder the proceeds of the narcotics importing operation, the lawyer established a web of offshore corporate entities. These entities were incorporated in Country C, where scrutiny of ownership, records and finances was not strong. A local management company in Country D administered these companies. These entities were used to camouflage movement of illicit funds, acquisition of assets and financing criminal activities. Mr S was the holder of 100% of the bearer share capital of these offshore entities. Several other lawyers and their trust accounts were used to receive cash and transfer funds, ostensibly for the benefit of commercial clients in Country A.

When they were approached by law enforcement during the investigation, many of these lawyers cited privilege in their refusal to cooperate. Concurrently, the lawyer established a separate similar network (which included other lawyers' trust accounts) to purchase assets and place funds in vehicles and instruments designed to mask the beneficial owner's identity. The lawyer has not been convicted of any crime in Country A.

Source: FATF (2007)

Case 90 **Red flag indicators:**	• There are attempts to disguise the real owner or parties to the transaction • Use of a complicated ownership structure and multiple countries, including high risk countries, without legitimate reasons • There is only one shareholder of a company • Use of the client account without an underlying transaction

Case 91: **Legal professional creates, dissolves and re-creates corporate entities to assist in laundering the proceeds of large-scale tax evasion – civil law country**

The FIU received a disclosure from a bank on one of its clients, an investment company. This company was initially established in an offshore centre and had moved its registered office to become a limited company under Belgian law. It had consulted a lawyer for this transition.

Shortly afterwards the company was dissolved and several other companies were established taking

over the first company's activities. The whole operation was executed with the assistance of accounting and tax advisors.

The first investment company had opened an account in Belgium that received an important flow of funds from foreign companies. The funds were later transferred to accounts opened with the same bank for new companies. These accounts also directly received funds from the same foreign companies. Part of it was invested on a long-term basis and the remainder was transferred to various individuals abroad, including the former shareholders of the investment company.

The FIU's analysis revealed that the investment company's account and those of its various spin-offs, were used as transit accounts for considerable transfers abroad. The transformation of the investment company into a limited company under Belgian law, shortly followed by the split into several new companies, obscured the financial construction.

The scale of the suspicious transactions, the international character of the construction only partly situated in Belgium, the use of company structures from offshore centres, consulting judicial, financial and fiscal experts, and the fact that there was no economic justification for the transactions all pointed to money laundering related to serious and organised tax fraud, using complex mechanisms or procedures with an international dimension.

Additionally, the managing directors of the investment company had featured in another file that the FIU had forwarded on serious and organised tax fraud. The FIU forwarded this file for money laundering related to serious and organised tax fraud using complex mechanisms or procedures with an international dimension.

Source: Belgium (2012) questionnaire response

Case 91 **Red flag indicators:**	• Creation of complicated ownership structures where there is no legitimate or economic reason, including in high risk countries. • Incorporation and/or purchase of stock or securities of several companies within a short period of time with elements in common and with no logical explanation • There is an increase in capital from foreign countries with limited information as to the connection or basis for the payments.

Case 92: **Legal professional establishes 20 companies for one client on the same day – which are then used to launder the proceeds of organised crime – civil law country**

In a dossier on organised crime, the person concerned was a company director of some twenty companies. Ten of these companies had gone bankrupt. These companies were founded by the same notary. Several suspicious elements led to a notification to the FIU: all companies were founded on the same day, by the same persons and with a very broad social purpose. In addition, these companies had the same address but their company directors live in different countries. This dossier is subject of a judicial inquiry

Source: Cellule de traitement des informations financières (2006)

Case 92 **Red flag indicators:**	• Incorporations of multiple companies in a short period of time with elements in common with no logical explanation • Involvement of individuals from multiple countries as directors of a

	company, without legitimate reason

Case 93: **Legal professionals set up companies which promptly recycled the start up capital to establish new companies to help obscure ownership and layer criminal funds – civil law country**

Several notaries were involved in the setting up of a large number of companies over a number of years. Only the legal minimum of capital was paid up, it was then almost entirely withdrawn in cash and used again to establish new companies. The seat of some companies was also located at the address of an accounting firm and they were led by front men. Several cases showed that the head of the accounting firm himself had raised money for the capital. The established companies were then sold to third parties and used in the context of illegal activities.

Source: Cellule de traitement des informations financières (2009)

Case 93 **Red flag indicators:**	• Incorporation of several companies within a short period of time with elements in common, with no logical explanation • The transaction is unusual in that a company divests itself almost entirely of capital in order to set up other companies.

Case 94: **Junior legal professional involves law firm in laundering proceeds of drug crime – common law country**

A junior lawyer with a Calgary law firm incorporated numerous shell companies in Canada and off-shore on behalf of a client who was involved in a large scale drug importation conspiracy. One shell company incorporated by the lawyer was used to channel more than CAD 6m of funds provided by members of the criminal organisation to other assets. On one occasion the lawyer issued a CAD 7 000 cheque from this shell company to a Vancouver brokerage firm to purchase stock.

Source: Schneider, S. (2004)

Case 94 **Red flag indicators:**	• Incorporation of several companies within a short period of time with elements in common, with no logical explanation, including incorporation in high risk countries • Client is known to have involvement in criminal activity

Case 95: **Three lawyers investigated for establishing companies and purchasing properties on behalf of drug traffickers – common law country**

During one proceeds of crime investigation into three Alberta-based cocaine and marijuana traffickers – Mark Steyne, Pitt Crawley, and George Obsorne – police identified three lawyers who helped the accused establish and operates companies, which were eventually proven to be nothing more than money laundering vehicles.

Documents seized by the RCMP indicated that Becky Sharp acted as legal counsel on behalf of Steyne in the incorporation and preparation of annual returns for Vanity Fair Investments Inc., a public

company in which Steyne and Crawley each held 50 percent voting shares. The corporate address listed for this company was Sharp's law office.

Documents seized by police from the law office of Sharp also showed that she represented Steyne in the purchase of real estate, the title of which was registered in the name of Vanity Fair Investments Inc. Among the documents seized by police were letters from Sharp, addressed to the Vanity Fair Investments, which included certificates of incorporation, bank statements for commercial accounts, and documents showing that Steyne and Crawley were directors and shareholders of the company.

Another lawyer acted on behalf of Steyne and companies he controlled, providing such services as incorporating numbered companies, conducting real estate transactions, purchasing a car wash, and preparing lease agreements between Steyne and the tenants of a home that was used for a marijuana grow operation. Finally, documents seized by police indicated that Majah Dobbin, a partner in a local law firm, acted on behalf of Crawley and Osborne in the incorporation of three other Alberta companies.

Source: Schneider, S. (2004)

Case 95 **Red flag indicators:**	• Use of multiple legal advisors for different businesses without good reasons • Significant funding for companies not consistent with known legitimate income

Case 96: **Legal professional provides office address and acts as director for 17 companies they set up for drug traffickers – common law country**

Public documents seized as part of a police investigation into an international drug trafficking group based in Ontario showed that a Toronto lawyer incorporated 17 different businesses that were eventually traced to members of the crime group. Upon further investigation, police discovered that the office of the law firm was listed as the corporate address for many of the companies. The lawyer was also a director of two of the businesses he helped establish. During their investigation, police learned that two members of this crime group were to go to their lawyer's office —to sign for the new companies. Records obtained from the Ontario Ministry of Consumers and Corporate Relations show that a week later, two limited companies were incorporated listing both as directors.

Source: Schneider, S. (2004)

Case 96 **Red flag indicators:**	• Incorporation of several companies within a short period of time with elements in common, with no logical explanation, including incorporation in high risk countries • Client is known to have involvement in criminal activity

Case 97: **Legal professional creates companies to provide cover story for international travel and movement of funds – civil law country**

A number of Iranian citizens were involved in the incorporation or subsequent purchase of stock in companies. On occasion they attended in person, having travelled from Tehran, while on other occasions they are represented by a German citizen or, more typically, a fellow Iranian citizen resident in Spain.

In 2007 and 2008 Company A was incorporated by an Iranian citizen and the German citizen or by other Iranians citizens acting under their guidance, and the shares of the company were sold to various Iranian citizens, in each transaction for low prices (*e.g.* EUR 25).

In 2009 and 2010 Company B was incorporated directly by Iranian citizens, with the representative or director of the company incorporated either one of the Iranian citizens or the German, appearing in all cases as interpreter.

In both the purchase of stock and the incorporation of companies, the Iranian citizens travel to Spain on occasion, while on other occasions they provide a power of attorney for this purpose executed before a notary in Tehran.

There was no information about the intended business of the companies and the creation of two companies in the same regional area made it unlikely that the companies would be implementing a normal business or economic project. The FIU were of the view that the creation of the companies and involvement of such a wide range of Iranian nationals was to enable them to obtain visas for entry into Spain and therefore to travel through the European Union, for which they receive substantial sums of money, thereby constituting a criminal activity generating funds to be laundered.

Source: Spain (2012) questionnaire response

Case 97 **Red flag indicators:**	• The parties or their representatives are native to and resident in a high risk country and there is no clear connection with the country in which the transaction is happening • A large number of securities are issued at a low price which is not consistent with genuine capital raising purposes • The objects of the company are vague and there appears to be limited commercial viability for both companies

Case 98: **Legal professional assists in creating multijurisdictional web of companies with no legitimate reason for the complexity – civil law jurisdiction**

A Spanish citizen is listed as the director of numerous Spanish limited liability companies with a wide range of corporate purposes (from renewable energies to aquaculture to information technology), although it is not clear whether these companies are genuinely operational.

Within a short space of time these Spanish companies are transferred to recently incorporated Luxembourg-registered companies, for a purchase price of several million euros. Following the transfer of stock, rights issues, involving very considerable sums are performed.

The Luxembourg-registered companies which purchased the stock in the Spanish companies

invested by means of the subscription of corporate stakes in the stock issues of Spanish companies. The foreign purchaser companies were based in Uruguay, Gibraltar, Seychelles, Panama, British Virgin Islands and Portugal. Several of the directors of the purchasing companies are also listed as representatives or directors of some of the transferred companies.

The representatives of the foreign purchaser companies declare that there is no beneficial owner (a natural person with a controlling stake above 25%).

Spanish notaries are required to be involved in all company incorporations and share sales.

Source: Spain (2012) questionnaire response

Case 98 **Red flag indicators:**	• Creation of complicated ownership structures, including multiple countries some of which are high risk, without legitimate reason • Incorporation and/or purchase of stock or securities of several companies within a short period of time with elements in common with no logical explanation. • The company receives an injection of capital which is notably high in comparison with the business size and market value of the company, with no logical explanation.

Case 99: **Legal professional secures banking services for yet to be created companies with significant funds deposited into the accounts and to be transferred between the companies without any apparent underlying economic activity – civil law country**

A lawyer opens bank accounts in the Netherlands in the name of various foreign companies yet to be established. In one of those accounts is deposited an amount of almost 20 million guilders. The intention was that between the accounts of the companies transactions would seem to take place. Per transaction would be a (fictitious) profit of approximately half a million guilders. The bank examines these arrangements and concludes that the lawyer is organising a money laundering scam. The bank refuses further cooperation and sends the money back. The money comes from a large-scale international fraudster.

Source: Netherlands (1996)

Case 99 **Red flag indicators:**	• Involvement of multiple countries without legitimate reason • Significant private funding not consistent with known legitimate income • The transaction is unusual given the amount of profit likely to be generated • Client has been convicted of acquisitive crimes

Case 100: **Legal professional continues to establish corporate entities and conduct share transactions which launder funds despite concerns – civil law country**

Notary Klaas regularly establishes legal entities at the request of client Joep and also conducts share

transactions. Client Joep trades fraudulently in companies. At one point, given the dubious circumstances surrounding the transactions, Klaas consults with a colleague notary who has previously rendered services to Joep. Although they are not able to discover anything suspicious, notary Klaas is left with a 'gut-feeling' that his services are being abused. Klaas does not conduct any deeper investigation into the background of his client and allows himself to be misled on the basis of the documents. He continues to render services without further question. During the police interrogation, Joep states that he used the services of Klaas because the notary worked fast and did not ask tricky questions.

Source: Lankhorst, F. and Nelen, H. (2005

Case 100 **Red flag indicators:**	• Incorporation of multiple companies for a single client, without clear economic justification • Use of multiple legal advisors

Case 101: **Legal professional convicted for allowing client account and personal account to be used by a client engaged in tax fraud – common law country**

In 2002, Mr Hyde, a solicitor assisted a client who had engaged in tax (MTIC) fraud and property development fraud to set up shell companies with off shore accounts, and wittingly allowed his client account and a personal account in the Isle of Man to be used to transfer funds. Over GBP 2m in criminal proceeds were laundered in this way. The solicitor was convicted in 2007 of concealing or disguising criminal property. He was jailed for three and a half years and in 2008 was stuck off.

Source: United Kingdom (2012) questionnaire response

Case 101 **Red flag indicators:**	• Disproportionate amounts of private funding • Complex companies with unnecessary foreign element • Use of client account without underlying transaction • Client known to be involved in criminal activity

Case 102: **Legal professional launders millions through companies for a corrupt PEP due to the mistaken belief that money laundering only involved cash – common law country**

A United Kingdom solicitor who assisted with laundering funds removed from Zambia by a former President. Funds allegedly for defence purposes were transferred through companies which the solicitor had set up, but were then used to fund property purchases, tuition fees and other luxury goods purchases. The solicitor ultimately made a STR and was not prosecuted. The solicitor was also found not to be liable in a civil claim for knowing assistance as dishonesty was not proven. This was on the basis that the claimant did not sufficiently controvert the solicitor's evidence that he had genuinely believed that money laundering only occurred when cash was used and not when money came through a bank. The case related to conduct between 1999 and 2001.

Source: United Kingdom (2012) questionnaire response

Case 102 **Red flag indicators:**	• Client holds a public position in a high risk country • Use of company and government funds to pay for private purchases • There are attempts to obscure the real owners or parties to the transaction

Case 103: **Legal professional convicted for assisting a corrupt PEP to purchase property, vehicles and private jets – common law country**

In 2006, Bhadresh Gohil, a solicitor acted for an African governor. He helped to set up shell companies, transferred funds to foreign accounts, opened bank accounts, purchased property, cars and a private jet for the client. The transactions involved amounts far in excess of the client's income as a governor or other legitimate income. Mr Gohil was convicted in 2010 of entering into arrangements to facilitate money laundering and concealing criminal property and was sentenced to 7 years jail. He was subsequently struck off in 2012. The criminal conviction is currently the subject of an appeal. The governor was convicted of fraud in 2012.

Source: United Kingdom (2012) questionnaire response

Case 103 **Red flag indicators:**	• Client holds a public position in a high risk country • Disproportionate private funding in light of known legitimate income • Use of company and government funds to pay for private purchases

Case 104: **Legal professional prosecuted for allegedly creating companies and otherwise assisting the laundering of the proceeds of drug trafficking – common law jurisdiction**

On November 5, 2012, an indictment was unsealed in the Western District of Texas charging an El Paso attorney, Marco Antonio Delgado, with conspiracy to launder the proceeds of a foreign drug trafficking organization, Cartel de los Valencia (AKA the Milenio Cartel), based in Jalisco, Mexico. Delgado was a principal in his own international law firm, Delgado and Associates, and is alleged to have laundered around USD 2 million, although he reportedly was asked to launder an amount exceeding $600 million.

Between July 2007 and September 2008, Delgado is accused of, among other things: establishing shell companies in the Turks and Caicos for the purpose of laundering drug proceeds; employing couriers to deliver shipments of currency and drawing up fraudulent court documents to provide the couriers with a back story should they be stopped by authorities; arranging a bulk cash smuggling operation unknown to law enforcement while simultaneously "cooperating" with the Government; and attempting to utilize his girlfriend's bank account to launder drug proceeds, although, ultimately, Delgado deposited the funds into his attorney trust account at a U.S. bank.

On February 27, 2013, a second indictment was handed down in the Western District of Texas charging Delgado with wire fraud and money laundering. This prosecution involves a scheme separate and distinct from the drug money laundering above. Here, Delgado defrauded a Nevada company and a Mexican state-owned utility (the *Comision Federal de Electricidad*), in connection a USD 121 million contract to provide heavy equipment and maintenance services for such equipment to a power plant located in Agua Prieta, Sonora, Mexico. FGG Enterprises, LLC ("FGG") is owned and

solely managed by "F.J.G," an unnamed third party. FGG won the contract described above, and payments on the contract were supposed to be directed, by the Mexican utility, through Banco Nacional de Comercio Exterior, to an account owned by FGG at Wells Fargo Bank in El Paso, Texas. Delgado sent a letter to the legal representative of the Mexican utility, instructing the representative to make the payments meant for FGG to a bank account in the Turks and Caicos Islands controlled by Delgado. This letter was sent without the knowledge and consent of F.J.G., the owner of FGG. In total, USD 32 million was wired into the Turks and Caicos account for Delgado's personal enrichment. These funds were subsequently laundered back into the United States to accounts controlled by Delgado.

Furthermore, in a related civil forfeiture action, prosecutors have frozen the proceeds of Delgado's fraud that were sent to the benefit of "Delgado & Associates LLC" from the Mexican utility. The account holding the funds is actually a client account belonging to a local law firm in the Turks & Caicos. The funds belonging to Delgado have been segregated and restrained, as the law firm filed a petition the Turks and Caicos court to modify the initial restraint. Evidently, the legal representatives of Delgado & Associates LLC were unaware that their client account was being used for criminal purposes, as they were informed that the purpose of the Delgado & Associates legal structure was to assist in receiving and disbursing funds related to a client's subcontract to sell turbines to Mexico.

Source: United States (2012) questionnaire response: United States v. Delgado, *No. 3:12-cr-02106-DB (W.D. Tex.) (drug money laundering);* United States v. Delgado, *No. 3:13-cr-00370-DB (W.D. Tex.) (Mexican utility scheme); and* United States v. Any and All Contents of FirstCaribbean International Bank Account Number 10286872, *No. EP 12-cv-0479 (W.D. Tex.).*

Case 104 **Red flag indicators:**	• Clients are known to be under investigation for acquisitive crimes • Involvement of multiple foreign bank accounts and foreign companies without legitimate reasons • Use of the client account without underlying transactions

Case 105: **Legal professional convicted for setting up a sham company and helping to create a cover story to launder the proceeds of crime – common law country**

In a government sting operation, an undercover agent approached attorney Angela Nolan-Cooper, who was suspected of helping launder criminal proceeds for clients, seeking help in laundering supposed drug proceeds. Nolan-Cooper agreed to help, and did so by establishing a sham entity, a purported production company, and hiding the proceeds in Bahamian bank accounts. Nolan-Cooper told the undercover agent that funnelling his money through a corporation would make it appear legitimate because it would establish a source of income and facilitate filing false tax returns that would legitimise the money.

Nolan-Cooper later arranged for an accountant to help draw up false corporation papers and corporate tax returns, although it appears the conspiracy was intercepted before this could occur. Nolan-Cooper also facilitated the deposit of large sums of cash into a Cayman Island account at the direction of the undercover agent, who told her that he needed the money in that account to complete a drug transaction. Nolan-Cooper entered a conditional plea to multiple counts of money laundering. Upon resentencing on remand, Nolan-Cooper was sentenced to 72 months incarceration and three years' supervised release. See 155 F.3d 221 (3rd Cir. 1998) (affirming denial of motion to dismiss and vacating sentence); see also United States v. Carter, 966 F. Supp. 336 (E.D. Pa. 1997)

(reversing the district court's grant of judgment of acquittal).

Source: United States (2012) questionnaire response: United States v. Nolan-Cooper, *No. 95-cr-435-1 (E.D. Pa.)*

Case 105 **Red flag indicators:**	• Involvement of structures and bank accounts in multiple high risk countries with no legitimate reason • Creation of a company whose main purpose is to engage in activities within an industry with which neither the shareholders or the managers have experience or connection • Use of client account without an underlying transaction

Case 106: **Legal professional convicted of setting up companies to launder proceeds of corruption – common law country**

Attorney Jerome Jay Allen pleaded guilty to conspiring to commit money laundering in connection with his assistance in laundering the proceeds of a fraudulent kickback scheme. The scheme involved two employees of a steel processing company who caused their company to overpay commission on certain contracts. A portion of the inflated commission was then funnelled back to the employees through shell companies created by Allen. See United States v. Graham, 484 F.3d 413 (6th Cir. 2007).

Source: United States questionnaire response 2012: United States v. Allen, *No. 5:03-cr-90014 (E.D. Mich.)*

Case 106 **Red flag indicators:**	• Source of funds not consistent with known legitimate income • There are attempts to disguise the real owners or parties to the transactions • U-turn transactions

METHOD: MANAGEMENT OF COMPANIES AND TRUSTS

TECHNIQUE: MANAGEMENT OF A COMPANY OR TRUST – CREATION OF LEGITIMACY AND PROVISION OF LEGAL SERVICES

Case 107: **Legal professional involved in managing an offshore company which was laundering the proceeds of a pyramid scheme – civil law country**

In 2004 the A-FIU received several STRs. The reporting entities have mentioned that some suspects were using several bank accounts (personal bank accounts, company bank accounts and bank accounts from offshore companies). After the analysis the A-FIU assumed that the origin of the money is from fraud and pyramid schemes. The A-FIU disseminated the case to a national law enforcement authority and coordinated the case on international level. The A-FIU requested information from abroad (using Interpol channel, Egmont channel and L/O). The results proved that the Austrian lawyer was a co-perpetrator because he was managing an involved offshore company and the bank account of the company. These results were also disseminated to the national law enforcement agency. The investigation revealed approximately 4000 victims with a total damage of app. EUR 20 mil. The public prosecutor's office issued two international arrest warrants. In 2008

four suspects were convicted for breach of trust. Also the lawyer was convicted for breach of trust with a penalty of 3 years.

Source: Austria (2012) questionnaire response

Case 107 **Red flag indicators:**	• Use of foreign bank accounts and companies without a legitimate reason • Payments made were not consistent with contractual terms

Case 108: **Legal professionals set up companies and accept multiple deposits to launder proceeds of liquor smuggling – hybrid common / civil law country**

A police investigation into Joseph Yossarian, a Quebec liquor smuggler, revealed that he invested money into and eventually purchased a company for which lawyer Pierre Clevingier was the founder, president, director, and sole shareholder. Clevingier was also the comptroller for the company and was listed as a shareholder of three other numbered companies, which police traced to Yossarian. Yet another company, registered in the name of Yossarian's sister, was used as a front for Joseph's investment into a housing development. This company was incorporated by lawyer Robert Heller, who had established other shell companies registered in the name of the sister and used by her brother to launder money. Heller was also involved in transactions relating to companies that he set up for the benefit of Yossarian, including issuing and transferring shares in these companies and lending money between the different companies. Yossarian invested CAD 18 000 in another housing development in Montreal through a company established by Quebec real estate lawyer Albert Tappman. Records seized by police during a search of Tappman's law office established that he had received cash and cheques from Yossarian, including a deposit of CAD 95 000 (CAD 35 000 of which was cash), which he deposited for Yossarian in trust. Police also found copies of two cheques, in the amount of CAD 110 000 and CAD 40 000, drawn on Tappman's bank account, and made payable to the order of a company he created on behalf of Yossarian. Tappman used a numbered company, for which another lawyer was the director and founder, as the intermediary through which Yossarian and others invested in housing developments.

Source: Schneider, S. (2004)

Case 108 **Red flag indicators:**	• Incorporation of several companies in a short period of time with elements in common with no logical reason • Use of multiple legal advisors without legitimate reasons • Significant cash deposits • There are attempts to disguise the real owners of or parties to the transactions • Potential use of a client account without underlying transactions

METHOD: MANAGING CLIENT AFFAIRS AND MAKING INTRODUCTIONS

TECHNIQUE: OPENING BANK ACCOUNTS ON BEHALF OF CLIENTS

Case 109: **Legal professional assists organised criminal to open bank account – civil law country**

A foreigner residing in Belgium was introduced to a bank by a Belgian lawyer's office in order to open an account. This account was then credited by substantial transfers from abroad that were used for purchasing immovable goods. The FIU's analysis revealed that the funds originated from organised crime.

Source: Belgium (2012) questionnaire response

Case 109 **Red flag indicators:**	• Client requires introduction to financial institutions to help secure banking facilities

Case 110: **Legal professional assists foreign PEP to open bank accounts – civil law country**

In a file regarding corruption, a politically exposed person (PEP) was the main beneficial owner of companies and trusts abroad. Accounts in Belgium of these companies received considerable amounts from the government of an African country. The FIU's analysis revealed that the individual had been introduced to the financial institution by a lawyer. It turned out that the lawyer was also involved in other schemes of a similar nature in other judicial investigations.

Source: Belgium (2012) questionnaire response

Case 110 **Red flag indicators:**	• Client holds a public position and is the beneficial owner of multiple companies and trusts in foreign countries • Government funds being used to pay for private or commercial expenses • Client requires introduction to financial institutions to help secure banking facilities

Case 111: **Legal professional assists front company to open bank account – civil law country**

One file regarded a company established in an offshore centre, which was quoted on the stock exchange. Information obtained by the Unit revealed that the stock exchange supervisor had published an official notice stating that the stock of this company had been suspended due to an investigation into fraudulent accounting by this company.

A network of offshore companies was used to intentionally circulate false information regarding this stock in order to manipulate the price. In the meantime a procedure had been initiated by the American stock exchange supervisor to cancel this stock. Information obtained by the Unit revealed that the main stockholder of this company had laundered money from this stock exchange offence by transferring money to an account that he held in a tax haven. In addition, it also became clear that he had called upon a lawyer in Belgium to request opening a bank account in name of a front

company, and to also represent this company in order to facilitate money laundering.

Source: Belgium (2012) questionnaire response

Case 111 **Red flag indicators:**	• Client currently under investigation for acquisitive crime • Involvement of structures with multiple countries, some of which were high risk, without legitimate reason • Client requires introduction to financial institutions to help secure banking facilities

Case 112: **Legal professional convicted for providing laundering services to a criminal group undertaking a Ponzi scheme – common law country**

Six defendants were indicted on 89 counts related to a Treasury bill-leasing Ponzi scheme perpetrated through the corporation K-7. Subsequently, the group's attorney, Louis Oberhauser, was added as a defendant in a superseding indictment. Oberhauser had held some of the invested funds in an attorney trust account designated for K-7 pursuant to an escrow agreement he had drafted. He also had helped to incorporate K-7 and arrange lines of credit on K-7's behalf, as well as entered into contracts with investors on behalf of his law firm that authorized Oberhauser to act on behalf of the investors in entering into a trading program. All defendants excepting Oberhauser and one other co-conspirator pleaded guilty. In a joint trial, the co-conspirator was convicted of 68 counts, and Oberhauser acquitted on 62 of 66 counts and convicted on two counts of money laundering. The district court granted judgment of acquittal, but the appeals court reversed that decision. Oberhauser was sentenced to 15 months' incarceration, two years' supervised release, community service, and restitution in an amount of USD 160 000. *See* 284 F.3d 827 (8th Cir. 2002).

Source: United States (2012) questionnaire response United States v. Oberhauser, No. 99-cr-20(7) (D. Minn.)

Case 112 **Red flag indicators:**	• Legal professional acting in a potential conflict of interest situation • Client requires introduction to financial institutions to help secure banking facilities

Case 113: **Legal professional convicted after setting up companies, structuring deposits and maintaining the company accounts to launder funds – common law country**

Attorney Luis Flores was convicted of one count of conspiracy to commit money laundering, three counts of money laundering, and one count of structuring currency transactions to avoid reporting requirements. A client approached Flores representing himself to be an Ecuadoran food importer/exporter. Flores opened several corporations for the client and established several business accounts. Flores maintained the accounts for a USD 2,000 weekly salary. Flores held himself out as the president of the corporations and was the only authorized signatory on the corporation accounts. Cash deposits into the accounts always totalled less than USD 10 000. As banks closed accounts due to suspicious activity, Flores would open new accounts. He also laundered cash through brokerages on the black market peso exchange. See 454 F.3d 149 (3rd Cir. 2006) (affirming conviction and 32-month sentence).

Source: United States (2012) questionnaire response United States v. Flores, No. 3:04-cr-21 (D.N.J.)

Case 113 **Red flag indicators:**	• Incorporation of multiple corporations and use of multiple bank accounts within a short space of time where there are elements in common with no logical explanation. • Attorney fees disproportionate to the income of the companies. • Structuring of payments • Client requires introduction to financial institutions to help secure banking facilities

TECHNIQUE: MANAGEMENT OF CLIENT'S GENERAL AFFAIRS THROUGH CLIENT ACCOUNT

Case 114: **Legal professional helps to hide cash from a bankruptcy through a life insurance policy – common law country**

A bankrupt individual used the name of a family member to pay cash into an account and to draw a cheque to the value of the cash. He provided the cheque to a lawyer. The lawyer provided a cheque to the family member for part of the sum and then deposited the remainder of the funds into the person's premium life policy which was immediately surrendered. The surrender value was paid into the family member's account.

Source: Australia (2012) questionnaire response

Case 114 **Red flag indicators:**	• Legal professional involved in a U turn transaction • Provision of financial services not in connection with an underlying transaction • Provision of funds from a third party without legitimate reason • Use of client account without an underlying transaction

Case 115: **Legal professional creates web of fake loans and contracts between companies of which he was a director to launder the proceeds of crime – civil law country**

Company A established abroad, with very vague corporate goals and directors residing abroad, had opened an account with a bank in Belgium. This company had been granted a very large investment loan for purchasing a real estate company in Belgium. This loan was regularly repaid by international transfers from the account of Z, one of company A's directors, who was a lawyer. The money did not originate from company A's activities in Belgium. Furthermore, the loan was covered by a bank guarantee by a private bank in North America. This bank guarantee was taken over by a bank established in a tax haven shortly afterwards. Consequently, the financial structure involved a large number of countries, including offshore jurisdictions. The aim was probably to complicate any future investigations on the origin of the money. Furthermore, company A's account was credited by an international transfer with an unknown principal. Shortly afterwards the money was withdrawn in cash by lawyer Z, without an official address in Belgium. Information from the FIU's foreign counterparts revealed that the lawyer's office of which Z was an associate, was suspected of being involved in the financial management of obscure funds. One of the other directors of company A was known for trafficking in narcotics and money laundering. All of these elements indicated that

company A and its directors were part of an international financial structure that was set up to launder money from criminal origin linked to trafficking in narcotics and organised crime.

Source: Belgium (2012) questionnaire response

Case 115 **Red flag indicators:**	• Investment in immovable property, in the absence of links with the place where the property is located • Funding from a private bank in a country not connected with either the location of the company or the location of the property being purchased • Instruction of a legal professional at a distance from the transaction • Third party funding without apparent legitimate connection and withdrawal of that funding in cash shortly after deposit

Case 116: **Lawyer accepts cash, creates companies and purchases property for drug trafficker – common law country**

While an Alberta-based drug trafficker used numerous law firms to facilitate his money laundering activity, he appeared to have preferred one firm over all the others. On numerous occasions, a partner in this preferred law firm accepted cash from the drug trafficker, which was then deposited by the lawyer for his client, in trust. According to deposit slips seized by police, between August 19, 1999 and October 1, 2000 a total of USD 265 500 in cash was deposited by the lawyer in trust for this client. The funds would then be withdrawn to purchase assets, including real estate and cars. The drug trafficker often used shell and active companies to facilitate his money laundering activities. Documents seized by the RCMP showed that on November 9, 1999, the lawyer witnessed the incorporation a company, of which the drug trafficker was a director. Along with the brother of the lawyer, the drug trafficker was also listed as a director of another company and police later identified cash deposits of USD 118 000 into the legal trust account on behalf of this company. The deposit slips were signed by the lawyer. Funds were also transferred between the various trust account files the lawyer established for this client and his companies. In one transaction under the lawyer‘s signature, USD 83 000 was transferred from this client‘s trust account file to the latter company he incorporated on behalf of this client.

Source: Schneider, S. (2004)

Case 116 **Red flag indicators:**	• Use of multiple legal advisors without legitimate reason • Significant deposits of cash not consistent with known legitimate income • Incorporation of multiple companies without legitimate business purposes • Use of client account without an underlying transaction

Case 117: **Legal professional convicted and removed from practice for laundering the proceeds of fraud through his client account and personal account – common law jurisdiction**

The Louisiana Office of Disciplinary Counsel (ODC) filed a petition to permanently disbar attorney Derrick D.T. Shepherd. In April 2008, a federal grand jury indicted Shepherd, who was then serving as a Louisiana state senator, on charges of mail fraud, conspiracy to commit mail and wire fraud, and conspiracy to commit money laundering. The indictment alleged that Shepherd helped a convicted bond broker launder nearly USD 141 000 in fraudulently generated bond fees, and in October 2008, Shepherd pleaded guilty to the money laundering charge. Shepherd admitted to helping broker Gwendolyn Moyo launder construction bond premiums paid to AA Communications, Inc., long after the company was banned from engaging in the insurance business and its accounts were seized by state regulators. Specifically, in December 2006, Shepherd deposited into his client trust account USD 140 686 in checks related to bond premiums and made payable to AA Communications. He then wrote checks totalling USD 75 000 payable to the broker and her associates. Of the remaining funds, Shepherd transferred USD 55 000 to his law firm's operating account and deposited USD 15 000 into his personal checking account. He then moved USD 8 000 from the operating account back into his client trust account. On December 21, 2006, respondent paid off USD 20 000 in campaign debt from his operating account, writing "AA Communications" on the memo line of the check. To conceal this activity, respondent created false invoices and time sheets reflecting work purportedly done by his law firm on behalf of the Ms. Moyo.

Upon investigating Shepherd for multiple ethical violations, the ODC obtained copies of Shepherd's client trust account statements and determined that he had converted client funds on numerous occasions, frequently to mask negative balances in the account. He also commingled client and personal funds and failed to account for disbursements made to clients.

Shepherd submitted untimely evidence to the Court documenting his "substantial assistance to the government in criminal investigations," but the Court found Shepherd's money laundering, which promoted his co-conspirators' unlawful activity and benefitted him personally, to be reprehensible and deserving of the harshest sanction. Despite Shepherd's contention that his federal conviction was not "final" and his denial of any misconduct, the Court permanently disbarred Shepherd from the practice of law.

Source: United States (2012) questionnaire response In re Shepherd, 91 So.3d 283 (La. 2012)

Case 117 **Red flag indicators:**	• Client is known to have convictions for acquisitive crime • Client company is engaging in businesses without a relevant licence / having been banned from engaging in that business • Client is unable to access financial services • Use of client account without underlying transactions, contrary to client account rules • Legal professional acting in potential conflict of interest situation – by making payments into personal accounts

Case 118: **Legal professional convicted for helping ex-police officer launder drug money by accepting cash through his client account for the purchase of stocks – common law jurisdiction**

Defence attorney Scott Crawford was convicted of laundering drug proceeds through his escrow account. Patrick Maxwell, an ex-police officer turned drug dealer, wanted to invest his drug proceeds in the stock market, but wanted to avoid suspicion that would arise if he deposited two large amounts of cash in a bank account. A third party would give Maxwell's cash to Crawford, who would then deposit it in his legal practice's escrow account. From that account, Crawford drew cashier's checks payable to Prudential Securities. The checks were then deposited in a brokerage account controlled by Maxwell. See 281 F. App'x 444 (6th Cir. 2008) (affirming 71-month sentence).

Source: United States (2012) questionnaire response United States v. Crawford, No. 2:04-cr-20150 (W.D. Tenn.)

Case 118 **Red flag indicators:**	• Significant level of cash deposits not consistent with known legitimate income • Payments via a third party in an attempt to disguise the true parties to the transaction • Use of the client account without an underlying legal transaction

Case 119: **Legal professional convicted of money laundering after safe keeping cash obtained from clients he represented in relation to drug charges – common law country**

Attorney Juan Carlos Elso was convicted of money laundering and conspiracy to launder money by engaging in a transaction designed to conceal the origin of drug proceeds and by conspiring to engage in a financial transaction involving drug proceeds so as to avoid reporting requirements. With respect to the money laundering offense, Elso agreed to launder the proceeds of a former client, who he had represented in a drug case and who had paid attorney and investigator fees in cash. Elso retrieved USD 266 800 in cash from the client's house for safekeeping (in case of search by law enforcement). On the way back to his office with the cash, Elso was stopped and arrested. The conspiracy count was based upon a wire transfer Elso made on behalf of the wife of another former drug client. The wife, who was given USD 200 000 to launder, brought Elso USD 10 000, which he deposited into his law firm's trust account and then wired USD 9 800 to an account affiliated with Colombian drug suppliers. Elso did not file federally required reports in conjunction with this transaction. See 422 F.3d 1305 (11th Cir. 2005) (affirming Elso's conviction and 121-month sentence).

Source: United States questionnaire response 2012: United States v. Elso, No. 03-cr-20272 (S.D. Fla.)

Case 119 **Red flag indicators:**	• Client is known to be under investigation / prosecution for acquisitive crimes • Disproportionate amounts of cash not consistent with known legitimate income • Use of the client account without an underlying legal transaction • Structuring of payments

METHOD: USE OF SPECIALISED LEGAL SKILLS

Case 120: **Legal professional arrested after attempting to clear a drug dealers accounts subject to a power of attorney – civil law jurisdiction**

A drug dealer is in detention. He fears that the Prosecutor/judge will confiscate his bank accounts in Luxembourg. The lawyer also approaches a colleague in Luxembourg and asks him how the relationship between the dealer and the money can be broken. The lawyer obtains a power of attorney over the account and attends the bank to withdraw all of the assets from the bank. The lawyer was arrested in his efforts to retrieve the money from the bank.

Source: The Netherlands (1996)

Case 120 **Red flag indicators:**	• Client is known to be under investigation / have convictions for acquisitive crime • Use of foreign bank accounts without legitimate reasons • A power of attorney is sought for the administration or disposal of assets under conditions which are unusual.

Case 121: **Legal professional prosecuted for allegedly creating a range of entities and accounts to launder proceeds of fraud – common law country**

The predicate offence was fraud involving several persons, one of whom was an attorney-at-law and several companies. The offence was committed during the period 1997 to 2000 and the subjects were arrested and charged in 2002.

The attorney-at-law was instrumental in creating different types of financial vehicles such as loans, bonds, shares, trusteeships and a myriad of personal, business and client accounts to facilitate the illicit activity which started with the loan-back method being used to purchase bonds.

It was alleged that the attorney designed documents and transactions to facilitate the laundering of proceeds of the offence, namely obtaining money by false pretences contrary to section 46 of the Proceeds of Crime Act 2000. This matter is before the Courts of Trinidad and Tobago.

Source: Trinidad & Tobago (2012) questionnaire response

Case 121 **Red flag indicators:**	• Involvement of multiple entities, arrangements and bank accounts with elements in common with no legitimate explanation • Client requires introduction to a financial institution to secure banking facilities

Case 122: **Legal professional accepts large amounts of cash for safekeeping and paying bail from criminals he is defending – common law country**

Between 1993 and 2006 a solicitor, Anthony Blok, acted for a number of clients facilitating money laundering. In one case he entered into negotiations to sell a painting he knew clients had stolen and to have it removed from the arts theft register. In another case he received and paid

GBP 75 000 in cash for bail where he was acting for a client whose only source of income had been fraud and money laundering, and lied as to where the money had come from when asked by investigators. Finally, he had large amounts of unexplained cash in envelopes in the office with the names of clients on them – who he was defending in criminal matters. The Court accepted that if the funds had been for the payment of fees, they should have been banked, and absent any explanation as to the reason for holding those funds, the jury conclude that Mr Blok must have been concealing the proceeds of crime on behalf of the clients. In 2009 Mr Blok was convicted of transferring criminal property, possessing criminal property, entering into an arrangement to facilitate money laundering and failure to disclose, 4 years jail. In 2011 he was stuck off the roll.

Source: United Kingdom (2012) survey response

Case 122 **Red flag indicators:**	• Client is known to be under investigation for acquisitive crimes • The holding of large deposits of money without the provision of legal services • Significant amounts of cash not consistent with known legitimate income levels

Case 123: **Legal professional convicted for assisting in laundering the proceeds of a drug deal found in a safe through a real estate investment company – common law country**

Walter Blair was convicted of laundering drug proceeds obtained from a client. His client had possession of a safe containing the drug proceeds of a Jamaican drug organization. After the head of the organization (who owned the safe) was murdered, Blair helped his client to launder the money by inventing an investment scheme based on the Jamaican tradition of cash-based "partners money," setting up a real estate corporation in the name of the client's son, opening an account in the corporation's name, and obtaining loans on behalf of the corporation to make real estate investments. Blair misrepresented the amount of currency in the safe to his client and retained some of the funds in addition to withholding fees for his legal services. See 661 F.3d 755 (4th Cir. 2011), cert. denied 132 S. Ct. 2740 (2012) (affirming conviction and sentence).

Source: United States questionnaire response 2012: United States v. Blair, No. 8:08-cr-505 (D. Md.)

Case 123 **Red flag indicators:**	• Client is known to have connections with criminals • There are attempts to disguise the real owners or parties to the transaction • Source of funds is not consistent with known legitimate income • Client requires introduction to financial institutions to help secure banking facilities • Legal professional is acting in a conflict of interest situation

Appendix S:

FATF, *Guidance for a Risk-Based Approach: Accounting Profession* (Paris: FATF, 2019)

FATF

GUIDANCE FOR A RISK-BASED APPROACH

ACCOUNTING PROFESSION

JUNE 2019

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2019), *Risk-based Approach for the Accounting Profession,* FATF, Paris, www.fatf-gafi.org/publications/documents/ rba-accounting-profession.html

Table of contents

Acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Client[1] due diligence
DNFBP	Designated non-financial businesses and professions
FATF	Financial Action Task Force
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
ML	Money laundering
NRA	National Risk Assessment
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-based approach
SRB	Self-regulatory body
STR	Suspicious transaction report
TCSP	Trust and company service providers
TF	Terrorist financing

[1] In some jurisdictions or professions, the term "customer" is used, which has the same meaning as "client" for the purposes of this document.

Executive Summary

1. The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. It means that supervisors, financial institutions, and professional accountants in public practice (also referred to as "accountants" or "accountancy profession" for the purpose of this Guidance) identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed, and implement the most appropriate mitigation measures. This approach enables them to focus their resources where the risks are higher.

2. The FATF RBA Guidance aims to support the implementation of the RBA, taking into account national ML/TF risk assessments and AML/CFT legal and regulatory frameworks. It includes a general presentation of the RBA and provides specific guidance for the accountancy profession and for their supervisors. The Guidance was developed in partnership with the profession, to make sure it reflects expertise and good practices from within the industry.

3. The development of the ML/TF risk assessment is a key starting point for the application of the RBA. It should be commensurate with the nature, size and complexity of the business. The most commonly used risk criteria are country or geographic risk, client risk, service/transaction risk. The Guidance provides examples of risk factors under these risk categories.

4. The Guidance highlights that it is the responsibility of the senior management of accountants to foster and promote a culture of compliance as a core business value. They should ensure that accountants are committed to manage ML/TF risks when establishing or maintaining business relationships.

5. The Guidance highlights that accountants should design their policies and procedures so that the level of initial and ongoing client due diligence measures addresses the ML/TF risks they are exposed to. In this regard, the Guidance explains the obligations for accountants regarding identification and verification of beneficial ownership information and provides examples of standard, simplified and enhanced CDD measures based on ML/TF risk.

6. The Guidance has a section for supervisors of the accountancy profession and highlights the role of self-regulatory bodies (SRBs) in supervising and monitoring. It explains the risk-based approach to supervision as well as supervision of the risk-based approach by providing specific guidance on licensing or registration requirements for the accountancy profession, mechanisms for on-site and off-site supervision, enforcement, guidance, training and value of information-exchange between the public and private sector.

7. The Guidance also highlights the importance of supervision of beneficial ownership requirements and nominee arrangements. It underscores how supervisory frameworks can help ascertain whether accurate and up-to-date beneficial ownership information on legal persons and legal arrangements is maintained by the accountants and made available in a timely manner to competent authorities when required.

Section I - Introduction and key concepts

This Guidance should be read in conjunction with the following, which are available on the FATF website: www.fatf-gafi.org.

a) The FATF Recommendations, especially Recommendations 1, 10, 11, 12, 17, 19, 20, 21, 22, 23, 24, 25 and 28 and their Interpretive Notes (INR), and the Glossary.

b) Other relevant FATF Guidance documents such as:

- The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)
- FATF Guidance on Transparency and Beneficial Ownership (October 2014)
- FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers (TCSPs) (June 2019)
- FATF Guidance on the Risk-Based Approach for legal professionals (June 2019)

c) Other relevant FATF Reports such as the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018).

Background and context

8. The risk-based approach (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012[2]. The FATF has reviewed its 2009 RBA Guidance for accountants, in order to bring it in line with the new FATF requirements[3] and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version applies to professional accountants in public practice (hereinafter also referred to as "accountants" or "accountancy profession"- see paragraph 16 below). Accountants should also refer to the RBA Guidance for trust and company service providers, when they provide TCSP services.

9. The RBA Guidance for accountants was drafted by a project group comprising FATF members and representatives of the private sector. The project group was co-led by the UK, the United States, the Institute of Chartered Accountants in England and Wales, the International Bar Association and the Society of Trust and Estate Practitioners. Membership of the project group is set out in Annex 4.

10. The FATF adopted this updated RBA Guidance for accountants at its June 2019 Plenary.

2 FATF (2012).

3 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

Purpose of the Guidance

11. The purpose of this Guidance is to:

a) Support a common understanding of a RBA for the accountancy profession, financial institutions and designated non-financial businesses and professions (DNFPBs)[4] that maintain relationships with accountants, competent authorities and self-regulatory bodies (SRBs)[5] responsible for monitoring the compliance of accountants with their AML/CFT obligations;

b) Assist countries, competent authorities and accountants in the design and implementation of a RBA to AML/CFT by providing guidelines and examples of current practice, with a particular focus on providing advice to sole practitioners and small firms;

c) Recognise the difference in the RBA for different accountants providing diverse services such as statutory audit, financial and tax advice, insolvency related services, among others;

d) Outline the key elements involved in applying a RBA to AML/CFT related to accountants;

e) Highlight that financial institutions that have accountants as clients should identify, assess and manage the ML/TF risk associated with accountants and their services;

f) Assist countries, competent authorities and SRBs in the implementation of the FATF Recommendations with respect to accountants, particularly Recommendations 22, 23 and 28;

g) Assist countries, SRBs and the private sector to meet the requirements expected of them, particularly under IO.3 and IO.4;

h) Support the effective implementation of action plans of NRAs conducted by countries; and

i) Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks as well as preventive and mitigating measures.

Target audience, status and content of the Guidance

12. This Guidance is aimed at the following audience:

a) Practitioners in the accountancy profession;

b) Countries and their competent authorities, including AML/CFT supervisors of accountants, SRBs, AML/CFT supervisors of banks that rely on the CDD performed by accountants, and Financial Intelligence Units (FIU); and

c) Practitioners in the banking sector, other financial services sectors and DNFPBs that rely on the CDD performed by accountants.

13. The Guidance consists of four sections. Section I sets out introduction and key concepts. Section II contains key elements of the RBA and should be read in conjunction with specific guidance to accountants (Section III) and guidance to

[4] See definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary.

[5] See definition of the term 'Self-regulatory body' in the FATF Glossary

supervisors of accountants on the effective implementation of a RBA (Section IV). There are four annexes:

a) Beneficial ownership information in relation to a company, trust or other legal arrangements to whom an accountant provides services (Annex 1);

b) Glossary of terminology (Annex 2);

c) Supervisory practices for implementation of the RBA (Annex 3); and

d) Members of the RBA Drafting Group (Annex 4).

14. This Guidance recognises that an effective RBA will take into account the national context, consider the legal and regulatory approach and relevant sector guidance in each country, and reflect the nature, diversity, maturity and risk profile of a country's accountancy profession and the risk profile of individual accountants operating in the sector. The Guidance sets out different elements that countries and accountants could consider when designing and implementing an effective RBA.

15. This Guidance is non-binding and does not overrule the purview of national authorities[6], including on their local assessment and categorisation of the accountancy profession based on the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector to assist competent authorities and accountants to implement applicable FATF Recommendations effectively. National authorities may take this Guidance into account while drawing up their own Guidance for the sector. DNFPBs should also refer to relevant legislation and sector guidance for the country in which an accountant is based.

Scope of the Guidance and key features of the accountancy profession

Scope and Terminology

16. This Guidance is for professional accountants in public practice[7] and is aimed to help them comply with the FATF Recommendations that apply to them. Professional accountant in public practice refers to professional accountants, irrespective of functional classification (for example, audit, tax, advisory or consulting) in a firm or individual practitioners that provide professional services. The nature of services provided (e.g. statutory audit as against other professional services such as financial advice, company services) will determine the scope and depth of due diligence and risk assessment. Professional accountants should also consider their ethical obligations as set out under the Code of Ethics issued by the International Federation of Accountants (IFAC)[8] where relevant.

17. This Guidance is not meant to apply to professional accountants in business, which includes professional accountants employed or engaged in an executive or non-executive capacity in such areas as commerce, industry, service, the public sector, education, the not-for-profit sector, regulatory bodies or professional bodies. Such

6 National authorities should however take the Guidance into account when carrying out their supervisory functions.

7 The term 'accountant' is used interchangeably with 'professional accountant in public practice' throughout this guidance.

8 Handbook of the International Code of Ethics for Professional Accountants issued in 2018.

accountants should refer to their professional code of conduct or other alternative sources of Guidance, on the appropriate action to take in relation to suspected illegal activity by their employer or a third party.

Key features

18. Accountants provide a range of services and activities that vastly differ (e.g. in their methods of delivery and in the depth and duration of the relationships formed with clients, and the size of their operation). This Guidance is written at a high-level to cater for all, and the different levels and forms of supervision or monitoring that may apply. Each country and its national authorities should aim to establish a partnership with its designated non-financial businesses and professions (DNFBP) sector that will be mutually beneficial to combating ML/TF.

19. The roles, and therefore risks, of the different DNFBP and/or professional constituents, including accountants frequently differ. However, in some areas, there are inter-relationships between different DNFBP and/or professional sectors, and between the DNFBPs and financial institutions. For example, businesses or professionals within other DNFBP and/or professional sectors or by financial institutions that may instruct accountants. In some jurisdictions, accountants may also provide trust and company services covered by the FATF Recommendations. For such activities, accountants should refer to the guidance on the risk-based approach for Trust and Company Service Providers (TCSPs).

20. Professional accountants in public practice may provide a wide range of services, to a diverse range of clients. The actual services delivered by accountants may vary between jurisdictions and the examples provided here may not be applicable in every jurisdiction. Services may include (but are not limited to) the following, though not necessarily to the same client. The FATF recommendations apply to specified activities in R.22 (see paragraph 31).

a) Audit and assurance services (including reporting accountant work in initial public offerings);

b) Book-keeping and the preparation of annual and periodic accounts;

c) Tax compliance work;

d) Tax advice;

e) Trust and company services;

f) Internal audit (as a professional service), and advice on internal control and risk management;

g) Regulatory and compliance services, including outsourced regulatory examinations and remediation services;

h) Company liquidation/insolvency/receiver-managers/bankruptcy related services;

i) Advice on the structuring of transactions;

j) Due diligence in relation to mergers and acquisitions

k) Succession advice;

l) Advice on investments and custody of client money; and

m) Forensic accounting.

21. In many countries, accountants are the professionals frequently consulted by many small businesses and individuals when seeking general business advice and a wide range of regulatory and compliance advice. Subject to the codes of professional conduct in the relevant jurisdiction, where services are not within their competence or risk appetite or comfort zone, accountants should refuse the engagement. However, they may advise on an alternate professional advisor (such as a legal professional, notary or trust and company service provider, or another professional accountant).

Vulnerabilities of accounting services

22. Some of the functions performed by accountants that are the most susceptible to the potential launderer include:

a) Financial and tax advice – criminals may pose as individuals seeking financial or tax advice to place assets out of reach in order to avoid future liabilities.

b) Company and trust formation – criminals may attempt to confuse or disguise the links between the proceeds of a crime and the perpetrator through the formation of corporate vehicles or other complex legal arrangements (trusts, for example).

c) Buying or selling of property – criminals may use property transfers to serve as either the cover for transfers of illegal funds (layering stage) or else the final investment of these proceeds after their having passed through the laundering process (integration stage).

d) Performing financial transactions – criminals may use accountants to carry out or facilitate various financial operations on their behalf (e.g. cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers, etc.).

e) Gaining introductions to financial institutions- criminals may use accountants as introducers or intermediaries. This can occur both ways as criminals may use financial institutions to gain introductions to accountants as well.

23. Further, maintenance of incomplete records by clients as revealed during the accounting/bookkeeping services provided by accountants can be an area of higher risk. Also, preparation, review and auditing of financial statements may be susceptible to misuse by criminals where there is a lack of professional body oversight or required use of accounting and auditing standards.

24. Many aspects of this Guidance on applying a RBA to AML/CFT may also apply in the context of predicate offences, particularly for other financial crimes such as tax crimes. The ability to apply the RBA effectively to relevant predicate offences will also reinforce the AML/CFT obligations. Accountants may also have specific obligations in respect of identifying risks of predicate offences such as tax crimes, and supervisors may have a role to play in oversight and enforcement against those crimes. Therefore, in addition to this guidance, accountants and supervisors should have regard to other sources of guidance that may be relevant in managing the risks of predicate offences.

25. Services relating to the formation and management of companies and trusts are seen as being a particular area of vulnerability.

Formation of companies and trusts[9]

26. In some countries, accountants are involved in the formation of a company. While in other countries members of the public are able to register a company themselves directly with the company registry, an accountant's advice is sometimes sought at least in relation to initial corporate, tax and administrative matters.

27. Criminals may seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and often trusts and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies[10], which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy. Criminals may also seek to misuse shelf companies[11], which can be formed by accountants, by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be in an attempt to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of corporate structures, further concealing the underlying beneficial ownership information.

Management of companies and trusts

28. In some cases, criminals will seek to have accountants involved in the management of companies and trusts in order to provide greater respectability and legitimacy to the company or trust and its activities. In some countries professional rules preclude an accountant from acting as a trustee or as a company director, or require a disclosure of directorship positions to ensure independence and transparency is maintained. This will affect whether any funds relating to activities by the company or trust can go through the relevant accountant's client account.

Acting as nominee

29. Individuals may sometimes have accountants or other persons hold their shares as a nominee, where there are legitimate privacy, safety or commercial concerns. However, criminals may also use nominee shareholders to obscure their ownership of assets. In some countries, accountants are not permitted to hold shares in entities for whom they provide advice, while in other countries accountants regularly act as nominees. Accountants should identify beneficial owners when establishing business relations in these situations. This is important to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess and mitigate the potential ML/TF risks associated with the business relationship. Where accountants are asked to act as a nominee, they should understand the reason for this request and ensure they are able

9 The illustrations could also apply to other legal persons and arrangements.

10 A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.

11 A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established.

to verify the identity of the beneficial owner of the shares and that the purpose appears to be legitimate.

Accountancy services for falsified accounts and tax evasion, misuse of client accounts and of insolvency services

30. Criminals may abuse services provided by accountants to provide a sense of legitimacy to falsified accounts in order to conceal the source of funds. For example, accountants may review and sign off such accounts for businesses engaged in criminality, thereby facilitating the laundering of the proceeds. Accountants may also perform high value financial transactions allowing criminals to misuse accountants' client accounts. Insolvency practice, which may be conducted by certain accountancy professionals also pose a risk of criminals concealing the audit trail of money laundered through a company and transferring the proceeds of crime. Accountancy services may also be used to facilitate tax evasion and VAT fraud.

FATF Recommendations applicable to accountants

31. The basic intent behind the FATF Recommendations as it relates to accounting professionals is consistent with their ethical obligations as professionals, namely to avoid assisting criminals or facilitating criminal activity. The requirements of R.22 regarding customer due diligence, record-keeping, PEPs, new technologies and reliance on third parties set out in R. 10, 11, 12, 15 and 17 apply to accountants in certain circumstances. Specifically, the requirements of R.22 applies to accountants when they prepare for or carry out transactions for their clients concerning the following activities:

a) Buying and selling of real estate;

b) Managing of client money, securities or other assets;

c) Management of bank, savings or securities accounts;

d) Organisation of contributions for the creation, operation or management of companies; and

e) Creating, operating or management of legal persons or arrangements, and buying and selling of business entities.

32. R.23 requires that R.18, 19, 20 and 21 provisions regarding internal AML/CFT controls, measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, reporting of suspicious activity and associated prohibitions on tipping-off and confidentiality apply to accountants when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in R.22 above. Section III provides further guidance on the application of R.22 and R.23 obligations to accountants.

33. Countries should establish the most appropriate regime, tailored to address relevant ML/TF risks, which takes into consideration the activities and applicable code of conduct for accountants.

Section II – The RBA to AML/CFT

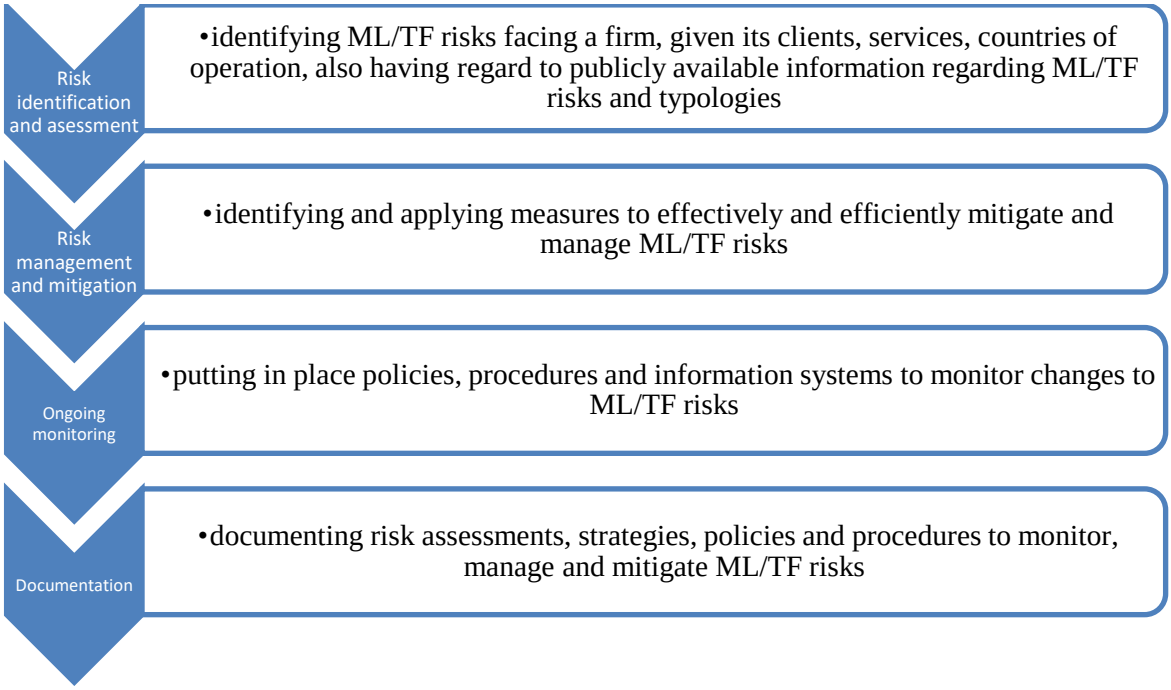
What is the risk-based approach?

34. The RBA to AML/CFT means that countries, competent authorities, DNFBPs, including accountants[12] should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures to effectively and efficiently mitigate and manage the risks.

35. For accountants, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions in which they operate and the effectiveness of actual and potential risk controls that are or can be put in place, will require the investment of resources and training. For supervisors, this will also require maintaining an understanding of the ML/TF risks specific to their area of supervision, and the degree to which AML/CFT measures can reasonably be expected to mitigate such risks.

36. The RBA is not a "zero failure" approach; there may be occasions where an accountancy practice has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks, but is still used for ML or TF purposes in isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that accountants must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

37. Key elements of a RBA can be summarised as follows:



[12] Including both legal and natural persons, see definition of Designated Non-Financial Businesses and Professions in the FATF Glossary.

The rationale for the new approach

38. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards. Its purposes remain to protect the integrity of the financial system by providing governments with updated tools needed to take action against financial crime.

39. There was an increased emphasis on the RBA to AML/CFT, especially in preventive measures and supervision. Though the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations considered the RBA to be an essential foundation of a country's AML/CFT framework.[13]

40. The RBA allows countries, within the framework of the FATF requirements, to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are commensurate with the nature of risks.

41. The application of a RBA is therefore essential for the effective implementation of the FATF Standards by countries and accountants.[14]

Application of the risk-based approach

42. The FATF standards do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF. The overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of factors, including, services, products, clients, geography and the strength of an entity's compliance program.

43. R.1 sets out the scope of application of the RBA as follows:

a) **Who should be subject to a country's AML/CFT regime?** In addition to the sectors and activities already included in the scope of the FATF Recommendations[15], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.[16]

---

13. R.1.

14 The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take into account the risks and the flexibility allowed by the RBA when determining whether there are deficiencies in a country's AML/CFT measures, and their importance *(FATF, 2013f).*

15 See Glossary, definitions of "Designated non-financial businesses and professions" and "Financial institutions".

16 See INR.1.

b) **How should those subject to the AML/CFT regime be supervised or monitored for compliance with this regime?** Supervisors should ensure that accountants are implementing their obligations under R.1. AML/CFT supervisors should consider an accountant's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA.

c) **How should those subject to the AML/CFT regime be required to comply?** The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. Accountants are required to apply each of the CDD measures under (a) to (d) below[17]: (a) identification and verification of the client's identity; (b) identification and taking reasonable measures to verify the identity of the beneficial owner; (c) understanding the purpose and nature of the business relationship; and (d) on-going monitoring of the relationship. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

d) **Consideration of the engagement in client relationships:** Accountants are not obliged to avoid risk entirely. Even if the services they provide to their clients are considered vulnerable to the risks of ML/TF based on risk assessment, it does not mean that all accountants and all their clients or services pose a higher risk when taking into account the risk mitigating measures that have been put in place.

e) **Importance of accountancy services to the overall economy:** Accountants often play significant roles in the legal and economic life of a country. The role of accountants in providing objective assurance regarding the financial status and activity of a business is vital. The risks associated with any type of client group is not static and the expectation is that within a client group, based on a variety of factors, individual clients could also be classified into risk categories, such as low, medium, medium, medium-high or high risk (see section III below for a detailed description). Measures to mitigate risk should be applied accordingly.

Challenges

44. Implementing a RBA can present a number of challenges for accountants in identifying what necessary measures they need to take. A RBA requires resources and expertise, both at a country and sector level, to gather and interpret information on risks, to develop policies and procedures and to train personnel. A RBA is also reliant on individuals exercising sound and well-trained judgement when designing and implementing such policies and procedures. It will also lead to a diversity in practice, although this can result in innovative solutions to address areas of higher risk. On the other hand, accountants may be uncertain as to how to comply with the regulatory

[17] See R.10

framework itself and the accountancy profession may find it difficult to apply an informed approach to RBA.

45. Accountants need to have a good understanding of the risks and should be able to exercise sound judgement. This requires the profession, and the individuals within it, to build expertise through practice and training. If accountants attempt to adopt a RBA without sufficient expertise, or understanding and knowledge of the risks faced by the sector, they may make flawed judgements. Accountants may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, and thereby creating vulnerabilities.

46. Accountants may find that some staff members are uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. It may also encourage a 'tick-box' approach to risk assessment.

47. Developing sound judgement needs good information, and intelligence sharing by designated competent authorities and SRBs. The existence of good practice guidance, training, industry studies and other available information and materials will also assist the accountants to develop methods to analyse the information in order to obtain risk based criteria. Accountants must be able to access this information and guidance easily so that they have the best possible knowledge on which to base their judgements.

48. The services and products accountants provide to their clients vary and are not wholly of financial nature. The FATF Recommendations apply equally to accountants when they are engaged in a specified activity (see paragraph 31), including obligations related to customer due diligence, reporting of suspicious transactions and associated prohibitions on tipping off, record-keeping, identification and risk management related to politically exposed persons or new technologies, and reliance on other third-party financial institutions and DNFBPs.

Box 1. Particular RBA challenges for accountants

Culture of compliance and adequate resources. Implementing a RBA requires that accountants have a sound understanding of the risks and are able to exercise good professional judgement. Above all, management should recognise the importance of a culture of compliance across the organisation and ensure sufficient resources are devoted to its implementation, appropriate to the size, scale and activities of the organisation. This requires the building of expertise including for example, through training, recruitment, taking professional advice and 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making. The process will benefit from information sharing by relevant competent authorities, supervisors and SRBs. The provision of good practice guidance by competent authorities, supervisors and SRBs is also valuable.

Significant variation in services and clients. Accountants may vary substantially in the breadth and nature of services provided and the clients

they serve, as well as the size, focus, and sophistication of the firm and its employees. In implementing the RBA, accounting (and related auditing) professionals should make reasonable judgements for their particular services and activities. Supervisors and SRBs should acknowledge that in a risk-based regime, not all accountants will adopt identical AML/CFT controls. Appropriate mitigation measures will also depend on the nature of the professional's role and involvement. Circumstances may vary considerably between professionals who represent clients directly and those that are engaged for distinct purposes. Where these services involve tax laws and regulations, accounting professionals also have additional considerations related to a country or jurisdiction's permissible means to structure transactions and entities or operations to legally avoid taxes.

Transparency of beneficial ownership on legal persons and arrangements[18]. Accountants may be involved in the formation, management, or administration of legal entities and arrangements, though in many countries any legal or natural person also may be able to conduct these activities. Where professionals do play this "gatekeeper" role, they may be challenged in obtaining and keeping current and accurate beneficial ownership information depending upon the nature and activities of their clientele. Other challenges may arise when taking on new clients with minimal economic activity associated with the legal entity and/or its owners or beneficial owners - such as start-up firms. Finally, whether the source is a public registry or the clientele, there is always potential risk in the correctness of the information, in particular where the underlying information has been self-reported (accountants should refer to the RBA Guidance for TCSPs in this respect). Those risks notwithstanding, from the outset the accountant should seek answers from the immediate client in determining beneficial ownership (having first determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the client is a publicly listed company). The information provided by the client should then be appropriately confirmed by reference to public registers and other third party sources where possible. This may require further and clarifying questions to be put to the immediate client. The goal is to ensure that the accountant is reasonably satisfied about the identity of the beneficial owner. For more practical guidance on beneficial ownership, refer to the guidance in Box 2.

Risk of criminality. Because of their crucial role in providing a legally required window into the financial health and operations of a firm, accountants should be particularly alert to ML/TF risks posed by the services they provide to avoid the possibility that they may unwittingly commit or become an accessory to the commission of a substantive offence of ML/TF. Accounting (and related auditing) firms must protect themselves from misuse by criminals and terrorists.

18 Reference should also be made to the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

Allocating responsibility under a RBA

49. An effective risk-based regime builds on, and reflects, a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector, and its risk profile. Accountants should identify and assess their own ML/TF risk taking account of the NRAs in line with R.1, as well as the national legal and regulatory framework, including any areas of prescribed significant risk and mitigation measures. Accountants are required to take appropriate steps to identify and assess their ML/TF risks and have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.[19] Where ML/TF risks are higher, accountants should always apply enhanced CDD, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g. varying the degree of enhanced ongoing monitoring).

50. Strategies adopted by accountants to mitigate ML/TF risks has to take account of the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which accountants can decide how to mitigate risk, countries should consider the ability of the sector to effectively identify and manage ML/TF risks as well as the expertise and resources of their supervisors to adequately supervise how accountants manage ML/TF risks and take action to address any failures. Countries may also consider evidence from competent authorities on the level of compliance in the sector, and the sector's approach to dealing with ML/TF risk. Countries whose services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that accountants are not fully equipped to effectively identify and manage ML/TF risk. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until understanding and experience of the sector is strengthened.[20]

51. Accountants should not be exempted from AML/CFT supervision even where their compliance controls are adequate. However, the RBA allows competent authorities to focus more supervisory resources on higher risk entities.

Identifying ML/TF risk

52. Access to accurate, timely and objective information on ML/TF risks is a prerequisite for an effective RBA. INR.1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, SRBs, financial institutions and accountants. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share important information on ML/TF risks and threats, or where access to information is restricted by censorship, it will be difficult for accountants to correctly identify ML/TF risk.

53. R.34 requires competent authorities, supervisors and SRBs to establish guidelines and provide feedback to financial institutions and DNFBPs. Such guidelines

[19] R.1 and IN.1.

[20] This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or FSAP.

and feedback help institutions and businesses to identify the ML/TF risks and to adjust their risk mitigating programmes accordingly.

Assessing ML/TF risk

54. Assessing ML/TF risk requires countries, competent authorities, including supervisors, SRBs and accountants to determine how the ML/TF threats identified will affect them. They should analyse the information obtained to understand the likelihood of these risks occurring, and the impact that these would have, on the individual accountants, the entire sector and on the national economy. As a starting step, ML/TF risks are often classified as low, medium-low, medium, medium-high and high Assessing ML/TF risk therefore goes beyond the mere gathering of quantitative and qualitative information, without its proper analysis; this information forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.[21]

55. Competent authorities, including supervisors and SRBs should employ skilled and trusted personnel, recruited through fit and proper tests, where appropriate. They should be technically equipped commensurate with the complexity of their responsibilities. Accounting firms/accountants that are required to routinely conduct a high volume of enquiries when on-boarding clients, e.g. because of the size and geographic footprint of the firm may also consider engaging skilled and trusted personnel who are appropriately recruited and checked. Such accounting firms are also likely to consider using the various technological options (including artificial intelligence) and software programs that are now available to assist accountants in this regard.

56. Accounting firms should develop internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees. Accounting firms should also develop an ongoing employee training programme. They should be trained commensurate with the complexity of their responsibilities.

Mitigating and managing ML/TF risk

57. The FATF Recommendations require that, when applying a RBA, accountants, countries, competent authorities and supervisors decide on the most appropriate and effective way to mitigate and manage the ML/TF risk they have identified. They should take enhanced measures to manage and mitigate situations when the ML/TF risk is higher. In lower risk situations, less stringent measures may be applied:[22]

a) Countries may decide not to apply some of the FATF Recommendations requiring accountants to take certain actions, provided (i) there is a proven low risk of money laundering and terrorist financing, this occurs in strictly limited and justified circumstances and it relates to a particular type of accountants or (ii) a financial activity is carried out by a natural or legal person

21 FATF (2013a), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

22 Subject to the national legal framework providing for Simplified Due Diligence.

on an occasional or very limited basis such that there is a low risk of ML/TF, according to the exemptions of INR 1.6 are met.

b) Countries and accountants looking to apply simplified measures should conduct an assessment to ascertain the lower risk connected to the category of clients or services targeted, establish a threshold for the lower level of the risks involved, and define the extent and the intensity of the required AML/CFT measures, provided that the specific conditions required for one of the exemptions of INR 1.6 are met. Specific Recommendations set out in more detail how this general principle applies to particular requirements.[23]

Developing a common understanding of the RBA

58. The effectiveness of a RBA depends on a common understanding by competent authorities and accountants of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, accountants should deal with the risks they identify. Competent authorities should issue guidance to accountants on meeting their legal and regulatory AML/CFT obligations in a risk-sensitive way. Supporting ongoing and effective communication between competent authorities and the sector is essential.

59. Competent authorities should acknowledge that not all accountants will adopt identical AML/CFT controls in a risk-based regime. On the other hand, accountants should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls with a RBA.

[23] For example, R.22 on Customer Due Diligence.

Section III: Guidance for accountants on implementing a risk-based approach

Risk identification and assessment

60. Accountants should take appropriate steps to identify and assess the risk firm-wide, given their particular client base, that they could be used for ML/TF. This is usually performed as part of the overall client and engagement acceptance processes. They should document those assessments, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and supervisors.[24] The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations.

61. ML/TF risks can be organised into three categories: (a) country/geographic risk, (b) client risk and (c) transaction/service and associated delivery channel risk[25]. The risks and red flags listed in each category are not exhaustive but provide a starting point for accountants to use when designing their RBA.

62. When assessing risk, accountants should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supra-national risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in accounting services/sector, risk reports in other jurisdictions where the accountant based in, and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Accountants may well also draw references to FATF Guidance on indicators and risk factors. During the course of a client relationship, procedures for ongoing monitoring and review of the client's risk profile are also important. Competent authorities should consider how they can best alert accountants to the findings of any national risk assessments, the supranational risk assessments and any other information which may be relevant to assess the risk level particular to an accounting practice in the relevant country.

63. Due to the nature of services that an accountant generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most accountants. There may be some scope to use artificial intelligence and analytical tools in an audit context to spot unusual transactions. The accountant's knowledge of the client and its business will develop throughout the duration of a longer term and interactive professional relationship (in some cases, such relationships may exist for short term clients as well, e.g. for property transactions). However, although individual accountants are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of business relationship. Accountants will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily

24 Paragraph 8 of INR.1

25 Including products, transactions or delivery channels.

be low risk (e.g. one-off client relationship). Accountants should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

64. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow accountants to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the accountant's role and involvement. Circumstances may vary considerably between professionals who represent clients on a single transaction and those involved in a long term advisory relationship.

65. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. An accountant may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB or other credible sources (including a referring accountant).

66. Accountants may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling accountants, where required, to subject each client to reasonable and proportionate risk assessment.

67. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the accountant and/or firm. These criteria, however, should be considered holistically and not in isolation. Accountants, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

68. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller firms and sole practitioners, it is advisable to look at the services they offer (e.g. providing company management services may entail greater risk than other services).

69. Criminals use a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common mechanisms/techniques have been compiled by FATF in the previous studies, including the 2014 FATF Guidance on Transparency and Beneficial Ownership and the 2018 Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership. Accountants may refer to the studies for more details on the use of obscuring techniques and relevant case studies.

70. A practical starting point for accounting firms (especially smaller firms) and accountants (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

a) Client acceptance and know your client policies: identify the client (and its beneficial owners where appropriate) and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of

wealth[26] of the client, where required, its owners and the purpose of the transaction.

b) Engagement acceptance policies: Understand the nature of the work. Accountants should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where an accountant does not have the requisite expertise, the accountant should not undertake the work.

c) Understand the commercial or personal rationale for the work: Accountants need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. Accountants however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.

d) Be attentive to red flag indicators: exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. These cases would trigger reporting obligations. Documenting the thought process by having an action plan may be a viable option to assist in interpreting/assessing red flags/indicators of suspicion.

e) Then consider what action, if any, needs to be taken.

f) The outcomes of the above action (i.e. the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures (including evidence of source of wealth or funds).

g) Accountants should adequately document and record steps taken under a) to e).

Country/Geographic risk

71. A client may be higher risk when features of their business are connected to a higher risk country as regards:

a) the origin, or current location of the source of wealth or funds;

b) where the services are provided;

---

[26] The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust), while the source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). While these may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

c) the client's country of incorporation or domicile;

d) the location of the client's major operations;

e) the beneficial owner's country of domicile; or

f) target company's country of incorporation and location of major operations (for potential acquisitions).

72. There is no universally agreed definition of a higher risk country or geographic area but accountants should pay attention to those countries that are:

a) Countries/areas identified by credible sources[27] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.

c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations.

d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.

e) Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.

Client risk

73. The key risk factors that accountants should consider are:

a) The firm’s client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.

b) The firm’s clients include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients (Please refer to the FATF Guidance (2013) on politically-exposed persons for further guidance on how to identify PEPs).

27 “Credible sources” refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

Box 2. Particular considerations for PEPs and source of funds and wealth

If an accountant is advising a PEP client, or where a PEP is the beneficial owner of assets in a transaction, appropriate enhanced CDD is required if a specified activity under R.22 is involved. Such measures include, obtaining senior management (e.g. senior partner, managing partner or CEO) approval before establishing a business relationship, taking reasonable measures to establish the source of wealth and source of funds of clients and beneficial owners identified as PEPs, and conducting enhanced ongoing monitoring on that relationship.

The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust). Source of funds relates directly to the literal origin of funds to be used in a transaction. This is likely to be a bank account. Generally, this would be evidenced by bank statements or similar. Source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). Source of wealth is the origin of the accrued body of wealth of an individual. Understanding source of wealth is about taking reasonable steps to be satisfied that the funds to be used in a transaction are not the proceeds of crime.

While source of funds and wealth may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

Relevant factors that influence the extent and nature of CDD include the particular circumstances of a PEP, PEPs separate business interests and the time those interests prevailed in relation to the public position, whether the PEP has access to official funds, makes decisions regarding the allocation of public funds or public procurement contracts, the PEP's home country, the type of activity that the PEP is instructing the accountant to perform, whether the PEP is domestic or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

c) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).

d) Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling

interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:

i. Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee and corporate directors, legal persons or legal arrangements, splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.

ii. Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.

iii. Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities or other factors are not consistent with the accountants' understanding of the client's business and economic purpose.

e) Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.

f) Clients that are cash (and/or cash equivalent) intensive businesses. Where such clients are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations, this will aid to mitigate the risks. These may include, for example:

i. Money or Value Transfer Services (MVTS) businesses (e.g. remittance houses, currency exchange houses, casas de cambio, centros cambiarios, remisores de fondos, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities);

ii. Operators, brokers and others providing services in virtual assets;

iii. Casinos, betting houses and other gambling related institutions and activities;

iv. Dealers in precious metals and stones

g) Businesses that while not normally cash intensive appear to have substantial amounts of cash.

h) Non-profit or charitable organizations engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

i) Clients using financial intermediaries, financial institutions or DNFBPs that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or SRBs.

j) Clients who appear to be acting on somebody else's instructions without disclosure.

k) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are

otherwise evasive or very difficult to reach, when this would not normally be expected.

l) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for the accountants to perform a proper risk assessment.

m) Clients with previous convictions for crimes that generated proceeds, who instruct accountants (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.

n) Clients who have no address, or multiple addresses without legitimate reasons.

o) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).

p) Clients who change their settlement or execution instructions without appropriate explanation.

q) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.

r) Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.

s) Clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where accountants may receive a significant premium for a successful provision of their services, should not be considered a risk factor.

t) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.

u) Where there are certain transactions, structures, geographical location, international activities or other factors that are not consistent with the accountants' understanding of the client's business or economic situation.

v) The accountants' client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.

w) Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions.

x) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership.

y) The relationship between employee numbers/structure and nature of the business is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets used compared to similar businesses).

z) Sudden activity from a previously dormant client without any clear explanation.

aa) Clients that start or develop an enterprise with unexpected profile or abnormal business cycles or clients that enters into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.

bb) Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.

cc) Reason for client choosing the accountant is unclear, given the firm's size, location or specialisation.

dd) Frequent or unexplained change of client's professional adviser(s) or members of management.

ee) Client is reluctant to provide all the relevant information or accountants have reasonable grounds to suspect that the information provided is incorrect or insufficient.

ff) Clients seeking to obtain residents rights or citizenship in the country of establishment of the accountants in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.

74. The clients referred to above may be individuals that are, for example, trying to obscure their own business interests and assets or the clients may be representatives of a company's senior management who are, for example, trying to obscure the ownership structure.

Transaction/Service and associated delivery channel risk

75. Services which may be provided by accountants and which (in some circumstances) risk being used to assist money launderers may include:

a) Use of pooled client accounts or safe custody of client money or assets without justification.

b) Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.

c) In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting as trustees of such a trust.

d) Services where accountants may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.

e) Services that are capable of concealing beneficial ownership from competent authorities.

f) Services requested by the client for which the accountant does not have expertise except where the accountant is referring the request to an appropriately trained professional for advice.

g) Non-cash wire transfers through the use of many inter-company transfers within the group to disguise the audit trail.

h) Services that rely heavily on new technologies (e.g. in relation to initial coin offerings or virtual assets) that may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.

i) Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.

j) Transactions where it is readily apparent to the accountant that there is inadequate consideration, where the client does not provide legitimate reasons for the transaction.

k) Administrative arrangements concerning estates where the deceased was known to the accountant as being a person who had been convicted of proceeds generating crimes.

l) Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal under the circumstances and in the experience of the accountant.

m) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.

n) Transactions using unusual means of payment (e.g. precious metals or stones).

o) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

p) Unexplained establishment of unusual conditions/clauses in credit arrangements that do not reflect the commercial position between the parties and may require accountants to be aware of risks. Arrangements that may be abused in this way might include unusually short/long amortisation periods, interest rates materially above/below market rates, or unexplained repeated cancellations of promissory notes/mortgages or other security instruments substantially ahead of the maturity date initially agreed.

q) Transfers of goods that are inherently difficult to value (e.g. jewels, precious stones, objects of art or antiques, virtual assets), where this is not common for

the type of clients, transaction, or with accountant's normal course of business such as a transfer to a corporate entity, or generally without any appropriate explanation.

r) Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.

s) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

t) Power of representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.

u) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.

v) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner) with no apparent legal, tax, business, economic or other legitimate reason.

w) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

x) Commercial, private, or real property transactions or services to be carried out by the client with no apparent legitimate business, economic, tax, family governance, or legal reasons.

y) Existence of suspicions regarding fraudulent transactions, or transactions that are improperly accounted for. These might include:

   i. Over or under invoicing of goods/services.

   ii. Multiple invoicing of the same goods/services.

   iii. Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading).

   iv. Multiple trading of goods/services.

76. In relation to the areas of risk identified above, accountants may also consider the examples of fraud risk factors listed in International Standard of Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements (ISA 240) and the examples of conditions and events that may indicate risks of material misstatement in International Standard of Auditing 315: Identifying and assessing risks of material misstatement through understanding the entity and its environment (ISA315). Even where the accountant is not performing an audit, ISA 240 and ISA 315 provide helpful lists of additional red flags.

Variables that may impact on a RBA and on risk

77. While all accountants should follow robust standards of due diligence in order to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale and expertise amongst accountants, as well as the nature of the clients they serve. As a result, consideration should be given to these factors when creating a RBA that complies with the existing obligations of accountants.

78. Consideration should also be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. In such cases, it may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client for a risk assessment than it would be for a large firm having a diverse client base with different risk profiles. However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may be regarded by criminals as more of a target for money launderers than large law firms. Accountants in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice, and of all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following a RBA.

79. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular accountant. This factor must always be considered in the context of the accountant's practice, as well as the legal, professional, and ethical obligations in the jurisdiction(s) of practice. An accountant's RBA methodology may thus take account of risk variables specific to a particular client or type of work. Consistent with the RBA and proportionality, the presence of one or more of these variables may cause an accountant to conclude that either enhanced CDD and monitoring is warranted, or conversely that standard CDD and monitoring can be reduced, modified or simplified. When reducing, modifying or simplifying CDD, accountants should always adhere to the minimum requirements as set out in national legislation. These variables may increase or decrease the perceived risk posed by a particular client or type of work. While the presence of the specific factors referred to in paragraphs 71-76 may tend to increase risk, there are more general client/ engagement-related variables that may add to or mitigate that risk.

80. Examples of factors that may increase risk are:

a) Unexplained urgency of assistance required.

b) Unusual sophistication of client, including complexity of control environment.

c) Unusual sophistication of transaction/scheme.

d) The irregularity or duration of the client relationship. One-off engagements involving limited client contact throughout the relationship may present higher risk.

81. Examples of factors that may decrease risk are:

a) Involvement of adequately regulated financial institutions or other DNFBP professionals.

b) Similar country location of accountants and client.

c) Role or oversight of a regulator or multiple regulators.

d) The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact and easy flow of information throughout the relationship may present less risk.

e) Private companies that are transparent and well-known in the public domain.

f) Accountant's familiarity with a particular country, including knowledge of and compliance with local laws and regulations as well as the structure and extent of regulatory oversight.

Documentation of risk assessments

82. Accountants must always understand their ML/TF risks (for clients, countries or geographic areas, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis and exercise due professional care and use compelling good judgement. However, competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

83. Accountants may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time efficient yet comprehensive manner has become more important.

84. Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment, and dated. In assessing the risk profile of the client at this stage, reference must be made to the relevant targeted financial sanctions lists to confirm neither the client nor the beneficial owner is designated and included in any of them.

85. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties.

Risk mitigation

86. Accountants should have policies, controls and procedures that enable them to effectively manage and mitigate the risks that they have identified (or that have been identified by the country). They should monitor the implementation of those controls and enhance or improve them if they find the controls to be weak or ineffective. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether

higher or lower) should be consistent with national requirements and with guidance from competent authorities and supervisors. Measures and controls may include:

a) General training on ML/TF methods and risks relevant to accountants.

b) Targeted training for increased awareness by the accountants providing specified activities to higher risk clients or to accountants undertaking higher risk work.

c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain, evidence and record source of wealth and beneficial ownership information if required.

d) Periodic review of the services offered by the accountant, and the periodic evaluation of the AML/CFT framework applicable to the accountant and the accountant's own AML/CFT procedures, to determine whether the ML/TF risk has increased.

e) Reviewing client relationships from time to time to determine whether the ML/TF risk has increased.

Initial and ongoing CDD (R.10 and 22)

87. Accountants should design CDD procedures to enable them to establish with reasonable certainty the true identity of each client and, with an appropriate degree of confidence, know the types of business and transactions the client is likely to undertake. Accountants should have procedures to:

a) Identify the client and verify that client's identity using reliable, independent source documents, data or information.

b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that accountants are satisfied that they knows who the beneficial owner is. This should include accountants' understanding of the ownership and control structure of the client. This is articulated in the following box

Box 3. Beneficial ownership information obligations (see R.10, R.22 and INR.10)

R.10 sets out the instances where accountants will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF, when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the

risks. Accountants should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk. Accountants should also have regard to the AML/CFT 2013 Methodology Criteria 10.5 and 10.8-10.12.

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. Accountants can verify the identity of a client by, for example meeting the client in person and then verifying their identity through the production of a passport/identity card and documentation confirming his/her address. Accountants can further verify the identity of a client on the basis of documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the accountant is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client, and may include conducting public searches as well as by seeking information directly from the client.

Accountants will likely need to obtain the following information for a client that is a legal entity:

a) the name of the company;
b) the company registration number;
c) the registered address and/ or principal place of business (if different);
d) the identity of shareholders and their percentage ownership;
e) names of the board of directors or senior individuals responsible for the company's operations;
f) the law to which the company is subject and its constitution; and
g) the types of activities and transactions in which the company engages.

To verify the information listed above, accountants may use sources such as the following:

a) constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);
b) details from company registers;
c) shareholder agreements or other agreements between shareholders concerning control of the legal person; and
d) filed audited accounts.

Accountants should adopt a RBA to verify beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to-date or to ask for additional documentation that confirms the beneficial ownership and company structure. The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires reasonable steps to be taken to identify the beneficial ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

d) Conduct ongoing due diligence on the business relationship. Ongoing due diligence ensures that the documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of suspicious transaction reports (STRs) to the financial intelligence unit (FIU), or to respond to requests for information from an FIU and the law enforcement agencies.

88. Accountants should design their policies and procedures so that the level of client due diligence addresses the risk of being used for ML/TF by the client. In accordance with the national AML/CFT framework, accountants should design a 'standard' level of CDD for normal risk clients and a reduced or simplified CDD process for low risk clients. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply. Enhanced due diligence should be applied to those clients that are assessed as high risk. These activities may be carried out in conjunction with firms' normal client acceptance procedures and should take account of any specific jurisdictional requirements for CDD.

89. In the normal course of their work, accountants are likely to learn more about some aspects of their client, such as their client's business or occupation and/or their level and source of income, than other advisors. This information is likely to help them reassess the ML/TF risk.

90. A RBA means that accountants should perform varying levels of work according to the risk level. For example, where the client or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, and that information is publicly available, fewer checks may be appropriate. In the case of trusts, foundations or similar legal entities where the beneficiaries are distinct from the legal owners of the entity, it will be necessary to form a reasonable level of knowledge and understanding of the classes and nature of the beneficiaries; the identities of the settlor, trustees or natural persons exercising effective control; and an indication of the purpose of the trust. Accountants will need to obtain a reasonable level of comfort that the declared purpose of the trust is in fact its true purpose.

91. Changes in ownership or control of clients should lead to review or repeat of client identification and verification procedures. This may be carried out in conjunction with any professional requirements for client continuation processes.

92. Public information sources may assist with this ongoing review (scrutinising transactions undertaken throughout the course of that relationship). The procedures that need to be carried out can vary, in accordance with the nature and purpose for which the entity exists, and the extent to which the underlying ownership differs from apparent ownership by the use of nominees and complex structures.

93. The following box provides a non-exhaustive list of examples of standard, enhanced and simplified CDD:

Box 4. Examples of Standard/Simplified/Enhanced CDD measures (see also INR.10)

Standard CDD

- Identifying the client and verifying that client's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the accountant is satisfied about the identity of beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required
- Understanding and obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the business and risk profile the client, including, where necessary, the source of wealth and funds

Simplified CDD

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

Enhanced CDD

- Obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of client and beneficial owner
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of accountants should enable them to disregard source documents, data or information, which is perceived to be unreliable)
- Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship
- Obtaining information on the source of funds and/or source of wealth of the client and clearly evidencing this through appropriate documentation obtained
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship

- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards
- Increasing awareness of higher risk clients and transactions, across all departments with a business relationship with the client, including the possibility of enhanced briefing of engagement teams responsible for the client.
- Enhanced CDD may also include lowering the threshold of ownership (e.g. below 25%), to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.

Politically exposed persons (PEP) (R.12 and R.22)

94. Accountants should take reasonable measures to identify whether a client is a PEP or a family member or close associate of a PEP. Accountants should also refer to the 2013 FATF Guidance on politically-exposed persons for further guidance on how to identify PEPs.

95. If the client or the beneficial owner is a PEP or a family member or close associate of a PEP, accountants should perform the following additional procedures:

a) obtain senior management approval for establishing (or continuing, for existing clients) such business relationships;
b) take reasonable measures to establish the source of wealth and source of funds[28]; and
c) conduct enhanced ongoing monitoring of the business relationship.

96. Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, the PEP's role in a particular government/ government agency, whether the PEP has access to official funds, the PEP's home country, the type of work the PEP is instructing the accountant to perform or carry out (i.e. the services that are being asked for), whether the PEP is domestically based or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

97. The nature of the risk should be considered in light of all relevant circumstances, such as:

a) The nature of the relationship between the client and the PEP. If the client is a trust, company or legal entity, even if the PEP is not a natural person exercising effective control or the PEP is merely a discretionary beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.

b) The nature of the client (e.g. where it is a public listed company or regulated entity which is subject to and regulated for a full range of AML/CFT requirements consistent with FATF recommendations, the fact that it is

[28] See INR 28.1.

subject to reporting obligations will be a relevant factor, albeit this should not automatically qualify the client for simplified CDD).

c) The nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate consideration.

Ongoing monitoring of clients and specified activities (R.10 and 22)

98. Accountants are not expected to scrutinise every transaction that goes through their clients' books and some accounting services are provided only on a one-off basis, without a continuing relationship with the client and without the accountant having access to client's books and/or bank records. However, many of the professional services provided by accountants put them in a relatively good position to encounter and recognise suspicious activities (or transactions) carried out by their clients through their inside knowledge of, and access, to the client's records and management processes and operations, as well as through close working relationships with senior managers and owners. The continued administration and management of the legal persons and arrangements (e.g. account reporting, asset disbursements and corporate filings) would also enable the relevant accountants to develop a better understanding of the activities of their clients.

99. Accountants need to be alert for events or situations which are indicative of a reason to be suspicious of ML/TF, employing their professional experience and judgement in the forming of suspicions where appropriate. An advantage in carrying out this function is the professional scepticism which is a defining characteristic of many professional accountancy functions and relationships.

100. Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that accountants are aware of any changes in the client's identity and risk profile established at client acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds where necessary, to judge consistency with expected behaviour based on accumulated CDD information. As discussed below, ongoing monitoring may also give rise to filing a STR.

101. Accountants should also consider reassessing CDD on an engagement/assignment basis for each client. Well-known, reputable, long-standing clients may suddenly request a new type of service that is not in line with the previous relationship between the client and accountant. Such an assignment may suggest a greater level of risk.

102. Accountants should not conduct investigations into suspected ML/TF on their own but instead file a STR or if the behaviour is egregious they should contact the FIU or law enforcement or supervisors, as appropriate, for guidance. Within the scope of engagement, an accountant should be mindful of the prohibition on "tipping off" the client where a suspicion has been formed. Carrying out additional investigations, which are not within the scope of the engagement should also be considered against the risk alerting a money launderer.

103. When deciding whether or not an activity or transaction is suspicious, accountants may need to make additional enquiries (within the normal scope of the assignment or business relationship) of the client or their records this could typically be done as part of the accountant's CDD process. Normal commercial enquiries, being

made to fulfil duties to clients, may assist in understanding an activity or transaction to determine whether or not it is suspicious.

Suspicious activity/transaction reporting, tipping-off, internal controls and higher-risk countries (R.23)

104. R.23 sets out obligations for accountants on reporting and tipping-off, internal controls and higher-risk countries as set out in R.20, R.21, R.18 and R.19.

Suspicious transaction reporting and tipping-off (R.20, 21 and 23)

105. R.23 requires accountants to report suspicious transactions set out in R.20. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must always be made promptly. The requirement to file a STR is not subject to a RBA, but must be made whenever required in the country concerned.

106. Accountants may be required to report suspicious activities, as well as specific suspicious transaction, and so may make reports on a number of scenarios including suspicious business structures or management profiles which have no legitimate economic rationale and suspicious transactions, such as the misappropriation of funds, false invoicing or company purchase of goods unrelated to the company's business. As specified under INR.23, where accountants seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

107. However, it should be noted that a RBA is appropriate for the purpose of identifying a suspicious activity or transaction, by directing additional resources at those areas that have been identified as higher risk. The designated competent authorities or SRBs may provide information to accountants, which can inform their approach for identifying suspicious activity or transactions, as part of a RBA. Accountant should also periodically assess the adequacy of their system for identifying and reporting suspicious activity or transactions.

108. Accountants should review CDD if they have a suspicion of ML/TF.

Internal controls and compliance (R.18 and 23)

109. In order for accountants to have effective RBA, the risk-based process must be imbedded within the internal controls of the firm and they must be appropriate for the size and complexity of the firm.

Internal controls and governance

110. Strong leadership and engagement by senior management and the Board of Directors (or equivalent body) in AML/CFT is an important aspect of the application of the RBA. Senior management must create a culture of compliance, ensuring that staff adhere to the firm's policies, procedures and processes designed to limit and control risks.

111. The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:

a) designating an individual or individuals, at management level responsible for managing AML/CFT compliance;

b) designing policies and procedures that focus resources on the firm's higher-risk, services, products, clients and geographic locations in which their clients/they operate, and include risk-based CDD policies, procedures and processes;

c) ensuring that adequate controls are in place before new services are offered; and

d) ensuring adequate controls for accepting higher risk clients or providing higher risk services, such as management approval.

112. These policies and procedures should be implemented across the firm and include:

a) performing a regular review of the firm's policies and procedures to ensure that they remain fit for purpose;

b) performing a regular compliance review to check that staff are properly implementing the firm's policies and procedures;

c) providing senior management with a regular report of compliance initiatives, identifying compliance deficiencies, corrective action taken, and STRs filed;

d) planning for changes in management, staff or firm structure so that there is compliance continuity;

e) focusing on meeting all regulatory record-keeping and reporting requirements, recommendations for AML/CFT compliance and providing for timely updates in response to changes in regulations;

f) enabling the timely identification of reportable transactions and ensuring accurate filing of required reports;

g) incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel;

h) providing for appropriate training to be given to all relevant staff;

i) having appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP or a person subject to applicable financial sanctions;

j) providing for adequate controls for higher risk clients and services, as necessary (e.g. additional due diligence, evidencing the source of wealth and funds of a client and escalation to senior management, or additional review and/or consultation);

k) providing increased focus on the accountant/accounting firm's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse for ML/TF;

l) providing for periodic review of the risk assessment and management processes, taking into account the environment within which the accountant/accounting firm operates and the services it provides; and

m) providing for an AML/CFT compliance function and review programme, as appropriate, given the scale of the organisation and the nature of the accountant's practice.

113. The firm should perform a firm-wide risk assessment that takes into account the size and nature of the practice; the existence of high-risk clients (if any); and the provision of high-risk services (if any). Once completed, the firm-wide risk assessment will assist the firm in designing its policies and procedures.

114. Accountants should consider using proven technology-driven solutions to minimise the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the needs of accountants as they continue to develop, this may be particularly important for smaller firms that may be less able to commit significant resources of time to these activities.

115. Depending on the size of the firm, the types of services provided, the risk profile of clients and the overall assessed ML/TF risk, it may be possible to simplify internal procedures. For example, for sole practitioners, providing limited services to low risk clients, client acceptance may be reserved to the sole owners/proprietors taking into account their business and client knowledge and experience. The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms, serving a diverse client base and providing multiple services across geographical locations, more sophisticated procedures are likely to be necessary.

Internal mechanisms to ensure compliance

116. Accountants (at the senior management level) should monitor the effectiveness of internal controls. If accountants identify any weaknesses in those internal controls, improved procedures should be designed.

117. The most effective tool to monitor the internal controls is a regular (typically at least annually) independent (internal or external) compliance review. If carried out internally, a staff member that has a good working knowledge of the firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff are properly applying the firm's procedures.

118. If the compliance review identifies areas of weakness and makes recommendations on how to improve the policies and procedures, then senior management should monitor how the firm is acting on those recommendations.

119. Accountants should review/update firm-wide risk assessments regularly and ensure that policies and procedures continue to target those areas where the ML/TF risks are highest.

Vetting and recruitment

120. Accountants should consider the skills, knowledge and experience of staff both before they are appointed to their role and on an ongoing basis. The level of

assessment should be proportionate to their role in the firm and the ML/TF risks they may encounter. Assessment may include criminal records checking and other forms of pre-employment screening such as credit reference checks and background verification (as permitted under national legislation) for key staff positions.

Education, training and awareness

121. R.18 requires that accounting firms/ accountants provide their staff with AML/CFT training. For accountants, and those in smaller firms in particular, such training may also assist with raising awareness of monitoring obligations. The accounting firm's commitment to having appropriate controls in place relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant staff with at least general information on AML/CFT laws, regulations and internal policies.

122. Firms should provide targeted training for increased awareness by the accountant providing specified activities to higher-risk clients and to accountants undertaking higher- risk work. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Training should also be targeted towards the role that the individual performs in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties, or training regarding red flags for those undertaking client/transactional risk assessment.

123. In line with a RBA, particular attention should be given to risk factors or circumstances occurring in accountant's own practice. In addition, competent authorities, SRBs and representative bodies should work with educational institutions to ensure that the relevant curricula address ML/TF risks. The same training should also be made available for students taking courses to train to become accountants.

124. Firms must provide their employees with appropriate AML/CFT training. In ensuring compliance with this requirement, accountants may take account of any AML/CFT training included in entry requirements and continuing professional development requirements for their professional staff. They must also ensure appropriate training for any relevant staff without a professional qualification, at a level appropriate to the functions being undertaken by those staff, and the likelihood of their encountering suspicious activities.

125. The overall risk-based approach and the various methods available for training and education gives accountants flexibility regarding the frequency, delivery mechanisms and focus of such training. Accountants should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

a) tailored to the relevant staff responsibility (e.g. client contact or administration);

b) at the appropriate level of detail (e.g. considering the nature of services provided by the accountants);

c) at a frequency suitable to the risk level of the type of work undertaken by the accountants; and

d) used to test to assess staff knowledge of the information provided.

Higher-risk countries (R.19 and 23)

126. Consistent with R.19, accountants should apply enhanced due diligence measures (also see paragraph 72 above), proportionate to the risks, to business relationships and transactions with clients from countries for which this is called for by the FATF.

Section IV – Guidance for supervisors

127. R.28 requires that accountants are subject to adequate AML/CFT regulation and supervision. Supervisors and SRBs must ensure that accountants are implementing their obligations under R.1.

Risk-based approach to supervision

128. A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resource to areas of higher ML/TF risk. R.28 requires that accountants are subject to adequate AML/CFT regulation and supervision. While it is each country's responsibility to ensure there is an adequate national framework in place in relation to regulation and supervision of accountants, any relevant supervisors and SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.

Supervisors and SRBs' role in supervision and monitoring

129. According to R.28, countries can designate a competent authority or SRB to ensure that accountants are subject to effective oversight, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF.

130. A SRB is body representing a profession (e.g. accountants, legal professionals, notaries, other independent legal professionals or TCSPs) made up of member professionals, which has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and who practise in the profession. A SRB also performs supervisory or monitoring functions (e.g. to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession).

131. Supervisors and SRBs should have appropriate powers to perform their supervisory functions (including powers to monitor and to impose effective, proportionate and dissuasive sanctions), and adequate financial, human and technical resources. Supervisors and SRBs should determine the frequency and intensity of their supervisory or monitoring actions on accountants on the basis of their understanding of the ML/TF risks, and taking into consideration the characteristics of the accountants, in particular their diversity and number.

132. Countries should ensure that supervisors and SRBs are as equipped as a competent authorities in identifying and sanctioning non-compliance by its members.

Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

133. Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives pertaining to the SRB's role in representing their members, while also being obligated to supervise them. If a SRB contains members of the supervised population, or represents those people, the relevant persons should not continue to take part in the monitoring/ supervision of their practice/firm to avoid conflicts of interest.

134. Supervisors and SRBs should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas

Understanding ML/TF risk

135. The extent to which a national framework allows accountants to apply a RBA should also reflect the nature, diversity and maturity of the sector and its risk profile as well the ML/TF risks associated with individual accountants.

136. Access to information about ML/TF risks is essential for an effective risk-based approach. Countries are required to take appropriate steps to identify and assess ML/TF risks on an ongoing basis in order to (a) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (b) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (c) make information available for AML/CFT risk assessments conducted by accountants and the jurisdictions' national risk assessment. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to competent authorities, SRBs and accountants. In situations where some accountants have limited capacity to identify ML/TF risks, countries should work with the sector to understand their risks.

137. Supervisors and SRBs should, as applicable, draw on a variety of sources to identify and assess ML/TF risks. These may include, but will not be limited to, the jurisdiction's national risk assessments, supranational risk assessments, domestic or international typologies, supervisory expertise and FIU feedback. The necessary information can also be obtained through appropriate information-sharing and collaboration among AML/CFT supervisors, when there are more than one for different sectors (legal professionals, accountants and TCSPs).

138. These sources can also be helpful in determining the extent to which an accountant is able to effectively manage ML/TF risk. Information-sharing and collaboration should take place among AML/CFT supervisors across all sectors (legal professionals, accountants and TCSPs).

139. Competent authorities may also consider undertaking a targeted sectoral risk assessment to get a better understanding of the specific environment in which accountants operate in the country and the nature of services provided by them.

140. Supervisors and SRBs should understand the level of inherent risk including the nature and complexity of services provided by the accountant. Supervisors and SRBs should also consider the type of services the accountant is providing as well as its size and business model (e.g. whether it is a sole practitioner), corporate

governance arrangements, financial and accounting information, delivery channels, client profiles, geographic location and countries of operation. Supervisors and SRBs should also consider the controls accountants have in place (e.g. the quality of the risk management policy, the functioning of the internal oversight functions and the quality of oversight of any outsourcing and subcontracting arrangements).

141. Supervisors and SRBs should seek to ensure their supervised populations are fully aware of, and compliant with, measures to identify and verify a client, the client's source of wealth and funds where required, along with measures designed to ensure transparency of beneficial ownership, as these are cross-cutting issues that affect several aspects of AML/CFT.

142. To further understand the vulnerabilities associated with beneficial ownership, with a particular focus on the involvement of professional intermediaries, supervisors should stay abreast of research papers and typologies published by international bodies.[29] Useful reference include the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

143. Supervisors and SRBs should review their assessment of accountants' ML/TF risk profiles periodically, including when circumstances change materially or relevant new threats emerge and appropriately communicate this assessment to the profession.

Mitigating and managing ML/TF risk

144. Supervisors and SRBs should take proportionate measures to mitigate and manage ML/TF risk. Supervisors and SRBs should determine the frequency and intensity of these measures based on their understanding of the inherent ML/TF risks. Supervisors and SRBs should consider the characteristics of accountants, particularly where they act as professional intermediaries, in particular their diversity and number. It is essential to have a clear understanding of the ML/TF risks: (a) present in the country; and (b) associated with the type of accountant and their clients, products and services.

145. Supervisors and SRBs should take account of the risk profile of accountants when assessing the adequacy of internal controls, policies and procedures.

146. Supervisors and SRBs should develop a means of identifying which accountants are at the greatest risk of being used by criminals. This involves considering the probability and impact of ML/TF risk.

147. Probability means the likelihood of ML/TF taking place as a consequence of the activity undertaken by accountants and the environment in which they operate. The risk can also increase or decrease depending on other factors:

a) service and product risk (the likelihood that services or products can be used for ML/TF);

b) client risk (the likelihood that clients' funds may have criminal origins);

c) the nature of transactions (e.g. frequency, volume, counterparties);

[29] Such as the FATF, the OECD, the WB, the IMF and the UNODC

d) geographical risk (whether the accountant, its clients or other offices trade in riskier locations); and

e) other indicators of risk are based on a combination of objective factors and experience, such as the supervisor's wider work with the accountant as well as information on its compliance history, complaints about the accountant or about the quality of its internal controls, and intelligence from law enforcement agencies on suspected involvement in financial crimes (including unwitting facilitation). Other such factors may include information from government/law enforcement sources, whistle-blowers or negative news reports from credible media particularly those related to predicate offences for ML/TF or to financial crimes.

148. In adopting a RBA to supervision, supervisors may consider allocating supervised entities sharing similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of business, type of clients serviced and geographic areas of activities. The setting up of such groupings could allow supervisors to take a comprehensive view of the sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual firms. If the risk profile of an accountant within a grouping changes, supervisors may reassess the supervisory approach, which may include removing the accountant from the grouping.

149. Supervisors and SRBs should also consider the impact, i.e. the potential harm caused if ML/TF is facilitated by the accountant or group of accountants. A small number of accountants may cause a high level of harm. This can depend on:

a) size (i.e. turnover), number and type of clients, number of premises, value of transactions etc.); and

b) links or involvement with other businesses (which could affect the susceptibility to being involved in 'layering' activity, e.g. concealing the origin of the transaction with the purpose to legalise the asset).

150. The risk assessment should be updated by supervisors and SRBs on an ongoing basis. The result from the assessment will help determine the resources the supervisor will allocate to the supervision of accountants.

151. Supervisors or SRBs should consider whether accountants meet the ongoing requirements for continued participation in the profession as well as assessments of competence and of fitness and propriety. This will include whether the accountant meets expectations related to AML/CFT compliance. This will take place both when a supervised entity joins the profession, and on an ongoing basis thereafter.

152. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to differentiate between categories of accountants based on factors such as their client base, countries they deal with and applicable AML/CFT controls etc.

153. Supervisors and SRBs should acknowledge that in a risk-based regime, not all accountants will adopt identical AML/CFT controls and that an isolated incident where the accountant is part of an illegal transaction unwittingly does not necessarily invalidate the integrity of the accountant´s AML/CFT controls. At the same time, accountants should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

154. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to accountants to enable them to enhance their RBA.

Supervision of the RBA

Licensing or registration

155. R.28 requires a country to ensure that accountants are subject to regulatory and supervisory measures to ensure compliance by the profession with AML/CFT requirements.

156. R.28 requires the supervisor or SRB to take the necessary measures to prevent criminals or their associates from being professionally accredited or holding or being the beneficial owner of a significant or controlling interest or holding a management function in an accountancy practice. This can be achieved through the evaluation of these persons through a "fit and proper" test.

157. A licensing or registration mechanism is one of the means to identify accountants to whom the regulatory and supervisory measures, including the "fit and proper" test should be applied. It also enables the identification of the number of accountants for the purposes of assessing and understanding the ML/TF risks for the country, and the action that should be taken to mitigate them in accordance with R.1.

158. Licensing or registration provides a supervisor or SRB with the means to fulfil a "gatekeeper" role over who can undertake the activities specified in R.22. Licensing or registration should ensure that upon qualification, accountants are subject to AML/CFT compliance monitoring.

159. The supervisor or SRB should actively identify individuals and businesses who should be supervised by using intelligence from other competent authorities (e.g. FIUs, company registry or tax authority), information from financial institutions and DNFBPs, complaints by the public, open source information from advertisements and business and commercial registries, or any other sources which indicate that there are unsupervised individuals or businesses providing the activities specified in R.22.

160. Licensing or registration frameworks should define the activities that are subject to licensing or registration, prohibit unlicensed or unregistered individuals or businesses providing these activities and set out measures for both refusing licences or registrations and for removing "bad actors".

161. The terms "licensing" or "registration" are not interchangeable. Licensing regimes generally tend to operate over financial institutions and impose mandatory minimum requirements based upon Core Principles on issues such as capital, governance, and resourcing to manage and mitigate prudential, conduct as well as ML/TF risks on an on-going basis. Some jurisdictions have adopted similar licensing regimes for accountants, generally where accountants carry out trust and corporate services, to encompass aspects of prudential and conduct requirements in managing the higher level of ML/TF risks that have been identified in that sector.

162. A jurisdiction may have a registration framework over the entire DNFBP sector, including accountants or have a specific registration framework for each constituent of a DNFBP. Generally, a supervisor or SRB carries out the registration function.

163. The supervisor or SRB should ensure that requirements for licensing or registration and the process for applying are clear, objective, publicly available and consistently applied. Determination of the licence or registration should be objective and timely. A SRB could be responsible for both supervision and for representing the interests of its members. If so, the SRB should ensure that registration decisions are taken separately and independently from its activities regarding member representation.

Fit and proper tests

164. A fit and proper test provides a possible mechanism for a supervisor or SRB to take the necessary measures to prevent criminals or their associates from owning, controlling or holding a management function in an accountancy practice.

165. In accordance with R.28, the supervisor or SRB should establish the integrity of every beneficial owner, controller and individual holding a management function in an accountancy practice. However, the decisions on an individual's fitness and propriety may also be based upon a range of factors concerning the individual's competency, probity and judgement as well as integrity.

166. In some jurisdictions, a "fit and proper test" forms a fundamental part of determining whether to license or register the applicant and whether on an ongoing basis the licensee or registrant (including its owners and controllers, where applicable) remains fit and proper to continue in that role. The initial assessment of an individual's fitness and propriety is a combination of obtaining information from the individual and corroborating elements of that information against independent credible sources to determine whether the individual is fit and proper to hold that position.

167. The process for determining fitness and propriety generally requires the applicant to complete a questionnaire. The questionnaire could gather personal identification information, residential and employment history, and require disclosure by the applicant of any convictions or adverse judgements, including pending prosecutions and convictions relating to the applicant. Elements of this information should be corroborated to establish the bona fides of an individual. Such checks could include enquiries about the individual with law enforcement agencies and other supervisors, or screening the individual against independent electronic search databases. The personal data collected should be kept confidential.

168. The supervisor or SRB should also ensure on an ongoing basis that those holding or being the beneficial owner of significant or controlling interest in and individuals holding management functions are fit and proper. A fit and proper test should apply to new owners, controllers and individuals holding a management function. The supervisor or SRB should consider re-assessing the fitness and propriety of these individuals arising from any supervisory findings, receipt of information from other competent authorities; or open source information indicating significant adverse developments.

Guarding against "brass-plate" operations

169. The supervisor or SRB should ensure that its licensing or registration requirements require the applicant to have a meaningful physical presence in the jurisdiction. This usually means that the applicant should have its place of business in the jurisdiction. Where the applicant is a legal person, those individuals who form its mind and management, should also be resident in the jurisdiction and be actively involved in the business. A business with only staff who do not possess the professional requirements of an accountant should not be licensed or registered.

170. A supervisor or SRB should consider the ownership and control structure of the applicant to determine that sufficient control over its operation will reside within the business, which it is considering licensing or registering. Factors to take account of could include consideration of where the beneficial owners and controllers reside, the number and type of management functions the applicant is proposing to have in the country, such as directors and managers, including compliance managers, and the calibre of the individuals who will be occupying those roles.

171. The supervisor or SRB should also consider whether the ownership and control structure of accountants unduly hinders its identification of the beneficial owners and controllers or presents obstacles to applying effective supervision.

Monitoring and supervision

172. Supervisors and SRBs should take measures to effectively monitor accountants through on-site and off-site supervision. The nature of this monitoring will depend on the risk profiles prepared by the supervisor or SRB and the connected risk-based approach. Supervisors and SRBs may choose to adjust:

a) the level of checks required to perform their licensing/registration function: where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited, and approvals may be made on a review of basic documentation. Where the ML/TF risk associated with the sector is high, supervisors and SRBs may ask for additional information.

b) the type of on-site or off-site AML/CFT supervision: supervisors and SRBs may determine the correct mix of on-site and off-site supervision of accountants. Off-site supervision may involve analysis of annual independent audits and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identification of persons responsible for the filing. It may also include undertaking thematic reviews of the sector, making compulsory the periodic information returns from firms. Off-site supervision alone may not be appropriate in higher risk situations. On-site inspections may involve reviewing AML/CFT internal policies, controls and procedures, interviewing members of senior management, compliance officer other relevant and staff, considering gatekeeper's own risk assessments, spot checking CDD documents and supporting evidence, looking at reporting of ML/TF suspicions in relation to clients and other matters, which may be

observed in the course of an onsite visit and, where appropriate, sample testing of reporting obligations.

c) the frequency and nature of ongoing AML/CFT supervision: supervisors and SRBs should proactively adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from accountants' inclusion in thematic review samples).

d) the intensity of AML/CFT supervision: supervisors and SRBs should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of accountants' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include; detailed testing of systems and files to verify the implementation and adequacy of the accountant's risk assessment, CDD, reporting and record-keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT assessment in particular lines of business.

173. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to accountants to enable them to enhance their RBA.

174. Record keeping and quality assurance are important, so that supervisors can document and test the reasons for significant decisions relating to AML/CFT supervision. Supervisors should have an appropriate information retention policy and be able to easily retrieve information while complying with the relevant data protection legislation. Record keeping is crucial and fundamental to the supervisors' work. Undertaking adequate quality assurance is also fundamental to the supervisory process to ensure decision-making/sanctioning is consistent across the supervised population.

Enforcement

175. R.28 requires supervisors or SRB to have adequate powers to perform their functions, including powers to monitor compliance by accountants. R.35 requires countries to have the power to impose sanctions, whether criminal, civil or administrative, on DNFPBs, to include accountants when providing the services outlined in R.22(d). Sanctions should be available for the directors and senior management of the firm when an accountant fails to comply with requirements.

176. Supervisors and SRBs should use proportionate actions, including a range of supervisory interventions and corrective actions to ensure that any identified deficiencies are addressed in a timely manner. Sanctions may range from informal or written warning, reprimand and censure to punitive measures (including disbarment and criminal prosecutions where appropriate) for more egregious non-compliance, as identified weaknesses can have wider consequences. Generally, systemic

breakdowns or significantly inadequate controls will result in more severe supervisory response.

177. Enforcement by supervisors and SRBs should be proportionate while having a deterrent effect. Supervisors and SRBs should have (or should delegate to those who have) sufficient resources to investigate and monitor non-compliance. Enforcement should aim to remove the benefits of non-compliance.

Guidance

178. Supervisors and SRBs should communicate their regulatory expectations. This could be done through a consultative process after meaningful engagement with relevant stakeholders, including accountants. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Guidance issued to accountants should also discuss ML/TF risk within their sector and outline ML/TF indicators to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways that are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction.

179. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the accountancy profession, which may cover operational and practical issues, and be more detailed and explanatory in nature. Where supervisors cooperate to produce combined guidance across sectors, supervisors should ensure this guidance adequately addresses the diversity of roles that come within the guidance's remit, and that such guidance provides practical direction to all its intended recipients. The private sector guidance should be consistent with national legislation and with any guidelines issued by competent authorities with regard to the accountancy profession and be consistent with all other legal requirements and obligations.

180. Supervisors should consider communicating with other relevant domestic supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities across sectors (such as legal professionals, accountants and TCSPs). Multiple guidance should not create opportunities for regulatory arbitrage. Relevant supervisory authorities should consider preparing joint guidance in consultation with the relevant sectors, while recognising that in many jurisdictions accountants will consider that separate guidance targeted at their profession will be the most appropriate and effective form.

181. Information and guidance should be provided by supervisors in an up-to-date and accessible format. It could include sectoral guidance material, newsletters, internet-based material, oral updates on supervisory visits, meetings and annual reports.

Training

182. Training is important for supervisory staff, and other relevant employees, to understand the accountancy profession and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness

and efficiency of AML/CFT policies, procedures and internal controls. It is recommended that the training has a practical basis/dimension.

183. Training should allow supervisory staff to form sound judgments about the quality of the risk assessments made by accountants and the adequacy and proportionality of AML/CFT controls of accountants. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Endorsements

184. Supervisors should avoid mandating the use of AML systems, tools or software of any third party commercial providers to avoid conflicts of interest in the effective supervision of firms.

Information exchange

185. Information exchange between the public and private sector and within private sector (e.g. between financial institutions and accountants) is important to combat ML/TF. Information sharing and intelligence sharing arrangements between supervisors and public authorities (such as Financial Intelligence Units and law enforcement) should be robust, secure and subject to compliance with national legal requirements.

186. The type of information that could be shared between the public and private sectors include:

a) ML/TF risk assessments;

b) Typologies (i.e. case studies) of how money launderers or terrorist financers have misused accountants;

c) feedback on STRs and other relevant reports;

d) targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with accountants as a class or individually; and

e) countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by R.6.

187. Domestic co-operation and information exchange between FIU and supervisors of the accountancy profession and among competent authorities including law enforcement, intelligence, FIU, tax authorities, supervisors and SRBs is also vital for effective monitoring/supervision of the sector. Such co-operation and co-ordination may help avoid gaps and overlaps in supervision and ensure sharing of good practices and findings. Intelligence about active misconduct investigations and completed cases between supervisors and law enforcement agencies should also be encouraged. When sharing information, protocols and safeguards should be implemented in order to protect personal data.

188. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the accountancy profession, taking account of the multi-jurisdictional reach of many accounting firms.

Supervision of Beneficial Ownership requirements and source of funds/wealth requirements

189. The FATF Recommendations require competent authorities to have access to adequate, accurate and timely information on the beneficial ownership and control of legal persons (R.24). In addition, countries must take measures to prevent the misuse of legal arrangements for ML/TF, in particular ensuring that there is adequate, accurate and timely information on express trusts (R.25). Implementation of the FATF Recommendations on beneficial ownership has proven challenging. As a result, the FATF developed a Guidance on Transparency and Beneficial Ownership (2014) to assist countries in their implementation of R.24 and R.25, as well as R.1 as it relates to understanding the ML/TF risks of legal persons and legal arrangements. The FATF and Egmont Group also published the Report on Concealment of Beneficial Ownership in July 2018 which identified issues to help address the vulnerabilities associated with the concealment of beneficial ownership.

190. R.24 and R.25 require countries to have mechanisms to ensure that information provided to registries is accurate and updated on a timely basis and that beneficial ownership information is accurate and current. To determine the adequacy of a system for monitoring and ensuring compliance, countries should have regard to the risk of AML/CFT in given businesses (i.e. if there is a proven higher risk then higher monitoring measures should be taken). Accountants must, however, be cautious in blindly relying on the information contained in registries. It is important for there to be some form of ongoing monitoring during a relationship to detect unusual and potentially suspicious transactions as a result of a change in beneficial ownership as registries are unlikely to provide such information on a dynamic basis.

191. Those responsible for company formation and the creation of legal arrangements fulfil a key gatekeeper role to the wider financial community through the activities they undertake in the formation of legal persons and legal arrangements or in their management and administration.

192. As DNFBPs, accountants are required to apply CDD measures to beneficial owners of legal persons and legal arrangements to whom they are providing advice or formation services. In a number of countries an accountant may be required as part of the process of registering the legal person and will be responsible for providing basic and/or beneficial ownership information to the registry.

193. In their capacity as company directors, trustees or foundation officials etc. of these legal persons and legal arrangement, accountants often represent these legal persons and legal arrangements in their dealings with other financial institutions and DNFBPs that are providing banking or audit services to these types of client.

194. These financial institutions and other DNFBPs may request the CDD information collected and maintained by accountants, who because of their role as director or trustee, will be their principal point of contact with the legal person or legal arrangement. These financial institutions and other DNFBPs may never meet the beneficial owners of the legal person or legal arrangement.

195. Under R.28, countries are to ensure that accountants are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which includes identifying the beneficial owner/s and taking reasonable measures to verify

them. R.24 and R.25, which deal with transparency of beneficial ownership of legal persons and legal arrangements, require countries to have mechanisms for ensuring that adequate, accurate and up-to-date information on these legal entities is available on a timely basis.

196. In accordance with R.28, accountants should be subject to risk-based supervision by a supervisor or SRB covering the beneficial ownership and record-keeping requirements of R.10 and R.11. The supervisor or SRB should have a supervisory framework, which can help in ascertaining that accurate and current basic and beneficial ownership information on legal person and legal arrangements is maintained and will be available on a timely basis to competent authorities.

197. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which accountants have established to identify and record the beneficial owner. In addition, they should undertake sample testing of client records on a representative basis to gauge the effectiveness of the application of those measures and the accessibility of accurate beneficial ownership information.

198. During onsite and offsite inspections, the supervisor or SRB should examine the policies, procedures and controls that are in place for taking on new clients to establish what information and documentation is required where the client is a natural person or legal person or arrangement. The supervisor or SRB should verify the adequacy of these procedures and controls to identify beneficial owners to understand the ownership and control structure of these legal persons and arrangements and to ascertain the business activity. For example, self-declaration on beneficial ownership provided by the client without any other mechanism to verify the information will not be adequate in all cases.

199. Sample testing of records will assist the supervisor or SRB in determining whether controls are effective for the accurate identification of beneficial ownership, accurate disclosure of that information to relevant parties and for establishing if that information is readily available. The extent of testing will be dependent on risk but the records selected should reflect the profile of the client base and include both new and existing clients.

200. The supervisor or SRB should consider the measures the accountants have put in place for monitoring changes in the beneficial ownership of legal person and legal arrangements to whom they provide services to ensure that beneficial ownership information is accurate and current and to determine how timely updated filings are made, where relevant to a registry.

201. During examinations, the supervisor or SRB should consider whether to verify the beneficial ownership information available on the records of accountants with that held by the relevant registry, if any. The supervisor or SRB may also consider information from other competent authorities such as FIUs, public reports and information from other financial institutions or DNFBPs, to verify the efficacy of accountants' controls.

202. Accountants should be subject to risk-based supervision by a supervisor or SRB covering the requirements to identify and evidence the source of funds and source of wealth for higher risk clients to whom they provide services. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current information on sources of funds and wealth is properly

evidenced and available on a timely basis to competent authorities. The supervisor or SRB should analyse the adequacy of the procedures and controls that accountants have established to identify and record sources of wealth in arrangements.

Nominee arrangements

203. A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the beneficial owner.

204. A nominee shareholder is a natural or legal person who is officially recorded in the register of members and shareholders of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held on trust or through a custodial agreement.

205. In a number of countries, accountants act or arrange for other persons (either individuals or corporate) to act as directors. Accountants also act or arrange for other persons (either individuals or corporate) to act as a nominee shareholder for another person as part of their professional services. In accordance with R.24, one of the mechanisms to ensure that nominee shareholders and directors are not misused, is by subjecting these accountants to licensing and recording their status in company registries. Countries may rely on a combination of measures in this respect.

206. There are legitimate reasons for accountants to act as or provide directors to a legal person or act or provide nominee shareholders. These may include the settlement and safekeeping of shares in listed companies where post traded specialists act as nominee shareholders. However, nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of the person from whom they will take instructions or whom they represent. They are sometimes referred to as “strawmen”.

207. Nominee directors and nominee shareholders can create obstacles to identifying the true beneficial owner of a legal person, particularly where the status is not disclosed. This is because it will be the identity of the nominee that is disclosed in the corporate records of the legal person held by a registry and in the company records at its registered office. Company law in various countries does not recognise the status of a nominee director because in law it is the directors of the company who are liable for its activities and the directors have a duty to act in the best interest of the company.

208. The supervisor or SRB should be aware that undisclosed nominee arrangements may exist. They should consider whether undisclosed nominee arrangements would be identified and addressed during their onsite and offsite inspections and examination of the policies, procedures, controls and client records of the accountant, including the CDD process and ongoing monitoring by the accountant.

209. An undisclosed nominee arrangement may exists where there are the following (non-exhaustive) indicators:

a) the profile of a director or shareholder is inconsistent with the activities of the company;

b) the individual holds numerous appointments to unconnected companies;

c) a director's or shareholder's source of wealth is inconsistent with the value and nature of the assets within the company;

d) funds into and out of the company are sent to, or received from unidentified third party/ies;

e) the directors or shareholders are accustomed to acting on instruction of another person; and

f) requests or instructions are subject to minimal or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the director/s.

Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom an accountant provides services

1. Taking a RBA, the amount of information that should be obtained by an accountant will depend on whether an accountant is establishing or administering the trust, company or other legal entity or is acting as or providing a trustee or director of the trust, company or other legal entity. In these cases, an accountant will be required to understand the general purpose behind the structure and the source of funds in the structure in addition to being able to identify the beneficial owners and controlling persons. An accountant who is providing other services (e.g. acting as registered office) to a trust, company or other legal entity will be required to obtain sufficient information to enable it to be able to identify the beneficial owners and controlling persons of the trust, company or other legal entity.

2. An accountant that is not acting as trustee may, in appropriate circumstances, rely on a synopsis prepared by other accountants, legal professionals or TCSPs providing services to the trust or relevant extracts from the trust deed itself to enable the accountant to identify the settlor, trustees, protector (if any), beneficiaries or natural persons exercising effective control. This is in addition to the requirement, where appropriate, to obtain evidence to verify the identity of such persons as discussed below.

In relation to a trust

3. An accountant should have policies and procedures in place to identify the following and verify their identity using reliable, independent source documents, data or information (provided that an accountant's policies should enable it to disregard source documents, data or information which are perceived to be unreliable):

i. the settlor;

ii. the protector;

iii. the trustee(s), where the accountant is not acting as trustee;

iv. the beneficiaries or class of beneficiaries; and

v. any other natural person actually exercising effective control over the trust.

Settlor

a) A settlor is generally any person (or persons) by whom the trust is made. A person is a settlor if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the settlor must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration).

b) A settlor may or may not be named in the trust deed. Accountants should have policies and procedures in place to identify and verify the identity of the real economic settlor.

c) An accountant establishing on behalf of a client or administering a trust, company or other legal entity or otherwise acting as or providing a trustee or

director of a trust, company or other legal entity should have policies and procedures in place (using a RBA) to identify the source of funds in the trust, company or other legal entity.

d) It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift or letter of wishes.

e) Where assets have been transferred to the trust from another trust, it will be necessary to obtain this information for both transferee and transferor trust.

Beneficiaries

a) An accountant should have policies and procedures in place, adopting a RBA to enable it to form a reasonable belief that it knows the true identity of the beneficiaries of the trust, and taking reasonable measures to verify the identity of the beneficiaries, such that an accountant is satisfied that it knows who the beneficiaries are. This does not require an accountant to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the accountant should at least identify and verify the identity of beneficiaries who have current fixed rights to distributions of income or capital or who actually receive distributions from the trust (e.g. a life tenant).

b) Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), an accountant should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).

c) Where beneficiaries are identified by reference to a class (e.g. children and issue of a person) or where beneficiaries are minors under the law governing the trust, although an accountant should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed) the accountant is not obliged to obtain additional information to identify the individual beneficiaries referred to in the class unless or until the trustees make a distribution to such beneficiary.

d) In some trusts, named individuals only become beneficiaries on the happening of a particular contingency (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, an accountant is not required to obtain additional information to identify such contingent beneficiaries unless or until the contingency is satisfied or until the trustees make a distribution to such beneficiary.

e) An accountant who administers the trust or company or other legal entity owned by a trust or otherwise provides or acts as trustee or director to the trust, company or other legal entity should have procedures in place so that there is a requirement to update the information provided if named beneficiaries are added or removed from the class of beneficiaries, or beneficiaries receive distributions or benefits for the first time after the information has been provided, or there are other changes to the class of beneficiaries.

f) An accountant is not obliged to obtain other information about beneficiaries other than to enable an accountant to satisfy itself that it knows who the beneficiaries are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust is a PEP.

Natural person exercising effective control

a) An accountant providing services to the trust should have procedures in place to identify any natural person exercising effective control over the trust.

b) For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:

   i. dispose of or invest (other than as an investment manager or adviser) trust property;

   ii. make or approve trust distributions;

   iii. vary or terminate the trust;

   iv. add or remove a person as a beneficiary or to or from a class of beneficiaries and or;

   v. appoint or remove trustees.

c) An accountant who administers the trust or otherwise act as trustee must, in addition, also obtain information to satisfy itself that it knows the identity of any other individual who has power to give another individual "control" over the trust; by conferring on such individual powers as described in paragraph (b) above.

Corporate settlors and beneficiaries

4. These examples are subject to the more general guidance on what information should be obtained by an accountant to enable it to identify settlors and beneficiaries. It is not intended to suggest that an accountant must obtain more information about a beneficiary that is an entity where it would not need to obtain such information if the beneficiary is an individual.

a) In certain cases, the settlor, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, an accountant should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to the entity.

b) In the case of a settlor that is a legal entity, an accountant should satisfy itself that it has sufficient information to understand the purpose behind the formation of the trust by the entity. For example, a company may establish a trust for the benefit of its employees or a legal entity may act as nominee for an individual settlor or on the instructions of an individual who has provided funds to the legal entity for this purpose. In the case of a legal entity acting as nominee for an individual settlor or on the instructions of an individual, an accountant should take steps to satisfy itself as to the economic settlor of the trust (i.e. the person who has provided funds to the legal entity to enable it to settle funds into the trust) and the controlling persons in relation to the legal entity at the time the assets were settled into trust. If the corporate settlor

retains powers over the trust (e.g. a power of revocation), an accountant should satisfy itself that it knows the current beneficial owners and controlling persons of the corporate settlor and understands the reason for the change in ownership or control.

c) In the case of a beneficiary that is an entity (e.g. a charitable trust or company), an accountant should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, an accountant should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate trustee

a) Where an accountant is not itself acting as trustee, it is necessary for an accountant to obtain information to enable it to identify and verify the identity of the trustee (s) and, where the trustee is a corporate trustee, identify the corporate entity, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity.

b) Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, an accountant should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. An accountant can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body that regulates the trustee and of the regulated trustee itself).

c) It is not uncommon for families to set up trust companies to act for trusts for the benefit of that family. These are typically called private trust companies and may have a restricted trust licence that enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, an accountant should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, an accountant does not need to obtain detailed information to identify the directors or controlling persons of that entity that acts as shareholder of the private trust company.

Individual and Corporate protector

a) Where an accountant is not itself acting as a protector and a protector has been appointed, the accountant should obtain information to identify and verify the identity of the protector.

b) Where the protector is a legal entity, an accountant should obtain sufficient information that it can satisfy itself who is the controlling person and beneficial owner of the protector, and take reasonable measure to verify their identity.

c) Where the protector is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, an accountant should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. An accountant can rely on external evidence, such as information in the public domain to satisfy itself as to the beneficial owner of the regulated protector (e.g. the web-site of the body that regulates the protector and of the regulated protector itself).

Annex 2: Glossary of terminology

Beneficial Owner

Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Competent Authorities

Competent authorities refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency and bearer negotiable instruments (BNIs); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.

Designated Non-Financial Businesses and Professions (DNFBPs)

Designated non-financial businesses and professions means:

a) Casinos (which also includes internet and ship based casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the Recommendations, and which as a business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;

- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

Express Trust

Express trust refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).'

FATF Recommendations

Refers to the FATF Forty Recommendations.

Legal Person

Legal person refers to any entities other than natural persons that can establish a permanent client relationship with an accountant or otherwise own property. This can include bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Legal Professional

In this Guidance, the term *"Legal professional"* refers to legal professionals, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Red Flags

Any fact or set of facts or circumstances which, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A *"red flag"* may be used as a short hand for any indicator of risk which puts an investigating accountant on notice that further checks or other appropriate safeguarding actions will be required.

Self-regulatory bodies (SRB)

A *SRB* is a body that represents a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or

monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

Supervisors

Supervisors refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("financial supervisors") and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

Annex 3: Supervisory practices for implementation of the RBA

China

People's Bank of China ("PBC") Conducts Risk Assessment on Accounting Firms in Jiangsu Province. In November 2017, the PBC Suzhou Branch conducted Money Laundering Risk Assessment on nine accounting firms. The assessments revealed that, for the inherent risk of the accounting firms, there are risks of the Certified Public Accountants utilizing the professional nature of their occupation and confidentiality privilege to assist customers in money laundering; failing to identify illicit funds being injected into the corporate's normal business activities when providing services, and providing services to customers on the monitoring lists or from sensitive jurisdiction. In respect of risk control areas, deficiencies were noted among the accounting firms including the unsound internal control system, weak AML awareness of practitioners, lack of capability, unsatisfactory mechanisms for sanction screening and lack of practical cases of suspicious transaction reports. However, as substantial business practitioners and the target clients of the auditing services are mainly corporates (and mostly being the listed companies and foreign enterprises), the overall money laundering risk of accounting firms was not considered high.

Malaysia

AML/CFT Supervisory Practices of Accountants in Malaysia

A. Fit and Proper Requirements – Self-Regulatory Body (SRB)

The accounting profession in Malaysia is regulated by the Malaysian Institute of Accountants (MIA), as the self-regulated body (SRB) under the Accountants Act (AA) 1967. Prior to their admission as MIA members and issuance of Practicing Certificates, they are subject to appropriate market entry controls in which they are required to fulfil the "fit and proper" requirements under the legislation.

B. AML/CFT Risk-based Supervision – Bank Negara Malaysia (BNM)

Under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), BNM is the designated competent authority for the AML/CFT supervision of the Designated Non-Financial Businesses and Professions (DNFBPs) & Other Financial Institutions in Malaysia, including accountants.

BNM adopts a risk-based approach supervision on accountants, in which the differentiation is guided by the outcome of the National Risk Assessment (NRA) and the application of Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF), as follows:

i. National Risk Assessment (NRA) 2017

Malaysia's third iteration of the NRA in 2017 comprising assessment of ML/TF inherent risk and overall control effectiveness had stipulated the accountants' net ML and TF risks as **"MEDIUM HIGH"** and **"MEDIUM"** level, respectively, as exacerbated by the sector's marginal control, as follows:

ML		TF	
Inherent Risk	Medium	Inherent Risk	Low
Control	Marginal	Control	Marginal
Net Risk	Medium High	Net Risk	Medium

ii. Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF)

D'SuRF encapsulates end-to-end governance and supervisory process, risk-based application of supervisory tools. In line with the ML/TF rating of the sector and the application of D'SuRF, the frequency and intensity of monitoring on accountants are guided accordingly to include a range of supervisory tools, as follows:

- **On-site Examination**

Firms are selected based on a robust selection process under the D'SuRF, which is in line with the risk profile of the reporting institutions (RIs). The on-site examination is in-depth, with assessments covering the RIs' inherent risk and quality of risk management. In applying RBA, BNM imposes post-onsite follow-up measures for RIs with heightened risks. This includes requiring the RI to submit proposals to BNM on planned measures to rectify any supervisory issues and progress report until full rectification. The D'SuRF sets the deadline for both submissions.

- **Off-site Monitoring and Supervisory Outreach Activities**

Apart from on-site examinations, BNM employs a range of off-site monitoring and supervisory outreach activities, aimed to elevate awareness and guide the implementation of the AMLA requirements by the accountants. These off-site tools are also deployed according to the RBA, whereby the intensity and frequency for accountants is relatively higher compared to other sectors. Among the off-site monitoring, includes the submission of Data and Compliance Reports and internal audit reports. In addition, BNM and the relevant SRBs conduct periodic nationwide AML/CFT outreach and awareness programmes.

Monaco

Monaco completed its first NRA (National Risk Assessment) in 2017 and the accountants were included in the scope (see public NRA report in www.siccfin.mc/en/The-National-Risk-Assessment-NRA). The assessed risk

regarding accountants was rated ML (moderate low) so the accountants were not included in the priority professionals to be inspected on-site. However, since 2016, they are being inspected and about two third of the number of accountants has already been assessed. They are planned to have all been assessed by the end of 2021, the most prominent professional having already been inspected (including the Big four companies).

Considering the small number of accountants in Monaco, no real RBA was used for their supervision and these inspections are aimed to be comprehensive.

Annex 4: Members of the RBA Drafting Group

FATF members and observers	Office	Country/Institution
Sarah Wheeler (Co-chair)	Office for Professional Body AML Supervision (OPBAS), FCA	UK
Sandra Garcia (Co-chair)	Department of Treasury	USA
Erik Kiefel	FinCen	
Helena Landstedt and Josefin Lind	County Administrative Board for Stockholm	Sweden
Charlene Davidson	Department of Finance	Canada
Viviana Garza Salazar	Central Bank of Mexico	Mexico
Fiona Crocker	Guernsey Financial Services Commission	Group of International Finance Centre Supervisors(GIFCS)
Ms Janice Tan	Accounting and Regulatory Authority	Singapore
Adi Comeriner Peled	Ministry of Justice	Israel
Richard Walker	Financial Crime and Regulatory Policy, Policy & Resources Committee	Guernsey
Selda van Goor	Central Bank of Netherlands	Netherlands
Natalie Limbasan	Legal Department	OECD
Member	Accountants Office	Institution
Michelle Giddings (Co-chair)	Professional Standards	Institute of Chartered Accountants of England & Wales
Amir Ghandar	Public Policy & Regulation	International Federation of Accountants
Member	Legal professionals and Notaries Office	Institution
Stephen Revell (Co-chair)	Freshfields Bruckhaus Deringer	International Bar Association
Keily Blair	Economic Crime, Regulatory Disputes department	PWC, UK
Mahmood Lone	Regulatory issues and complex cross-border disputes	Allen & Overy LLP, UK
Amy Bell	Law Society's Task Force on ML	Law Society, UK
William Clark	ABA's Task Force on Gatekeeper Regulation and the Profession	American Bar Association (ABA)
Didier de Montmollin	Founder	DGE Avocats, Switzerland
Ignacio Gomá Lanzón Alexander Winkler	CNUE's Anti-Money Laundering working group	Council of the Notariats of the European Union (CNUE)
	Notary office	Austria
Rupert Manhart	Anti-money laundering Committee	Council of Bars and Law Societies of Europe
Silvina Capello	UINL External consultant for AML/CFT issues	International Union of Notariats (UINL)

Member	TCSPs Office	Institution
John Riches (Co-chair) Samantha Morgan	RMW Law LLP	Society of Trust and Estate Practitioners (STEP)
Emily Deane	Technical Counsel	
Paul Hodgson	Butterfield Trust (Guernsey) Ltd	The Guernsey Association of Trustees
Michael Betley	Trust Corporation International	
Paula Reid	A&L Goodbody	A&L Goodbody, Ireland

FATF

GUIDANCE FOR A RISK-BASED APPROACH
ACCOUNTING PROFESSION

The risk-based approach (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012.

This guidance highlights the need for a sound assessment of the money laundering and terroist financing risks that accountants face so that the policies, procedures and ongoing customer due diligence measures mitigate these risks.

The FATF developed this guidance with significant input from the profession itself, to ensure that it reflects the experience gained by public authorities and the private sector over the years.

www.fatf-gafi.org | June 2019

Appendix T:

FATF, *Guidance for a Risk-Based Approach: Legal Professionals*
(Paris: FATF, 2019)

FATF

GUIDANCE FOR A RISK-BASED APPROACH

LEGAL PROFESSIONALS

JUNE 2019

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2019), *Guidance for a Risk-Based Approach for Legal Professionals,* FATF, Paris, www.fatf-gafi.org/publications/documents/Guidance-RBA-legal-professionals.html

TABLE OF CONTENTS

Acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Client[1] due diligence
DNFBP **FIU**	Designated non-financial businesses and professions Financial intelligence unit
INR.	Interpretive Note to Recommendation
ML	Money laundering
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-based approach
SRB **STR**	Self-regulatory body Suspicious transaction report
TCSP **TF**	Trust and company service providers Terrorist financing

[1] In some jurisdictions or professions, the term "customer" is used, which has the same meaning as "client" for the purposes of this document.

Executive Summary

1. The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. It means that competent authorities, supervisors and legal professionals should identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which legal professionals are exposed, and implement appropriate mitigation measures. This approach enables allocation of resources where the risks are higher.

2. The FATF RBA Guidance aims to support the implementation of the RBA, taking into account national ML/TF risk assessments and AML/CFT legal and regulatory frameworks. It includes a general presentation of the RBA and provides specific guidance for legal professionals and for their supervisors. The Guidance was developed in partnership with the profession, to make sure it reflects expertise and good practices from within the profession.

3. The Guidance acknowledges that legal professionals operate within a wide range of business structures - from sole practitioners to large, multi-national firms and provide a variety of services in different jurisdictions. Given the diversity in scale, activities and risk profile, there is, therefore, no one-size-fits-all approach.

4. The development of the ML/TF risk assessment is a key starting point for the application of the RBA. It should be commensurate with the nature, size and complexity of the law firm. The most commonly used risk criteria are country or geographic risk, client risk and service/transaction risk. The Guidance provides examples of risk factors under these risk categories.

5. The Guidance highlights that it is the responsibility of the senior management of legal professionals to foster and promote a culture of compliance. They should ensure that legal professionals are committed to manage ML/TF risks when establishing or maintaining relationships.

6. The Guidance highlights that legal professionals should design their policies and procedures so that the level of initial and ongoing CDD measures addresses the ML/TF risks to which they are exposed. The Guidance thus explains the obligations for legal professionals regarding identification and verification of beneficial ownership information and provides examples of standard, simplified and enhanced CDD measures based on ML/TF risk.

7. The Guidance has a section for supervisors of legal professionals and highlights the role of self-regulatory bodies (SRBs) in supervising and monitoring. It explains the RBA to supervision as well as supervision of the RBA by providing specific guidance on licensing or registration requirements for the profession, mechanisms for on-site and off-site supervision, enforcement, guidance, training and the value of information-exchange between the public and private sector.

8. The Guidance highlights the importance of supervision of beneficial ownership requirements and nominee arrangements. It underscores how supervisory frameworks can help ascertain whether accurate and up-to-date beneficial ownership information on legal persons and legal arrangements is maintained and made available in a timely manner.

Section 1- Introduction and key concepts

This Guidance should be read in conjunction with the following, which are available on the FATF website: *www.fatf-gafi.org.*

a) The FATF Recommendations, especially Recommendations 1, 10, 11, 12, 17, 19, 20, 21, 22, 23, 24, 25 and 28 and their Interpretive Notes (INR), and the FATF Glossary

b) Other relevant FATF Guidance documents such as:

- The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)
- FATF Guidance on Transparency and Beneficial Ownership (October 2014)
- FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers (TCSPs) (June 2019)
- FATF Guidance on the Risk-Based Approach for Accountants (June 2019)

c) Other relevant FATF reports such as:

- FATF Report on Money Laundering and Terrorist Financing: Vulnerabilities of Legal Professionals (June 2013)
- The Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018)

Background and context

9. The RBA is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012[2]. The FATF has reviewed its 2008 RBA Guidance for Legal Professionals, in order to bring it in line with the new FATF requirements[3] and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version applies to legal professionals when they prepare for, or carry out, transactions for their clients concerning certain specified activities[4].

2 FATF (2012).

3 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

4 The services provided by legal professionals include those provided by both lawyers and notaries, and these services are included under bullet (e) of the definition of "Designated non-financial businesses and professions" in the FATF Glossary. For details about specified activities of legal professionals under R.22 and other FATF Recommendations applicable to the legal professionals, please refer to paragraph 20 of this Guidance.

10. This Guidance was drafted by a project group comprising FATF members and representatives of the private sector. The project group was co-led by the UK, the United States, the Institute of Chartered Accountants in England and Wales, the International Bar Association and the Society of Trust and Estate Practitioners. Membership of the project group is set out in Annex 5.

11. The FATF adopted this updated RBA Guidance for legal professionals at its June 2019 Plenary.

Purpose of the Guidance

12. The purpose of this Guidance is to:

a) Assist legal professionals in the design and implementation of a RBA to AML/CFT compliance by providing guidelines and examples of current practice, with a particular focus on providing guidance to sole practitioners and small firms*;*

b) Support a common understanding of a RBA for legal professionals, financial institutions and designated non-financial businesses and professions (DNFBPs)[5] that maintain relationships with legal professionals (e.g. through pooled or client accounts or for trust and company accounts) and competent authorities and self-regulatory bodies (SRBs)[6] responsible for monitoring the compliance of legal professionals with their AML/CFT obligations;

c) Outline the key elements involved in applying a RBA to AML/CFT applicable to legal professionals;

d) Assist financial institutions and DNFBPs that have legal professionals as clients in identifying, assessing and managing the ML/TF risk associated with legal professionals and their services;

e) Assist countries, competent authorities and SRBs in the implementation of the FATF Recommendations with respect to legal professionals, particularly R.22, 23 and 28;

f) Assist countries, SRBs and the private sector to meet the requirements expected of them, particularly under IO.3 and IO.4;

g) Support the effective implementation of action plans of national risk assessments (NRAs) conducted by countries; and

h) Support the effective implementation and supervision by countries of national AML/CFT measures, by focusing on risks as well as preventive and mitigating measures.

[5] Including both legal and natural persons, see definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary.

[6] See definition of the term 'Self-regulatory body' in the FATF Glossary.

Target audience, status and content of the Guidance

13. This Guidance is aimed at the following audience:

a) Legal professionals;

b) Countries and their competent authorities, including AML/CFT supervisors of legal professionals, AML/CFT supervisors of banks that have legal professionals as customers, and Financial Intelligence Units (FIUs); and

c) Practitioners in the banking sector, other financial services sectors and DNFBPs that have legal professionals as customers.

14. The Guidance consists of four sections. Section I sets out introduction and key concepts. Section II contains key elements of the RBA and should be read in conjunction with specific guidance to legal professionals (Section III) and guidance to supervisors of legal professionals on the effective implementation of a RBA (Section IV). There are six annexes on:

a) Beneficial ownership information in relation to a company, trust or other legal arrangements to whom a legal professional provides services (Annex 1);

b) Sources of further information (Annex 2);

c) Glossary of terminology (Annex 3);

d) Supervisory practices for implementation of the RBA (Annex 4);

e) Red flag indicators highlighting suspicious activities or transactions for legal professionals (Annex 5); and

f) Members of the RBA Drafting Group (Annex 6).

15. This Guidance recognises that an effective RBA will take into account the national context, consider the legal and regulatory approach and relevant sector guidance in each country, and reflect the nature, diversity, maturity and risk profile a country's legal professionals and the risk profile of individual legal professionals operating in the sector and their clients. The Guidance sets out different elements that countries and legal professionals could consider when designing and implementing an effective RBA.

16. This Guidance is non-binding and does not overrule the purview of national authorities[7], including on their local assessment and categorisation of legal professionals based on the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector to assist competent authorities and legal professionals to implement effectively applicable FATF Recommendations. National authorities may take this Guidance into account while drawing up their own Guidance for the sector. Legal professionals should also refer to relevant legislation and sector guidance of the country where their clients are based.

[7] National authorities should however take the Guidance into account when carrying out their supervisory functions.

Scope of the Guidance: terminology, key features and business models

Terminology

Legal professionals

17. The FATF Recommendations apply to all legal professionals when they carry out specified transactional activities for third parties (see below) and do not apply to all activities carried out by legal professionals. Most notably, litigation is not a specified activity, and a legal professional representing a client in litigation will not be subject to the FATF Recommendations; unless during the course of such representation the legal professional additionally engages in one or more specified activities, in which case the Recommendations will apply to this specified activity or activities only. The FATF Recommendations do not apply where a person provides legal services 'in-house' as an employee of an entity that does not provide legal services.

18. The legal sector comprises a broad spectrum of practitioners and is not a homogenous group, from one country to another or even within a country. For the purposes of this Guidance, legal professionals include barristers, solicitors and other specialist advocates and notaries. In addition to obligations they may owe through the contracting of their services, legal professionals owe special duties both to their clients (e.g. duties of confidentiality and loyalty), as well as public duties to the legal institutions of their jurisdictions (e.g. through roles such as 'officers of the court'). These duties are designed to assist in the administration of justice and promote the rule of law, and generally set legal professionals apart from other professional advisors. In many jurisdictions, these duties and obligations are enshrined in law, regulations or court rules pursuant to historic and well established practices.

19. Titles given to different legal professionals vary among countries and legal systems, with the same title not always having the same meaning or area of responsibility. Although some common elements may exist based on whether the country has a common law or civil law tradition, even these generalisations will not always hold true. As the range of services provided and carried out by legal professionals is diverse and varies widely from one country to another, it is important to understand the specific roles undertaken by different legal professionals within their respective countries when assessing the AML/CFT obligations of the legal profession sector, as well as how these services interact with those of other professionals. Many legal professionals are required to comply with specific national legislation, rules and regulations adopted by professional associations or other SRBs.

20. R.22 provides that the customer due diligence and record-keeping requirements of the Recommendations apply to legal professionals when they prepare for and carry out certain specified activities for their clients, namely:

a) Buying and selling of real estate;

b) Managing of client money, securities or other assets;

c) Management of bank, savings or securities accounts;

d) Organisation of contributions for the creation, operation or management of companies; and

e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

21. The FATF Recommendations set an international standard, which countries should implement through measures adapted to the circumstances of their particular jurisdictions. In general terms, jurisdictions have closely followed the FATF Recommendations but differences exist and legal professionals need to carefully consider the laws, rules and regulations of the relevant jurisdictions as implemented in such jurisdictions. The overarching concept of the obligations applying to certain specified activities (as set out in paragraph 20) is considered to be common across all jurisdictions.

22. Some legal professionals and law firms may accordingly be able to conclude that based on the services they provide, they do not have any specific AML/CFT obligations as they do not prepare for, or carry out any of the specified activities. Even though specific AML/CFT obligations may not apply to a legal professional or a law firm, it is consistent with the overall ethics and best practices of the profession for all legal professionals to ensure that their services are not being misused, including by criminals. Accordingly, legal professionals and law firms should carefully consider what they need to do to guard against that risk irrespective of the application of specific AML/CFT obligations in order not to be unwittingly involved in ML/TF.

23. Legal professionals provide advisory services and representation to members of society, companies and other entities to

a) understand their increasingly complex legal rights and obligations;

b) facilitate business transactions;

c) assist their clients to comply with laws; and

d) provide access to justice and judicial redress.

24. They may provide these services alone, in collaboration with other independent legal professionals or as partners or as members of a law firm. A firm may consist of a sole practitioner or a few practitioners or thousands of legal professionals spread throughout numerous offices around the globe. There are also alternative business structures in which legal professionals combine with non-legal professionals to form partnerships. Most legal professionals practise alone or with other legal professionals in small firms.

25. Legal professionals include barristers, solicitors and other types of specialist advocates, however called. Typically, these legal professionals represent clients in court and also, in some countries, provide advisory services that might include one of the specified activities in R.22 and, as set forth above, they will therefore need to comply in respect of such services.

26. Services provided globally by legal professionals include advising on clients' financial transactions and legal structures that involve financial or business arrangements. As a result of their regulated status and to assist clients in transactions, legal professionals may also hold clients' funds in designated accounts or agree to act on behalf of clients (e.g. under a power of attorney) in relation to specific aspects of transactions. However, the counselling and advisory roles of legal professionals, especially in an increasing regional and global marketplace, do not generally involve handling funds. Legal professionals frequently work in collaboration with other professional advisors on transactions, such as accountants, TCSPs, escrow agents and title insurance companies and may refer their clients to particular professionals for services. Flows of funds are also often dealt with and facilitated exclusively by financial institutions.

27. The work of legal professionals is fundamental to promoting adherence to the rule of law. Legal professionals are typically regulated by laws, professional standards and codes of ethics and conduct. Breaches of the obligations imposed upon them can result in a variety of sanctions, including civil, contractual, disciplinary and criminal sanctions.

Legal professional privilege and professional secrecy

28. The actions and behaviours discussed in this Guidance are subject to applicable professional privilege and professional secrecy. Privilege/professional secrecy is a protection to the client, and a duty of the legal professional. Privilege (a common law concept existing in jurisdictions such as England and Wales and the United States) and professional secrecy (a civil law concept existing in jurisdictions such as Germany and France) aim to protect client information or advice from being disclosed. Though the two concepts differ in scope and purpose, both are founded on the nearly universal principle of the right of access to justice and the rationale that the rule of law is protected where clients are encouraged to communicate freely with their legal advisors without fear of disclosure or retribution. R.23 and the accompanying INR.23 recognise concepts of privilege and professional secrecy.

29. The degree and scope of legal professional privilege or professional secrecy and the consequences of a breach of these principles vary from one country to another and are determined by the relevant national laws.

30. In some jurisdictions, the protections against non-disclosure may be overridden by the consent or waiver of the client or by express provisions of law. Most jurisdictions seek to balance the right of access to justice and the public interest in investigating and prosecuting criminal activity. Accordingly, legal professional privilege or professional secrecy does not protect a legal professional from knowingly facilitating a client's illegal conduct.[8] Moreover, the protections against non-disclosure may not exist where the "crime/fraud" exception applies. Under the "crime/fraud" exception to privilege, privilege is not created where there is an illegal purpose whether or not the legal professional is aware of the illegality or is complicit in the illegality. The extent of that exception is a matter of national law.

31. Each country needs to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover some information that legal professionals receive from or obtain through their clients: (a) in the course of ascertaining the legal position of their clients, or (b) in performing their task of defending or representing their clients in, or concerning judicial, administrative, arbitration or mediation proceedings. There may be cases in which these professionals conduct activities that are clearly covered by the legal privilege (i.e. ascertaining the legal position of their client or defending or representing their client in judicial proceedings) alongside activities that may not be covered by it. In addition, within a single matter, privilege may attach to some but not all communications and advice.

32. A number of the DNFBP sectors, including legal professionals, are already subject to regulatory or professional requirements (including as promulgated by SRBs) that complement AML/CFT measures. For example, by virtue of their professional codes of conduct, many legal professionals are already subject to an obligation to identify their clients

[8] Also see IBA and the secretariat of the OECD: Report of the Task Force on the Role of Lawyers and International Commercial Structures (May 2019): Full Report and Executive Summary.

(e.g. to check for conflict of interest) and the substance of the matter submitted to them by such clients, to appreciate the consequences that their advice may have. If a legal professional provides legal advice to a client that helps the client commit an offence, that legal professional may, depending on the legal professional's state of knowledge, become an accomplice to the offence.

33. This Guidance must be considered in the context of these professional and ethical codes of conduct. In situations where legal professionals are claiming legal professional privilege or professional secrecy, they must be satisfied that the information is protected by the privilege/professional secrecy and the relevant rules. For example, it is important to distinguish between legal advice, which generally is subject to robust protections, and underlying facts, which in many cases are not protected by privilege.

Role of notaries as a legal professional

34. Both civil and common law countries have notaries, but the main difference between them is the roles that they play in their respective jurisdictions. In some common law countries, a notary public is a qualified, experienced practitioner, trained in the drafting and execution of legal documents. In other common law countries, a notary public is a public servant appointed by a governmental body to witness the signing of important documents (such as deeds and mortgages) and administer oaths. Notaries provide legal advice in the context of documenting transactions and legal arrangements, and do not necessarily direct this advice to a specific party. In some common law countries, such as the UK, the notary is no longer required for documenting transactions.

35. Most civil law notaries are members of autonomous legal professions (regulated by law) and qualified public officials, as they are appointed by the State through a selective public competition among law graduates. Civil law notaries, who are bound by an obligation of independence and impartiality with respect to parties to a transaction, must be regarded, in matters of real estate property (conveyancing), family law, inheritance and corporate legal services (e.g. the formation of companies, sale of shares, capital increases, liquidation and dissolution of companies), as practising non-adversarial activities. They act as gatekeepers by drafting and ensuring the legality and certainty of the instruments, and the authenticity of the content of the instrument and in some jurisdictions, also provide a public fiduciary function by performing the role of trusted third parties. Civil law notaries are obliged by law to remain impartial, fair and independent as between the parties they are advising, including bearing in mind any disparity of power between the parties. For this reason, civil law notaries are assigned functions of a public nature as part of their legal assignments and typically do not act for one of the parties in an advisory capacity.

36. In civil law jurisdictions, as notaries are entrusted with public functions, they act as public office holders in accordance with the principles of impartiality, legality, certainty and independence. In these jurisdictions, the involvement of notaries in transactions includes the notaries' responsibility and the specific legal value of the notarial form established by law. This legal framework for civil law notaries ensures a high degree of legal certainty and enhances the traceability and transparency of transactions between the parties. Notarial deeds as authentic instruments are recognised as a particular form of evidence, which is taken to be authoritative and in certain cases, as judicially enforceable as court orders and judgments and, sometimes, are an indispensable step in order to obtain other effects such as *traditio*, right of first refusal, third-party effectiveness and registration in substantive and administrative registries. State powers are therefore effectively delegated to civil law

notaries so that they can assign "public authority" to the authentic instruments they establish and are responsible for. The obligations of fairness and public office mean that services performed by civil law notaries are often very different in nature to the services provided by other legal professionals.

37. Notaries are subject to a duty of professional secrecy, as well as generally being subject to a duty to respect rights to confidentiality. Notaries are the party to interpret these duties in the light of their overarching obligation to ensure the common good and the general interests of society. Therefore, in practice, professional secrecy is not an absolute duty and is often subordinated to the public interest. Notaries may also be required to disclose the contents of their archives and communications in criminal proceedings or when required by law. In the context of ML/TF, notaries are obliged to co-operate with law enforcement, and to disclose all the relevant information to the competent authorities, in accordance with the laws of the jurisdiction. Notification to public authorities of any suspicious transactions should not be considered as an infringement of the notary's duty of professional secrecy. Information received by the civil law notaries in respect of a client and which is being transferred to the competent FIU in conformity with the AML/CFT legislation still remains confidential information.

38. This Guidance does not cover some common law notaries when those notaries perform merely administrative acts such as witnessing or authenticating documents, as these acts are not specified activities.

Services provided by legal professionals and their vulnerabilities for ML/TF

39. Legal professionals provide a vast range of services to a diverse range of clients. For example, services may include (but are not restricted to):

a) Advising on the purchase, sale, leasing and financing of real property;

b) Tax advice;

c) Advocacy before courts and tribunals;

d) Representing clients in disputes and mediations;

e) Advice in relation to divorce and custody proceedings;

f) Advice on the structuring of transactions;

g) Advisory services on regulations and compliance;

h) Advisory services related to insolvency/receiver-managers/bankruptcy;

i) Administration of estates and trusts;

j) Assisting in the formation of entities and trusts;

k) Trust and company services[9];

l) Acting as intermediaries in the trade of citizenship and residency or acting as advisors in residence and citizenship planning;

[9] For such activities, refer also to the guidance on risk-based approach for Trust and Company Service Providers (TCSPs).

m) Providing escrow services and token custody services in connection with legal transactions involving an initial coin offering or virtual assets;

n) Legitimising signatures by confirming the identity of the signatory (in the case of notaries); and

o) Overseeing the purchase of shares or other participations (also in the case of notaries).

40. While some of these services may involve activities that fall within the scope of the specified activities under R.22, not all (e.g. representing clients in disputes and mediations; providing advice in relation to divorce and custody proceedings; or providing advisory services on regulations) will do so. When considering the range of tasks undertaken by legal professionals only specified activities under R.22 are subject to the AML/CFT regime.

41. The specifics of the risk-based processes should accordingly be determined based on the activities undertaken by the legal professional, the ethical and existing supervisory structure for legal professionals and the susceptibility or vulnerability of activities of a legal professional to ML/TF. Firms with offices in multiple jurisdictions should apply a consistent approach across all of its offices with a general compliance tone from the top.

42. A RBA requires legal professionals to mitigate the risks that they face and with due regard to the resources available. Mitigating practices will invariably include initial CDD and ongoing monitoring, as well as a range of internal policies, training and systems to address the vulnerabilities faced in the particular practice setting of the legal professional. This section does not attempt to exhaustively list the mitigating practices that may be employed by legal professionals. For information on ways in which legal professionals might mitigate their vulnerabilities to ML/TF, see "Section 2 – Guidance for Legal professionals and Notaries" and chapters III and IV of the separate publication: "*A Lawyer's Guide to Detecting and Preventing Money Laundering*" published in October 2014 by a collaboration of the International Bar Association, American Bar Association and the Council of Bars and Law Societies of Europe[10].

Client funds

43. Most legal professionals can hold funds of clients. Client accounts are accounts held by legal professionals with a financial institution. In some civil law countries, a professional body holds the funds of clients, rather than legal professionals. For example, in France, where funds are held in CARPA (see Annex 4 "France"). Operating client accounts does not automatically require a legal professional to observe AML/CFT obligations. These obligations apply when the accounts are used in conjunction with a specified activity under R.22.

44. In most countries, legal professionals are required to hold client funds in a separate account with a financial institution and use the funds only in accordance with their client's instructions. In countries where client accounts are used, legal professionals are required to hold client funds separate from their own. The purpose of these accounts is to hold client funds in "trust" for or for a purpose designated by the client. Funds will also be

[10] The full publication is available at: www.ibanet.org/Article/NewDetail.aspx?ArticleUid=f272a49e-7941-42ee-aa02-eba0bde1f144

held or received for payment of costs incurred by the legal professional on behalf of the client. No funds may pass through a client account without being attached to an underlying legal transaction or purpose, and the legal professional is required to account for these funds.

45. The use of client accounts has been identified as a potential vulnerability, as it may be perceived by criminals as a means to either integrate tainted funds within the mainstream financial system or a means by which tainted funds may be layered in such a way to obscure their source, with fewer questions being asked by financial institutions because of the perceived respectability and legitimacy added by the involvement of the legal professional. Legal professionals can seek to limit their exposure to this risk by developing and implementing policies on the handling of funds (e.g. currency value limits) as well as restricting access to the account details of the client account in order to prevent unsanctioned deposits into the client account.

Advising on the purchase and sale of real property

46. Real estate, both commercial and residential, accounts for a high proportion of confiscated criminal assets, demonstrating that this as a clear area of vulnerability. In many countries, legal professionals are either required by law to undertake the transfer of property or their involvement is a matter of tradition, custom or practice. However, the specific role of legal professionals in real estate transactions varies significantly from country to country, or even within countries. In some countries, legal professionals will customarily hold or control (e.g. through a financial institution) and transfer or control the transfer of the relevant funds for the purchase of the real estate assets. In other countries this will be done by other parties, such as a title insurance company or escrow agent. Even if legal professionals are not handling the funds, they will typically be aware of the financial details and in many cases will be in a position to inquire about the transaction where appropriate.

47. Some criminals may seek to invest the proceeds of their crime in real estate without attempting to obscure their ownership of the real estate. Alternatively, criminals may seek to obscure the ownership of real property by using false identities or title the property in the names of family members, friends or business associates, or purchase property through an entity or a trust. Legal professionals should consider carefully who they are acting for at the outset of a real estate transaction, especially where there are multiple parties involved in a transaction. In some cases, legal professionals may also opt to apply specific checks on the settlement destinations of transactions (i.e. performing limited diligence on the seller of real property, when acting for the buyer and the seller and the buyer appear to be related parties).

Formation of companies and trusts[11]

48. In some countries, legal professionals (in civil law jurisdictions this will usually be a notary) must be involved in the formation of a company. In other countries members of the public are able to register a company themselves directly with the company register, in which case a legal professional's advice is sometimes sought at least in relation to initial liability management, corporate, tax and administrative matters.

49. Criminals may seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of

[11] The illustrations could also apply to other legal persons and arrangements.

the assets. Companies and often trust and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies[12], which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy. Criminals may also seek to misuse shelf companies[13] formed by legal professionals by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be in an attempt to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

Management of companies and trusts

50. In some cases, criminals will seek to have legal professionals involved in the management of companies and trusts in order to provide greater respectability and legitimacy to the company or trust and its activities. In some countries professional rules preclude a legal professional from acting as a trustee or as a company director, or require a disclosure of directorship positions to ensure independence and transparency is maintained. In countries where this is permitted, there are diverse rules as to whether that legal professional can also provide external legal advice or otherwise act for the company or trust. This will determine whether any funds relating to activities by the company or trust can go through the relevant legal professional's client account. In addition, in some countries, the non-legal counsel of a legal professional acting in a business capacity for formation or management of companies or trusts may not be protected by the legal professional privilege.

Acting as nominee

51. Individuals may sometimes have legal professionals or other persons hold their shares as nominees, where there are legitimate privacy, safety or commercial concerns. However, criminals may also use nominee shareholders to obscure their ownership of assets. In some countries, legal professionals are not permitted to hold shares in entities for whom they provide advice, while in other countries legal professionals regularly act as nominees. Legal professionals should identify beneficial owners when establishing business relations in these situations. This is important to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess and mitigate the potential ML/TF risks associated with the business relationship. Where legal professionals are asked to act as nominees, they should understand the reason for this request and ensure that they are able to verify the identity of the beneficial owner of the shares and that the purpose is legitimate.

General management of client affairs

52. In some jurisdictions, legal professionals may undertake a range of 'management' activities for clients permitted in limited circumstances by some professional rules. In some European jurisdictions, this is sometimes referred to as 'man of affairs work'.

---

[12] A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.

[13] A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established.

Situations where a legal professional may be undertaking these activities legitimately may involve a client who has limited capacity to manage his/her own affairs, or in other circumstances where the client has a clear legitimate rationale for seeking the continuing assistance from the legal professional. The legal professional, whether acting pursuant to a court order or a power of attorney, may use his/her client account to undertake transactions, but would more typically use accounts held by the client for whom the legal professional is acting. While ordinarily this type of activity should give the legal professional access to sufficient information to make considered assessments of a client's legitimacy under a RBA, it is possible that criminals will seek to use such ancillary services, in addition to legal services, to minimize the number of advisors and third parties who have access to the client's financial and organizational details. Legal professionals should carefully scrutinize any request to take on additional obligations for a client beyond their primary services and consider the justification of such a request in the totality of the circumstances and its overall legitimacy.

Other services that might indicate ML/TF activity

53. Legal professionals possess a range of specialised legal skills that may be of interest to criminals, in order to enable them to transfer value obtained from criminal activity between parties and obscure ownership. These specialised skills include the creation of financial instruments and arrangements, advice on and drafting of contractual arrangements, and the creation of powers of attorney. In other areas of legal specialisation, such as probate (succession) and insolvency or bankruptcy work, the legal professional may simply encounter information giving rise to a suspicion that the deceased or insolvent individual previously engaged in criminal activity or that parties may be hiding assets to avoid payment to legitimate creditors. Countries differ on how unexpected funds are treated in relation to probate or insolvency cases, in some, a threshold report will be made and the government becomes a super-creditor able to recover the money before any other beneficiary or creditor. Where these circumstances involve legal professionals engaging in a specified activity, legal professionals must carefully consider their AML/CFT obligations. Legal professionals should also consider the ML/TF risk in such circumstances.

54. Many aspects of this Guidance on applying a RBA to AML/CFT may also apply in the context of predicate offences, particularly for other financial crimes such as tax crimes. The ability to apply a RBA effectively to relevant predicate offences will also reinforce the AML/CFT obligations. Legal professionals may also have specific obligations in respect of identifying risks of predicate offences such as tax crimes, and supervisors may have a role to play in oversight and enforcement against those crimes. Therefore, in addition to this Guidance, legal professionals and supervisors should have regard to other sources of guidance that may be relevant in managing the risks of predicate offences.[14]

[14] For example, legal professionals may be subject to mandatory disclosure rules, requiring them to report arrangements that have the hallmarks of tax evasion to the tax authority. Legal professionals may also commit an offence where they facilitate the commission of tax evasion. These initiatives require legal professionals and supervisors to take many of the steps outlined in this Guidance to ensure they fulfil their obligations under applicable law.

Services performed by notaries

Overseeing the purchase of shares or other participations

55. Notaries are often involved in reviewing the documentation for the transfer of shares and/or for transactions that enable participation in a company's equity. It is possible for criminals to use fictitious or misleading accounting methods to distort the apparent value of a company, including by diminishing it in order to hide or obscure transfers of value. Although a notary is generally not responsible for verifying the 'true' value of companies, notaries may encounter information in the course of their duties that is at odds with the presented valuation of a company.

Legitimisation of identities of signatory

56. In certain situations, the intervention of a notary is required to legitimise the execution of a private document. Although this technically relates only to verifying the identity of the signing parties, notarisation can often lend an impression of credibility to the content of the document. Criminals may use this form of notarisation service to lend credibility, in particular, to information contained in such documents that asserts the identity of the owners of assets, thereby potentially hiding its true owners.

Legalisation of old documents

57. In certain situations, the intervention of a notary is required for the legalisation of private documents drafted several years before the time of notarisation. The purpose of this service is to provide certainty in relation to the validity of old documents. Criminals may seek to use such services in relation to documents that falsely assert that transactions occurred many years ago, in circumstances that cannot otherwise be verified.

Opening of safe deposit boxes

58. Notaries may be present at the opening of a safe deposit box held at a bank that is opened in the name of a deceased person. This service is to certify the contents of the safe deposit box. Criminals may fraudulently place contents that were not the property of the deceased person in such a deposit box in order to ensure that the title to this property passes in an apparently legitimate and 'clean' transfer from the estate of the deceased to the same criminal enterprise as the beneficiaries of the estates.

FATF Recommendations applicable to the legal professionals

59. The basic intent behind the FATF Recommendations as it relates to legal professionals is to ensure that their operations and services are not abused for facilitating criminal activities and ML/TF. This is consistent with the role of legal professionals, as guardians of justice and the rule of law namely to avoid knowingly assisting criminals or facilitating criminal activity. The requirements of R.22 regarding CDD, record-keeping, PEPs, new technologies and reliance on third parties set out in R.10, 11, 12, 15 and 17 should apply to legal professionals in certain circumstances.

60. R.22 mandates that the requirements for CDD, record-keeping, PEPs, new technologies and reliance on third parties set out in R. 10, 11, 12, 15 and 17 apply to legal professionals in certain circumstances. R.22 applies to legal professionals when they prepare

for and carry out certain specified activities. Unless legal advice and representation consist of preparing for or carrying out one or more of these specified activities, legal professionals are not subject to the FATF Recommendations. This Guidance has been prepared to assist in situations where legal professionals prepare for and carry out transactions for the clients concerning the specified activities. For example, FATF Recommendations would not be applicable if a legal professional only provides litigation advice or routine advice at legal aid or other legal help clinics.

61. Where more than one law firm or legal professional prepares for or carries out a transaction, each firm or legal professional must comply with the applicable CDD, record-keeping and other AML/CFT obligations. Where permitted, legal professionals may rely on third parties in accordance with R.17 to perform elements (a)-(c) of the CDD measures set out in R.10 or to introduce business. Where not all legal professionals are preparing for or carrying out the transaction, those legal professionals providing advice or services (e.g. a general legal opinion on the applicability of a local law) peripheral to the transaction need not be subject to the AML/CFT obligations.

62. R.23 requires that measures set out in R.18 (Internal controls and foreign branches and subsidiaries), 19 (Higher-risk countries), 20 (reporting of suspicious transactions) and 21(tipping-off and confidentiality) should apply to legal professionals subject to certain qualifications.

63. R.23 applies to legal professionals when they engage in a financial transaction on behalf of a client, in relation to the specified activities under R.22. If legal professionals suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to TF, they should be required to promptly report their suspicions to the FIU. Subject to certain limitations, legal professionals are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege, as recognised by INR.23. The lawyer-client relationship is protected in many countries, including in some instances by constitutional provisions.

64. The FATF Recommendations set the international standards on combating ML and the financing of terrorism and proliferation, which jurisdictions implement taking into consideration their national context including their legal framework. In general terms jurisdictions have closely followed the FATF Recommendations but differences do exist and legal professionals need to carefully consider these differences in their own jurisdictions. The overarching concept of the obligations only applying to certain specified activities is common across all jurisdictions. Section III provides further guidance on the application of obligations in R.22 and R.23 to legal professionals.

65. Even though individual legal professionals or law firms may be able to conclude that specific AML/CFT obligations do not apply to them, ethical standards require them to ensure that their services are not being misused, including by criminals, and they should carefully consider what they need to do to guard against that risk.

66. Countries should establish the most appropriate regime, tailored to address relevant ML/TF risks, which takes into consideration the activities and applicable code of conduct for legal professionals.

Section II- The RBA to AML/CFT

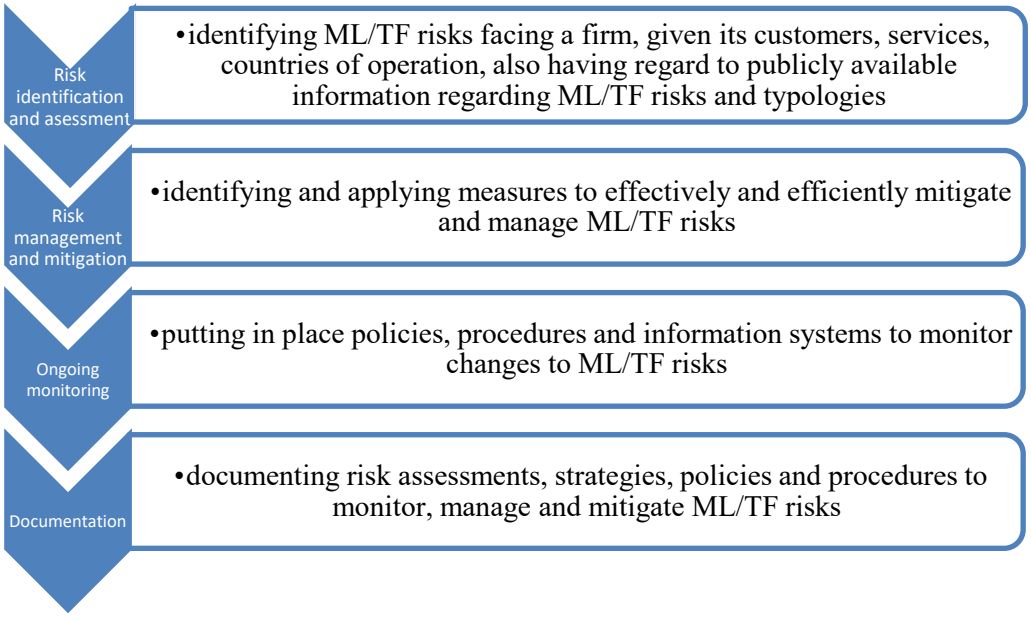
What is the RBA?

67. The RBA to AML/CFT means that countries, competent authorities and DNFBPs, including lawyers, notaries and other legal professionals should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures effectively and efficiently to mitigate and manage the risks.

68. For legal professionals, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions where they operate, and the effectiveness of their controls in place, will require the investment of resources and training. For supervisors, this will also require maintaining an understanding of the ML/TF risks specific to their area of supervision and the degree to which AML/CFT measures can reasonably be expected to mitigate such risks.

69. The RBA is not a "zero failure" approach; there may be occasions where a legal professional has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks, but is still used for ML/TF in isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that legal professionals must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

70. Key elements of a RBA can be summarised as follows:



The rationale for the RBA

71. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards. Its purposes remain to protect the integrity of the financial system by providing governments with updated tools needed to take action against financial crime.

72. There was an increased emphasis on the RBA to AML/CFT, especially in preventive measures and supervision. Though the 2003 Recommendations provided for the

application of a RBA in some areas, the 2012 Recommendations considered the RBA to be an essential foundation of a country's AML/CFT framework.[15]

73. The RBA allows countries, within the framework of the FATF Recommendations, to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are reasonable and proportionate to the nature of risks.

74. The application of a RBA is therefore essential for the effective implementation of the FATF Standards by countries and legal professionals.[16]

Application of the RBA

75. The FATF standards do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF. The overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of factors, including services, products, customers, geography, preventive measures and the strength of the entity's compliance program.

76. R.1 sets out the scope of application of the RBA as follows:

a) **Who should be subject to a country's AML/CFT regime?**
   - In addition to the sectors and activities already included in the scope of the FATF Recommendations[17], countries should extend their regime to additional institutions, sectors or activities if they pose a higher ML/TF risk. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.[18]

b) **How should those subject to the AML/CFT regime be supervised or monitored for compliance with this regime**
   - Supervisors should ensure that legal professionals are implementing their obligations under R.1. AML/CFT supervisors should consider a legal professional's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA.

c) **How should those subject to the AML/CFT regime be required to comply**
   - The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls

15 R.1.

16 The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take into account the risks and the flexibility allowed by the RBA, when determining whether there are deficiencies in a country's AML/CFT measures, and their importance *(FATF, 2013f).*

17 See FATF Glossary, definitions of "Designated non-financial businesses and professions" and "Financial institutions".

18 See INR.1.

conducted should be stronger in higher risk scenarios. Legal professionals are required to apply each of the following CDD measures[19]: (i) identification and verification of the client's identity; (ii) identification of the beneficial owner and taking reasonable measures to verify the identity of beneficial owner; (iii) understanding the purpose and nature of the business relationship; and (iv) on-going due diligence on the relationship. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

d) **Consideration of the engagement in client relationships**
   - Legal professionals are not obliged to avoid risk entirely. Even if the services they provide to their clients are considered vulnerable to ML/TF risks based on risk assessment, it does not mean that all legal professionals and all their clients or services pose a higher risk when taking into account the risk mitigating measures that have been put in place.

e) **Importance of legal professional services to overall economy**
   - Legal professionals often play significant roles in the legal and economic life of a country. The role of legal professionals in supporting the negotiation of business and other agreements is vital. The risks associated with any type of client group are not static and the expectation is that within a client group, based on a variety of factors, individual clients could also be classified into risk categories, such as low, medium-low, medium, medium-high or high risk (see section 3.1 below for a detailed description). Measures to mitigate risk should be applied accordingly.

Challenges

77. Implementing a RBA can present a number of challenges for legal professionals. A RBA requires resources and expertise, both at a country and sector level, to gather and interpret information on risks, to develop policies and procedures and to train personnel. A RBA is also reliant on individuals exercising sound and well-trained judgement when designing and implementing such policies and procedures.

Box 1. Particular RBA challenges for legal professionals

Culture of compliance and adequate resources. Implementing a RBA requires that legal professionals have a sound understanding of the ML/TF risks and are able to exercise good professional judgement. Above all, legal professionals and the leadership of law firms should recognise the importance of a culture of compliance across the organisation and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of the organisation. This requires the building of expertise including, for example, through training, recruitment, taking professional advice and 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on ML/TF risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making. The process will

[19] See R.10

benefit from information sharing by relevant competent authorities, supervisors and SRBs. The provision of good practice guidance by competent authorities, supervisors, legal professionals and SRBs is valuable and encouraged.

Significant variation in services and clients. Legal professionals will vary substantially in the breadth and nature of services provided and the clients they serve, as well as the size, focus, geographic reach and sophistication of the firm and its employees. In implementing the RBA, legal professionals should make reasonable judgements for their particular services and activities. This may mean that no two legal professionals and no two firms are likely to adopt the same detailed practices. Legal professionals should thus tailor their RBA based on their unique characteristics and practice profile.

Appropriate mitigation measures will also depend on the nature of the legal professional's role and involvement. Circumstances may vary considerably between professionals who represent clients directly and those who are engaged for distinct purposes. Where these services involve tax laws and regulations, legal professionals also have additional considerations related to a country's or jurisdiction's permissible means to structure transactions and entities or operations to legally avoid and/or minimise taxes.

Transparency of beneficial ownership on legal persons and arrangements. Legal professionals can be involved in the formation, management, or administration of legal entities and arrangements, though in many countries any legal or natural person may be able to perform these activities. Where legal professionals do play this "gatekeeper" role, they may encounter challenges in keeping current and accurate beneficial ownership information depending upon the nature and activities of their client. Other challenges may arise when on-boarding new clients with minimal economic activity associated with the legal entity and/or its owners, controlling persons, or beneficial owners, established in another jurisdiction. Finally, whether the source is a public registry, another third party source, or the client, there is always potential risk in the correctness of the information, in particular where the underlying information has been provided by the client.[20] Those risks notwithstanding from the outset the legal professional should seek answers from the immediate client in determining beneficial ownership (having first determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the client is a publicly listed company). The information provided by the client should then be appropriately confirmed by reference to public registers and other third party sources where possible. This may require further and clarifying questions to be put to the immediate client. The goal is to ensure that the legal professional is reasonably satisfied about the identity of the beneficial owner. For more practical guidance on beneficial ownership, refer to the guidance in Box 2.

[20] For further information legal professionals can refer to the FATF Guidance on Transparency and Beneficial Ownership.

Risk of criminality. Although the implementation of a RBA should not impair a client's right of access to justice, legal professionals and their firms must be alert to ML/TF risks posed by the services they provide to avoid the possibility that they may unwittingly commit or become an accessory to the commission of a substantive offence of ML/TF. There have been examples of unwitting involvement of or negligence on the part of legal professionals or complicit professionals intentionally enabling the laundering of proceeds of crime. Legal professionals and firms should protect themselves from misuse by criminals and terrorists. This may include restricting the method and source of payments (e.g. cash payments above a monetary threshold, unexplained third party payments) for the services being provided, dictating greater focus on monitoring and reporting of clients and their funds for unusual or suspicious activity.

Interplay between the requirement to comply with AML/CFT obligations and the principle of legal professional privilege and professional secrecy as applicable. Where legal professional privilege does apply, many countries provide exceptions in law that allow legal professionals to make disclosures of suspicion of ML/TF without incurring penalties or liability or breaching ethical obligations and in others to provide an exception to disclosure if the information is directly encompassed by a legitimate claim of privilege. However, legal professionals may be cautious of making disclosures that would otherwise breach privilege or confidentiality rules due to uncertainties in the application of these exceptions, lack of adequate information or training in relation to these rules, the complexities of their clients' situations or a combination of these factors. Criminals may misperceive that legal professional privilege and professional secrecy will delay, obstruct or prevent investigation or prosecution by authorities if they utilise the services of a legal professional. Criminals may also seek out legal professionals (over other non-legal professions) to perform the services listed in R.22 with the specific criminal intent of concealing their activities and identity from authorities through professional privilege/secrecy protections.

Allocating responsibility under a RBA

78. An effective risk-based regime builds on and reflects a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector and its risk profile. Legal professional should identify and assess their own ML/TF risk taking account of the NRAs in line with R.1, as well as the national legal and regulatory framework, including any areas of prescribed significant risk and mitigation measures. Legal professionals are required to take appropriate steps to identify and assess their ML/TF risks and have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.[21] Where ML/TF risks are higher, legal professionals should always apply enhanced CDD, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g. varying the degree of enhanced ongoing monitoring).

79. Strategies adopted by legal professionals to mitigate ML/TF risks should take into account the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which legal professionals can take measures to mitigate risk, countries should consider the ability of the sector to effectively identify and manage ML/TF risks as well as the expertise and resources of their supervisors to adequately supervise and take action to address any failures. Countries may also consider evidence from competent authorities on the level of compliance in the sector, and the sector's approach to dealing with ML/TF risk. Countries whose services sectors are emerging or whose legal and supervisory frameworks are still developing may determine that legal professionals are not fully equipped to effectively identify and manage ML/TF risk. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until the understanding and experience of the sector is strengthened.[22]

80. Legal professionals should not be exempted from AML/CFT supervision even where their compliance controls are adequate. However, the RBA allows competent authorities to focus more supervisory resources on higher risk entities.

Identifying ML/TF risk

81. Access to accurate, timely and objective information on ML/TF risks is essential for an effective RBA. INR.1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, financial institutions and legal professionals. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share relevant information on ML/TF risks and threats, or where access to information is restricted by censorship or data protection provisions, it will be difficult for legal professionals to correctly identify ML/TF risk.

82. R.34 requires competent authorities, supervisors and SRBs to establish guidelines and provide feedback to financial institutions and DNFBPs. Such guidelines and feedback help institutions and businesses to identify the ML/TF risks and to adjust their risk mitigating programmes accordingly.

---

21 R.1 and IN.1.

22 This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or Financial Sector Assessment Program (FSAP) evaluations.

Assessing ML/TF risk

83. Assessing ML/TF risk requires countries, competent authorities and legal professionals to determine how the ML/TF threats identified will affect them. They should analyse the information to understand the likelihood of these risks occurring, and the impact that these would have, on the individual legal professionals, the entire sector and on the national economy. As a starting step, ML/TF risks are often classified as low, medium-low, medium, medium-high and high. Assessing ML/TF risk goes beyond the mere gathering of quantitative and qualitative information, without its proper analysis; this information forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.[23]

84. Competent authorities, including supervisors and SRBs should employ skilled and trusted personnel, recruited through fit and proper tests, where appropriate. They should be technically equipped commensurate with the complexity of their responsibilities. Legal professionals and law firms that are required to routinely conduct a high volume of enquiries when on-boarding clients, e.g. because of the size and geographic footprint of the firm, may also consider engaging skilled and trusted personnel who are appropriately recruited and checked. Such law firms are also likely to consider using the various technological options (including artificial intelligence) and software programs that are now available to assist law firms in this regard.

85. Law firms should develop internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees. Law firms should also develop an ongoing employee training programme. They should be trained commensurate with the complexity of their responsibilities.

Mitigating and managing ML/TF risk

86. The FATF recommendations require that when applying a RBA, legal professionals should appropriately mitigate and manage the risks that they identify. Mitigating practices will invariably include initial and ongoing CDD, internal policies, training, and procedures to address the vulnerabilities faced in the legal professional's particular context. Legal professional should take enhanced measures to manage the ML/TF risks identified. This section does not attempt to exhaustively list the mitigating practices that may be employed by legal professionals. Instead, it provides select examples to illustrate how legal professionals might choose to address particular risks under the RBA.[24]

87. The FATF Recommendations require that, when applying a RBA, legal professionals, countries, competent authorities and SRBs decide on the most appropriate and

---

[23] FATF (2013a), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk. Also refer to The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013).

[24] For information on ways in which legal professionals might mitigate their ML/TF vulnerabilities, see Section 2 of this Guidance and chapters III and IV of the separate publication: "A Lawyer's Guide to Detecting and Preventing Money Laundering" published in October 2014 by a collaboration of the International Bar Association, American Bar Association and the Council of Bars and Law Societies of Europe.

effective way to mitigate the ML/TF risk they have identified. They should take enhanced measures to manage and mitigate situations when the ML/TF risk is higher. In lower risk situations, less stringent measures may be applied:[25]

a) Countries may decide not to apply some of the FATF Recommendations requiring DNFBPs to take certain actions, provided (i) there is a proven low risk of money laundering and terrorist financing, this occurs in strictly limited and justified circumstances and it relates to a particular type of DNFBP or (ii) a financial activity is carried out by a natural or legal person on an occasional or very limited basis such that there is a low risk of ML/TF, according to the exemptions of INR 1.6.

b) Countries looking to apply simplified measures should conduct an assessment to ascertain the lower risk connected to the category of clients or services, establish a threshold for the lower level of the risks involved, and define the extent and the intensity of the required AML/CFT measures, provided that the specific conditions required for one of the exemptions of INR 1.6 are met. Specific Recommendations set out in more detail how this general principle applies to particular requirements.[26]

Developing a common understanding of the RBA

88. The effectiveness of a RBA depends on a common understanding by competent authorities and legal professionals of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, legal professionals should deal with the risks they identify. Following a consultative process, competent authorities should issue RBA guidance to legal professionals on meeting and managing their legal and regulatory AML/CFT obligations. Supporting ongoing and effective communication between competent authorities and legal professionals is essential.

89. Competent authorities should acknowledge that not all legal professionals will adopt identical AML/CFT controls in a risk-based regime. On the other hand, legal professionals should understand that a RBA does not exempt them from applying effective AML/CFT controls.

25. Subject to the national legal framework providing for Simplified CDD.
26 For example, R.22 on CDD.

Section III – Guidance for legal professionals

Risk identification and assessment

90. Potential ML/TF risks faced by legal professionals will vary according to many factors including the activities undertaken by them, the type and identity of the client, and the nature and origin of the client relationship. When applying the RBA, legal professionals and firms should bear in mind that specified activities have been found to be more susceptible to ML/TF activities because they involve the movement or management of client assets; this susceptibility may be heightened when these activities are conducted on a cross-border basis. These specified activities include:

a) buying and selling of real estate;

b) managing of client money, securities or other assets;

c) management of bank, savings or securities accounts;

d) organisation of contributions for the creation, operation or management of companies; and

e) creating, operating or management of legal persons or arrangements and buying and selling of business entities.

91. Although a client's right of access to advice and justice should not be adversely affected by the implementation of the RBA, legal professionals and their firms must remain alert to ML/TF risks posed by the services they provide to avoid unwittingly committing or becoming an accessory to the commission of a ML/TF offence. Legal professionals and law firms must protect themselves from unwitting involvement in ML/TF; such involvement not only presents reputational risk to the individuals concerned, the law firm and the legal profession at large, it is also unacceptable for the legal profession to allow itself to be misused by criminals.

92. Legal professionals should perform a risk assessment of the client at the inception of a client relationship. Such risk assessment may well be informed by findings of the NRA, the supra-national risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in legal services/sector, risk reports in other jurisdictions where the legal professional is based, and any other information which may be relevant to assess the risk level particular to their legal practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Legal professionals may also draw references to FATF Guidance on indicators and risk factors[27]. During the course of a client relationship, procedures for ongoing monitoring and review of the client/transactional risk profile are also important. Competent authorities should consider how they can best alert legal professionals to the findings of any national risk assessments, the supra-national risk assessments and any other information that may be relevant to assess the risk level particular to a legal practice in the relevant country.

93. Due to the nature of services that a legal professional generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most legal professionals. The legal professional's knowledge of the client

[27] FATF Report on Vulnerabilities in the Legal Sector (2013), Chapters 4 and 5.

and its business will develop throughout the duration of a longer term and interactive professional relationship (in some cases, such relationships may exist for short term clients as well, e.g. for property transactions). Although individual legal professionals are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of the business relationship. Legal professionals should consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be low risk (e.g. one-off client relationship involving simple transactions). Legal professionals should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

94. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow legal professionals to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the legal professional's role and involvement. Circumstances may vary considerably between professionals who represent clients in a single transaction, those involved in a long term advisory relationship and those who are engaged for distinct and discrete purposes including, for example, civil law notaries and local counsel engaged in a specific jurisdiction within a transaction.

95. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. A legal professional may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB or other credible sources (including a referring legal professional).

96. Legal professionals may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling legal professionals, where required, to subject each client to reasonable and proportionate risk assessment.

97. The most commonly-used risk categories are:

a) country or geographic risk;

b) client risk; and

c) risk associated with the particular service offered.

98. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the legal professional and/or law firm. These criteria, however, should be considered holistically and not in isolation. Legal professionals, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

99. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller law firms and sole practitioners, it is advisable to look at the services they offer (e.g. providing company management services may entail greater risk than other services).

100. Criminals deploy a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common

mechanisms/techniques have been compiled by FATF in the previous studies, including the 2014 FATF Guidance on Transparency and Beneficial Ownership and the 2018 Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership. Legal professionals may refer to the studies for more details on the use of obscuring techniques and relevant case studies.

101. A practical starting point for law firms (especially smaller firms) and legal professionals (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

a) **Client acceptance and know your client policies**: identify the client and its beneficial owners and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of wealth of the client where required, its owners and the purpose of the transaction.

b) **Engagement acceptance policies:** understand the nature of the work. Legal professionals should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where a legal professional does not have the requisite expertise, the legal professional should not undertake the work.

c) **Understand the commercial or personal rationale for the work:** legal professionals need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. Legal professionals however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.

d) **Be attentive to red flag indicators:** exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. Subject to qualifications set forth in this Guidance, these cases would trigger reporting obligations. Documenting the thought process may be a viable option to assist in interpreting/assessing red flags/indicators of suspicion.

e) **Then consider what action, if any, needs to be taken and have an action plan:** the outcomes of the above action (i.e. the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures (including evidence of source of wealth or funds).

f) **Documentation:** legal professionals should adequately document and record steps taken under a) to e).

Country/Geographic risk

102. There is no universally agreed definition by competent authorities, SRBs or legal professionals that prescribes whether a particular country or geographic area (including the country within which the legal professional practices) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information on ML/TF risks. Geographic risks of ML/TF may arise in a variety of circumstances, including from the

domicile of the client, the location of the transaction or the source of the wealth or funds. Factors that are generally agreed to place a country in a higher risk category include:

a) Countries/areas identified by credible sources[28] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

b) Countries identified by credible sources as having significant levels of organised crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.

c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations.

d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.

   Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.[29]

Client risk

103. Determining the potential ML/TF risks posed by a client or category of clients is critical to the development and implementation of an overall risk-based framework. Based on their own criteria, law firms and legal professionals should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of clients whose activities may indicate a higher risk include:

a) PEPs and persons closely associated with or related to PEPs, are considered as higher risk clients (Please refer to the FATF Guidance (2013) on PEPs for further guidance on how to identify PEPs).

---

[28] "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

[29] www.oecd-ilibrary.org/taxation/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews_2219469x

Box 2. Particular considerations for PEPs and source of funds and wealth

If a legal professional is advising a PEP client, or where a PEP is the beneficial owner of assets in a transaction, appropriate enhanced CDD is required if a specified activity under R.22 is involved. Such measures include, obtaining senior management (e.g. senior partner, managing partner or executive partner) approval before establishing a business relationship, taking reasonable measures to establish the source of wealth and source of funds of clients and beneficial owners identified as PEPs, and conducting enhanced ongoing monitoring on that relationship.

The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust). Source of funds relates directly to the economic origin of funds to be used in a transaction. This is likely to be received via a bank account. Generally, this would be evidenced by bank statements or similar documentation showing from where funds in an account originated such as receipt of salary. Source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). Source of wealth is the origin of the accrued body of wealth of an individual. Understanding source of wealth is about taking reasonable steps, commensurate with risk to be satisfied that the funds to be used in a transaction appear to come from a legitimate source.

While source of funds and wealth may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, legal professionals should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is reasonable and proportionate to the risk profile of the client.

Relevant factors that influence the extent and nature of CDD include the particular circumstances of a PEP, PEPs separate business interests and the time those interests prevailed in relation to the public position, whether the PEP has access to official funds, makes decisions regarding the allocation of public funds or public procurement contracts, the PEP's home country, the type of activity that the PEP is instructing the legal professional to perform or carry out, whether the PEP is domestic or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

If a PEP is otherwise involved with a client, then the nature of the risk should be considered in light of all relevant circumstances, such as:

a) the nature of the relationship between the client and the PEP: If the client is a trust, company or legal entity, even if the PEP is not a natural person exercising effective control or the PEP is merely a discretionary

beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.

b) the nature of the client (e.g. where it is a public listed company or regulated entity who is subject to and regulated for a full range of AML/CFT requirements consistent with FATF Recommendations, the fact that it is subject to reporting obligations will be a relevant factor.

c) the nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate consideration. Higher risks may exist where a legal professional is involved in the movement or transfer of funds/assets, or the purchase of high value property or assets.

b) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).

c) Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:

   i. Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee and corporate directors, legal persons or legal arrangements, splitting company formation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.

   ii. Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.

   iii. Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities or other factors are not consistent with the legal professionals' understanding of the client's business and economic purpose.

d) Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.

e) Clients that are cash (and/or cash equivalent) intensive businesses. Where such clients are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations, this will aid to mitigate the risks. These may include, for example:

   i. Money or Value Transfer Services (MVTS) businesses (e.g. remittance houses, currency exchange houses, casas de cambio, centros cambiarios, remisores de fondos, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities).

ii. Operators, brokers and others providing services in virtual assets.

iii. Casinos, betting houses and other gambling related institutions and activities.

iv. Dealers in precious metals and stones.

f) Businesses that while not normally cash intensive appear to have substantial amounts of cash.

g) Businesses that rely heavily on new technologies (e.g. online trading platform) may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.

h) Non-profit or charitable organizations engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

i) Clients using financial intermediaries, financial institutions or legal professionals that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or SRBs.

j) Clients who appear to be acting on somebody else's instructions without disclosing the identity of such person.

k) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected.

l) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for the legal professionals to perform a proper risk assessment.

m) Clients with previous convictions for crimes that generated proceeds, who instruct legal professionals (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.

n) Clients who have no address, or who have multiple addresses without legitimate reasons.

o) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).

p) Clients who change their settlement or execution instructions without appropriate explanation.

q) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.

r) Clients who insist, without reasonable explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.

s) Clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where legal professionals may receive a significant premium for a successful representation, should not be considered a risk factor.

t) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.

u) Where there are certain transactions, structures, geographical location, international activities or other factors that are not consistent with the legal professional's understanding of the client's business or economic situation.

v) The legal professional's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent[30].

w) Clients who apply for residence rights or citizenship in a jurisdiction in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in that jurisdiction.

x) Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions.

y) The relationship between employee numbers/structure and nature of the business is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets compared to similar businesses).

z) Client seeking advice or implementation of an arrangement that has indicators of a tax evasion purpose, whether identified as the client's express purpose, in connection with a known tax evasion scheme or based on other indicators from the nature of the transaction.

aa) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies that might be used to obscure beneficial ownership.

bb) Sudden activity from a previously dormant client without clear explanation.

cc) Client that start or develop an enterprise with unexpected profile or abnormal business cycles or client that enters into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.

[30] See the FATF Report on Money Laundering and Terrorist Financing: Vulnerabilities of Legal Professionals (June 2013).

dd) Indicators that client does not wish to obtain necessary governmental approvals/filings.

ee) Reason for client choosing the firm is unclear, given the firm's size, location or specialisation.

ff) Frequent or unexplained change of client's professional adviser(s) or members of management.

gg) The client is reluctant to provide all the relevant information or legal professionals have reasonable suspicion that the provided information is incorrect or insufficient.

hh) Clients seeking to obtain residents rights or citizenship in the country of establishment of the legal professional, in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.

Transaction/Service risk

104. An overall risk assessment of a client should also include determining the potential risks presented by the services offered by a legal professional, given the nature of such services, noting that legal professionals provide a broad and diverse range of services. The context of the services being offered or delivered is always fundamental to a RBA. Any one of the factors discussed in this Guidance alone may not itself constitute a high-risk circumstance but the factors should be considered cumulatively and holistically. When determining the risks associated with the provision of services related to specified activities, consideration and appropriate weight should be given to such factors as:

a) Services where legal professionals, effectively acting as financial intermediaries, handle the receipt and transmission of funds through accounts they control in the act of facilitating a business transaction.

b) Services that allow clients to deposit/transfer funds through the legal professional's trust account that are not tied to a transaction for which the legal professional is performing or carrying out activities specified in R.22.

c) Services where the client may request financial transactions to occur outside of the legal professional's trust account (the account held by the legal professional for the client) (e.g. through the firm's general account and/or a personal or business account held by the legal professional himself/herself).

d) Services where legal professionals may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.

e) Services that are capable of concealing beneficial ownership from competent authorities.[31]

[31] For further details on the difficulties presented by arrangements which conceal beneficial ownership see joint FATF and Egmont group report "Vulnerabilities Linked to the Concealment of Beneficial Ownership" published in July 2018.

f) Services requested by the client for which the legal professional does not have expertise excepting where the legal professional is referring the request to an appropriately trained professional for advice.

g) Services that rely heavily on new technologies (e.g. in relation to initial coin offerings or virtual assets) that may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.

h) Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.[32]

i) Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment.

j) Transactions where it is readily apparent to the legal professional that there is inadequate consideration, especially where the client does not provide legitimate reasons for the amount of the consideration.

k) Administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted of proceeds generating crimes.

l) The use of shell companies, companies with ownership through nominee shares or bearer shares and control through nominee and corporate directors without apparent legal, tax, business, economic or other legitimate reason.[33]

m) Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose (including changes of name/corporate seat or on establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.[34]

n) Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal under the circumstances and in the experience of the legal professional.

o) Settlement of default judgments or alternative dispute resolutions is made in an atypical manner (e.g. if satisfaction of a settlement or judgment debt is made too readily).

---

[32] See the FATF Typologies report Money Laundering and Terrorist Financing through the Real Estate Sector.

[33] See also the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" published 13 October 2006.

[34] See also the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" Annex 2 on trusts, for a more detailed description of "potential for misuse" of trusts.

p) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.

q) Transactions using unusual means of payment (e.g. precious metals or stones).

r) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

s) Unexplained establishment of unusual provisions in credit arrangements that do not reflect the commercial position between the parties. Arrangements that may be abused in this way might include unusually short/long amortisation periods, interest rates materially above/below market rates, or unexplained repeated cancellations of promissory notes/mortgages or other security instruments substantially ahead of the maturity date initially agreed.

t) Transfers of goods that are inherently difficult to value (e.g. jewels, precious stones, objects of art or antiques, virtual assets), where this is not common for the type of client, transaction or with the legal professional's normal course of business, such as a transfer to a corporate entity, or generally without any appropriate explanation.

u) Successive capital or other contributions in a short period of time to the same entity with no apparent legal, tax, business, economic or other legitimate reason.

v) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

w) Power of representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.

x) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.

y) Legal persons that, as a separate business, offer TCSP services should have regard to the TCSP Guidance,[35] even if such legal persons are owned or operated by legal professionals. Legal professionals, however, who offer TCSP services should have regard to this Guidance, and should consider customer or service risks related to TCSPs such as the following:

    i. Unexplained delegation of authority by the client through the use of powers of attorney, mixed boards and representative offices.

    ii. Provision of registered office facilities and nominee directorships without proper explanations.

    iii. Unexplained use of discretionary trusts.

[35] See the FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers, published in July 2019

iv. In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power.

z) In the case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries

aa) Services where the legal professional acts as a trustee/director that allows the client's identity to remain anonymous.

bb) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner), with no apparent legal, tax, business, economic or other legitimate reason.

cc) Unexplained use of pooled client accounts or safe custody of client money or assets or bearer shares, where allowed, without justification.

dd) Commercial, private, or real property transactions or services to be carried out by the client with no apparent legitimate business, economic, tax, family governance, or legal reasons.

ee) Suspicion of fraudulent transactions or transactions which are improperly accounted for. These might include:

i. Over or under invoicing of goods/services.

ii. Multiple invoicing of the same goods/services.

iii. Falsely described goods/services

iv. Over or under shipments (e.g. false entries on bills of lading).

v. Multiple trading of goods/services.

Variables that may influence risk assessment

105. While all legal professionals should follow robust standards of due diligence in order to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale and expertise amongst legal professionals, as well as the nature of the clients they serve. As a result, consideration must be given to these factors when creating a RBA that complies with the existing obligations of legal professionals. Certain notaries, for example, are subject to an array of duties as public officeholders. By contrast, legal professionals do not have such extensive public duties, but are nearly universally subject to duties of professional secrecy and an obligation to uphold their clients' rights of legal professional privilege to their communications. Legal professionals with distinct "public" roles within national legal systems should carefully consider the interaction of their particular duties with the RBA outlined in this Guidance.

106. The particular responsibilities, status and role of the legal professional will, in general, have a significant influence on what is appropriate for risk assessment. For example, in many civil law jurisdictions, notaries do not represent parties to a contract and are not intermediaries. They are obliged to be impartial and independent, advising both parties bearing in mind any disparity of power between them. Notaries carry duties as public office holders. These duties will influence the scope of what the notary must do to assess the ML/TF risk and how to act based on that assessment. Notaries should be conscious of the

respectability they can add to documents, and the value this can add to those whose motives are nefarious.

107. Consideration should be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. It may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client for a risk assessment than it would be for a large law firm having a diverse client base with different risk profiles. However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may also be regarded by criminals as more of a target for money launderers than large law firms. Legal professionals in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice, and of all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following a RBA.

108. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular legal professional. This factor must be considered in the context of the legal professional's practice, as well as the legal, professional, and ethical obligations in the jurisdiction(s) of practice. A legal professional's RBA methodology may thus take account of risk variables specific to a particular client or type of work. Consistent with the RBA and proportionality, the presence of one or more of these variables may cause a legal professional to conclude that either enhanced CDD and monitoring is warranted, or conversely that standard CDD and monitoring can be reduced, modified or simplified. When reducing, modifying or simplifying CDD, legal professionals should always adhere to the minimum requirements as set out in national legislation. These variables may increase or decrease the perceived risk posed by a particular client or type of work and may include:

a) The nature of the client relationship and the client's need for the legal professional to prepare for or carry out specified activities.

b) The level of regulation or other oversight or governance regime to which a client is subject. For example, a client that is a financial institution or legal professional regulated in a country with a satisfactory AML/CFT regime poses less risk of ML/TF than a client in an industry that has ML/TF risks and yet is unregulated for ML/TF purposes.

c) The reputation and publicly available information about a client. Legal persons that are transparent and well known in the public domain and have operated for a number of years without being convicted of proceed generating crimes may have low susceptibility to money laundering. This may not be the case where such a legal person is in financial distress or in a situation of liquidation/insolvency.

d) The regularity, depth or duration of the client relationship may be a factor that lowers or heightens risk (dependant on the nature of the relationship).

e) The familiarity of the legal professional with a country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of a legal professional's own activities.

f) The proportionality between the magnitude or volume and longevity of the client's business and its legal requirements, including the nature of services sought.

g) Subject to other factors (including the nature of the services and the source and nature of the client relationship), providing limited legal services in the capacity of a local or special counsel may be considered a low risk factor. This may also, in any event, mean that the legal professional is not "preparing for" or "carrying out" a transaction for a specified activity identified in R.22.

h) Significant and unexplained geographic distance between the legal professional and the location of the client where there is no nexus to the type of activity being undertaken.

i) Where a prospective client has instructed the legal professional to undertake a single transaction-based service (as opposed to an ongoing advisory relationship) and one or more other risk factors are present.

j) Where the legal professional knows that a prospective client has used the services of a number of legal professionals for the same type of service over a relatively short period of time.

k) Risks that may arise from non-face-to-face relationships and could favour anonymity. Due to the prevalence of electronic communication between legal professionals and clients in the delivery of legal services, non-face-to-face interaction between legal professionals and clients would not be considered a high risk factor on its own. The treatment of non-face-to-face communications should always be subject to the approach taken by legislation and regulators in the relevant jurisdiction.

l) The nature of the referral or origin of the client. A prospective client may contact a legal professional in an unsolicited manner or without common or customary methods of introduction or referrals, which may indicate increased risk. By contrast, where a prospective client has been referred from another trusted source or a source regulated for AML/CFT purposes (e.g. from another legal professional), the referral may be considered a mitigating risk factor.

m) The structure of a client or transaction. Structures with no apparent legal, tax, business, economic or other legitimate reason may increase risk. Legal professionals often design structures (even if complex) for legitimate legal, tax, business, economic or other legitimate reasons, in which circumstances there may not be an indicator of increased risk of ML/TF. Legal professionals should satisfy themselves of a reasonable need for such complex structures in the context of the transaction.

n) Trusts that are pensions may be considered lower risk.

Documentation of risk assessments

109. Several jurisdictions mandate various documentation requirements in connection with AML/CFT.[36] Legal professionals must always understand their ML/TF risks (for clients, countries or geographic areas, services, transactions or delivery channels). They should document those assessments to be able to demonstrate their basis. However, competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.[37]

110. Legal professionals may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time efficient yet comprehensive manner has become more important as legal professionals are now obliged in various jurisdictions to conduct a documented risk assessment for each client and share it with supervisory authorities when required.

111. A documented risk assessment may cover a range of specific risks by breaking them down into the three common categories highlighted above: (a) geographic risks, (b) client-based risks and (c) service-based risks. These three risk categories have been identified and explained in the guide: "*A Lawyer's Guide to Detecting and Preventing Money Laundering*".[38] The guide also provides graphic illustrations and case studies of how to assess risk under these three categories. In practice, risk factors could be categorised differently in different jurisdictions. However, all relevant risk factors should be considered.

112. Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan[39] (if required) should then be outlined to accompany the assessment and dated. Action plans can help identify potential red flags, facilitate risk assessment and decide on CDD measures to be applied. A simple template of risk assessment may be as below, for instance:

Geographic risk	Client-based risk	Service-based risk
Low/medium/high risk	Low/medium/high risk	Low/medium/high risk
Explanation	Explanation	Explanation
Overall assessment: Low/Medium/High risk		
Action plan		

113. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, as required, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the

[36] For example, the European Union law places an obligation on legal professionals working in an AML-regulated service to document risk assessments and ensure they are kept up to date (Article 8 of the Fourth Anti-Money Laundering Directive (EU) 2015/849).

[37] Paragraph 8 of INR.1

[38] A Lawyer's Guide to Detecting and Preventing Money Laundering, is a collaborative publication of the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, published in October 2014.

[39] "Action plans" are described in some jurisdictions as the "document your thought process" form.

client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties. Proper safeguards should be put in place to ensure privacy of clients.

114. Where legal professionals are involved in longer term transactions, risk assessments should be undertaken at suitable intervals across the life of the transaction, to ensure no significant risk factors have changed in the intervening period (e.g. new parties to the transaction, new sources of funds etc.). See [3.4.2] *Ongoing monitoring of clients and special activities.*

115. A final risk assessment should be undertaken before a transaction has completed, allowing time for any required STR to be filed and any authority to move or transfer assets to be obtained from law enforcement (in countries where this is applicable).

Risk management and mitigation

116. Identification and assessment of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow legal professionals to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the legal professional's role and involvement. Circumstances may vary considerably between professionals who represent clients directly and those who are engaged for distinct purposes including, for example, civil law notaries. In high risk scenarios, legal professionals must consider the extent to which they might be involved in unwittingly enabling the substantive offence of ML/TF by providing a legal service even with the application of enhanced CDD measures. Under such scenario, legal professionals should consider not to provide services or establish/continue business relationship with the client.

117. Legal professionals should implement appropriate measures and controls to mitigate the potential ML/TF risks for those clients that, as the result of a RBA, are determined to be higher risk. These measures should be tailored to the specific risks faced, both to ensure the risk is adequately addressed and to assist in the appropriate allocation of finite resources for CDD. Paramount among these measures is the requirement to train legal professionals and appropriate staff to identify and detect relevant changes in client activity by reference to risk-based criteria. These measures and controls may include:

a) General training on ML/TF methods and risks relevant to legal professionals.

b) Targeted training for increased risk awareness by the legal professionals providing specified activities to higher risk clients or to legal professionals undertaking higher risk work.

c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain evidence and record source of wealth and beneficial ownership information if required.

d) Periodic review of the services offered by the legal professional and/or law firm, and the periodic evaluation of the AML/CFT framework applicable to the law firm or legal professional and the law firm's own AML/CFT procedures, to

determine whether the ML/TF risk has increased and adequate controls are in place to mitigate those increased risks.

e) Reviewing client relationships on a periodic basis to determine whether the ML/TF risk has increased.

Initial and ongoing CDD (R.10 and 22)

118. CDD measures should allow a legal professional to establish with reasonable certainty the true identity of each client. The legal professional's procedures should apply in circumstances where a legal professional is preparing for or carrying out[40] the specified activities listed in R.22 and include procedures to:

a) Identify and appropriately verify the identity of each client on a timely basis.

b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner on risk-sensitive basis such that the legal professional is reasonably satisfied that it knows who the beneficial owner is. The general rule is that clients should be subject to the full range of CDD measures, including the requirement to identify the beneficial owner in accordance with R.10. The purpose of identifying beneficial ownership is to ascertain those natural persons who exercise effective influence or control over a client, whether by means of ownership, voting rights or otherwise. Legal professionals should have regard to this purpose when identifying the beneficial owner. They may use a RBA to determine the extent to which they are required to verify the identity of beneficial owner, depending on the type of client, business relationship and transaction and other appropriate factors in accordance with R.10 and INR.10 as articulated in the following box. This information is in many circumstances critical to helping legal professionals avoid conflicts of interest with other clients.

Box 3. Beneficial ownership information obligations (see R.10, R.22 and INR.10)

R.10 sets out the instances where legal professionals will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF, when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. Legal professionals should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk.[41]

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. Legal professionals can

[40] See paragraphs 17-22 above for further information on when a legal professional would or would not be considered engaged in "preparing for" or "carrying out" transactions for clients, and hence when the requirements of R.22 would apply.

[41] For more information and guidance relating to beneficial ownership information please refer to AML/CFT 2013 Methodology Criteria 10.5 and 10.8-10.12.

verify the identity of a client by, for example meeting the client in person and then verifying their identity through the production of a passport/identity card and documentation confirming his/her address. Legal professionals can further verify the identity of a client on the basis of documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the legal professional is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client and may include conducting public searches as well as by seeking information directly from the client. Legal professionals will likely need to obtain the following information for a client that is a legal entity:

a) the name of the company;
b) the company registration number;
c) the registered address and/ or principal place of business (if different);
d) the identity of shareholders and their percentage ownership;
e) names of the board of directors or senior individuals responsible for the company's operations;
f) the law to which the company is subject and its constitution; and
g) the types of activities and transactions in which the company engages.

To verify the information listed above, legal professional may use sources such as the following:

a) constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);
b) details from company registers;
c) shareholder agreement or other agreements between shareholders concerning control of the legal person; and
d) filed audited accounts.

Legal professionals should adopt a RBA to verify beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to-date or to ask for additional documentation that confirms the beneficial ownership and company structure.

The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires reasonable steps to be taken to identify the beneficial ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

c) Obtain appropriate information to understand the client's circumstances and business depending on the nature, scope and timing of the services to be provided including, where necessary, the source of funds of the client. This

information may be obtained from clients during the normal course of their instructions to legal professionals.

d) Conduct ongoing CDD on the business relationship and scrutiny of transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with legal professional's knowledge of the client, its business and risk profile, including where necessary, the source of funds. Ongoing due diligence ensures that the documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of STRs to an FIU where required, or to respond to requests for information from an FIU and law enforcement agencies.

119. The starting point is for legal professionals to assess the risks that the client may pose taking into consideration any appropriate risk variables (and any mitigating factors) before making a final determination to accept the client, reject the client, or request additional information. In many situations and in many jurisdictions this risk assessment is required to be documented and kept in the client's file. The legal professional should review this file as necessary, especially in a situation where the client looks to engage in a one-off or atypical transaction or where new red flags arise. The legal professional's risk assessment should inform the overall approach to CDD and appropriate verification. Legal professionals should reasonably determine the CDD requirements appropriate to each client, which may include:

a) **Standard CDD:** A standard level of CDD, generally to be applied to all clients to whom specified services are provided.

b) **Simplified CDD:** The standard level being reduced after consideration of appropriate risk variables, and in recognised lower risk scenarios, such as:

   i. Publicly listed companies traded on certain exchanges (and their majority owned subsidiaries). Although it should not be assumed that all publicly listed companies will qualify for simplified CDD, for example appropriate levels of reporting to the market will be a factor to take into account, as well as geographic risk factors.

   ii. Financial institutions and other businesses and professions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations.

   iii. Public administration or enterprises (other than those from countries that are being identified by credible sources as having inadequate AML/CFT systems, being the subject of sanctions, embargos or similar measures issued by the United Nations, having significant levels of corruption or other criminal activity or providing funding or support for terrorist activities, or having designated terrorist organisations operating within their country).

c) **Enhanced CDD:** An increased level of CDD for those clients that are reasonably determined by the legal professional to be of higher risk. This may be the result of the client's business activity, ownership structure, particular service offered including work involving higher risk countries or defined by applicable law or regulation as posing higher risk.

120. Where the legal professional is unable to comply with the applicable CDD requirements, they should not carry out the transaction nor commence business relations, or should terminate the business relationship and consider filing an STR in relation to the client.

121. A RBA means that legal professionals should perform varying levels of work according to the risk level. For example, where the client or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, and that information is publicly available, fewer checks may be appropriate. In the case of trusts, foundations or similar legal entities where the beneficiaries are distinct from the legal owners of the entity, it will be necessary to form a reasonable level of knowledge and understanding of the classes and nature of the beneficiaries; the identities of the settlor, trustees or natural persons exercising effective control; and an indication of the purpose of the trust. Legal professionals will need to obtain a reasonable level of comfort that the declared purpose of the trust is in fact its true purpose.

122. The following box provides a non-exhaustive list of examples of standard, enhanced and simplified CDD:

Box 4. Examples of Standard/Simplified/Enhanced CDD measures (see also INR.10)

Standard CDD

- Identifying the client and verifying that client's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the legal professional is satisfied about the identity of beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required
- Understanding and obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the business and risk profile of the client, including, where necessary, the source of wealth and funds

Simplified CDD

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client's identity

- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

Enhanced CDD

- Obtaining additional client information, such as the client's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the client risk profile
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of legal professionals should enable them to disregard source documents, data or information, which is perceived to be unreliable)
- Where appropriate, undertaking further searches on the client or beneficial owner to specifically understand the risk that the client or beneficial owner may be involved in criminal activity
- Obtaining additional information about the client's source of wealth or funds involved to seek to ensure they do not constitute the proceeds of crime. This could include obtaining appropriate documentation concerning the source of wealth or funds
- Seeking additional information and, as appropriate, substantiating documentation, from the client about the purpose and intended nature of the transaction or the business relationship
- Increasing the frequency and intensity of transaction monitoring.
- Enhanced CDD may also include lowering the threshold of ownership (e.g. below 25%), to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of such holders.

Ongoing monitoring of clients and specified activities (R.10 and 23)

123. The degree and nature of ongoing monitoring by a legal professional will depend on the type of legal professional, and if it is a law firm, the size and geographic 'footprint' of the law firm, the ML/TF risks that the law firm has identified and the nature of the specified activity and services provided. In many instances, client information must already be monitored in this fashion to satisfy legal professionals' other obligations (e.g. legal, professional, or ethical) to both their clients and as part of their general regulatory

obligations. For example, legal professionals may need to have a full and up-to-date understanding of their clients' business to fully satisfy fiduciary duties towards their clients. In some jurisdictions, ethical or professional obligations may require a legal professional to discontinue their representation of a client on learning/knowing certain adverse information or in case of reasonable grounds to suspect that the client is involved in an ML/TF offence. Monitoring is often best achieved by individuals having contact with the client (either face-to-face or by other means of communication).

124. Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that legal professionals are aware of any changes in the client's identity and risk profile established at client acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds where necessary, to judge consistency with expected behaviour based on accumulated CDD information.

125. In larger law firms serving clients with a wide range of operations, legal professionals with regular contact with the client may be narrowly focused on one aspect of the client's business and/or need for specific advice. In these circumstances, it may be more effective to have screening processes and tools to identify potential risks that are generic to the client's overall business, and that can then be flagged for the attention of legal professionals who have the most client contact. However, monitoring does not require legal professionals to function as, or assume the role of, a law enforcement or investigative authority vis-a-vis the client. It rather refers to maintaining awareness throughout the course of work for a client to the possibility of ML/TF activity and/or changes in the clients activities/personnel and/or other changing risk factors.

126. Monitoring of these advisory relationships cannot be achieved solely by reliance on automated systems and whether any such systems would be appropriate will depend in part on the nature of a legal professional's practice and resources reasonably available to the legal professional. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large law firm; rather, the sole practitioner would be expected to develop appropriate monitoring systems and a RBA proportionate to the scope and nature of the practitioner's practice. A legal professional's advisory relationships may well be best monitored by the individuals having direct client contact being appropriately trained to identify and detect changes in the risk profile of a client. Where appropriate this should be supported by systems, controls and records within a framework of support by the firm (e.g. tailored training programs appropriate to the level of staff responsibility, the role each staff member plays in the AML/CFT process at the firm and the types and volumes of clients and transaction for which the firm provided services).

127. Legal professionals should assess the adequacy of any systems, controls and processes on a periodic basis. Monitoring programs should fall within the system and control framework developed to manage the risk of the firm. Certain jurisdictions may require that the results of the monitoring be documented.

128. The civil law notaries do not generally represent parties to a contract and therefore must maintain a fair position with regard to any duty to both parties.

Suspicious transaction reporting, tipping-off, internal control and higher-risk countries (R.23)

129. R.23 sets out obligations for legal professionals on reporting and tipping-off, internal controls and higher-risk countries as set out in R.20, R.21, R.18 and R.19.

Suspicious transaction reporting and tipping-off (R.20, R.21 and 23)

130. R.23 requires legal professionals to report suspicious transactions set out in R.20, when on behalf of, or for a client, they engage in a financial transaction in relation to the activities described in R.22. Subject to certain limitations, such reporting is not required if the relevant information is directly encompassed within a legitimate claim of professional secrecy or legal professional privilege. Legal professionals should be alert to these obligations in addition to separate requirements in their jurisdictions regarding tipping-off. These obligations, where they apply, can carry serious penalties when not properly complied with. As specified under INR.23, where legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

131. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must always be made promptly and, therefore, a RBA for the reporting of the suspicious activity under these circumstances is not applicable. STRs are not part of risk assessment, but rather reflect a response mechanism – typically to an FIU or SRB once a suspicion has been formed. Legal professionals have an obligation not to facilitate illegal activity, so if there are suspicions, they could contact their FIU or SRB for guidance, obtain independent legal advice, if necessary and do not provide services to that person/company and report the transaction or the attempted transaction. Legal professionals may be asked to advise a client on the client's own obligation to report suspicious activity. In doing so, the legal professional may become aware of the subject matter giving rise to the suspicion. In these circumstances, the legal professional will need to consider whether it should file an STR where required. In the context of an international law firm, which may have a global Money Laundering Reporting Officer (MLRO), where a reportable suspicion arises in relation to a client, the MLRO need not necessarily make a report to the FIU in each jurisdiction where a client has a relationship but, rather, in the jurisdictions with a nexus to the matter giving rise to the suspicion.

Internal controls (R.18 and 23)

132. Legal professionals differ significantly from financial institutions in terms of size. By contrast to most financial institutions, a significant number of legal professionals have only a few staff. This limits the resources that small businesses and professions can dedicate to the fight against ML/TF. For a number of legal professionals, a single person may be responsible for the functions of front office, back office, reporting, and senior management. This dimension of a legal professional's practice environment should be taken into account in designing a risk-based framework for internal controls systems. INR.18 specifies that the type and extent of measures to be taken for each of its requirements should be appropriate having regard to the size, nature and risk profile of the business.

133. The risk-based process must be a part of the internal controls of the legal professional or law firm. Legal professionals operate within a wide range of differing business structures, from sole practitioners to large, multi-national partnerships. In smaller legal practices, legal professionals' businesses tend to have a flat management structure and

accordingly, most or all of the principals (or partners) of the firm hold ultimate management responsibility. In other organisations, legal professionals employ corporate style organisational structures with tiered management responsibility. In both cases the principals or the managers are ultimately responsible for ensuring that the organisation maintains an effective internal control structure; regardless of the size of the legal practice, legal professionals are generally responsible for the actions of their partners and staff. Engagement by the principals and managers in AML/CFT is an important aspect of the application of the RBA since such engagement reinforces a culture of compliance, ensuring that staff adheres to the legal professional's policies, procedures and processes to manage effectively ML/TF risks.

134. The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:

a) the nature, scale and complexity of a legal professional's business.

b) the diversity of a legal professional's operations, including geographical diversity.

c) the legal professional's client, service and activity profile.

d) the degree of risk associated with each area of the legal professional's operations.

e) the services being offered and the frequency of client contact (either by face-to-face meetings or by other means of communication).

135. Subject to the size and scope of the legal professional's organisation, the framework of risk-based internal controls should:

a) have appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP;

b) provide for adequate controls for higher risk clients and services as necessary (e.g. additional due diligence, obtaining information on the source of wealth and funds of a client, escalation to senior management or additional review and/or consultation by the legal professional or within a law firm);

c) provide increased focus on a legal professional's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse for ML/TF;

d) provide for periodic review of the risk assessment and management processes, taking into account the environment within which the legal professional operates and the services it provides;

e) designate personnel at an appropriate level who are responsible for managing AML/CFT compliance;

f) provide for an AML/CFT compliance function and review programme as appropriate given the scale of the organisation and the nature of the legal professional's practice;

g) inform the principals of compliance initiatives, identified compliance deficiencies and corrective action taken;

h) provide for programme continuity despite changes in management or employee composition or structure;

i) focus on meeting all regulatory measures for AML/CFT compliance, including record-keeping requirements and provide for timely updates in response to changes in regulations;

j) implement risk-based CDD policies, procedures and processes, including review of client relationships from time to time to determine the level of ML/TF risks;

k) provide for adequate supervision and support for staff activity that forms part of the organisation's AML/CFT programme;

l) incorporate AML/CFT compliance into job descriptions of relevant personnel;

m) for legal professionals that share a common arrangement in some way (e.g. alliances of law firms), to the extent possible, provide a common control framework;

n) adhere to country specific legislative requirements (such as residence requirements);

o) provide for policies and procedures to ensure staff awareness of STR filing requirements; and

p) implement a documented program of ongoing staff AML/CFT awareness and training.

136. Same measures and controls may often address more than one of the risk criteria identified, and it is not essential that a legal professional establish specific controls targeting each risk criterion.

137. Legal professionals should consider using reputable technology-driven solutions to minimise the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the legal profession as they continue to develop, this may be particularly important for smaller law firms that may be less able to commit significant resources of time to these activities. Under R.17, the ultimate responsibility for CDD measures should remain with legal professionals relying on the technology-driven solutions utilized.

138. At larger law firms, senior management should have a clear understanding of ML/TF risks to manage the affairs of the law firm and to ensure adequate procedures are put in place to identify, manage, control and mitigate risks effectively. The RBA to AML/CFT needs to be embedded in the culture of law firms and the legal profession generally.

Internal mechanisms to ensure compliance

139. Legal professionals (and where relevant senior management and the board of directors (or equivalent body)) should monitor the effectiveness of internal controls. If they identify any weaknesses in those internal controls, improved procedures should be designed.

140. The most effective tool to monitor the internal controls is a regular (typically at least annually) independent (internal or external) compliance review. If carried out internally, a staff member who may have a good working knowledge of the law firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to

challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff are properly applying the law firm's procedures.

141. If the compliance review identifies areas of weakness and makes recommendations on how to improve the policies and procedures, then senior management should monitor how the law firm is acting on those recommendations.

142. Legal professionals should review their firm-wide risk assessments regularly and make sure that policies and procedures continue to target those areas where the ML/TF risks are highest.

Vetting and recruitment

143. Legal professionals should consider the skills, knowledge and experience of staff for AML/CFT both before they are appointed to their role and on an ongoing basis. The level of assessment should be proportionate to their role in the firm and the ML/TF risks they may encounter. Assessment may include criminal records checking and other forms of pre-employment screening such as credit reference checks and background verification (as permitted under national legislation) for key staff positions.

Education, training and awareness

144. R.18 requires that legal professionals provide their staff with AML/CFT training. For legal professionals, and those in smaller law firms in particular, such training may also assist with raising awareness of monitoring obligations, and may also satisfy some jurisdictions' continuing legal education obligations. A legal professional's commitment to having appropriate controls in place relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant legal professionals with at least general information on AML/CFT laws, regulations and internal policies.

145. Firms should provide targeted training for increased awareness by the legal professionals providing specified activities to higher risk clients or to legal professionals undertaking higher risk work. Training should also be targeted towards the role that individual legal professionals perform in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties, or training regarding red flags for those undertaking client/transactional risk assessment.

146. Training is not necessarily resource-intensive and it can take many forms. Training can include group study where one member of staff outlines to other staff, relevant guidance, credible sources of information on legal sector risk or firm policies and/or provides regular email updates.

147. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Legal professionals must also be alert to the interaction with, and importance of legal professional privilege and professional secrecy in relation to AML/CFT laws in their particular jurisdictions.[42] Likewise, legal professionals should be aware of the scope of application of the legal professional

[42] See also the FATF Report on Vulnerabilities in the Legal Sector (2013), Chapter 4 "ML Typologies".

privilege and professional secrecy in their jurisdictions, i.e. the cases and scenarios that fall under its application and those outside its scope.

148. In line with a RBA, particular attention should be given to risk factors or circumstances occurring in the legal professional's own practice. In addition, competent authorities, SRBs and representative bodies for both common and civil law notaries and law societies should work with educational institutions to ensure that the curriculum addresses ML/TF risks. The same training should also be made available for students taking courses to train to become legal professionals. For example, law societies and bar associations should be encouraged to produce jurisdiction-specific guidance based on this Guidance (such as the ABA's Voluntary Good Practices Guidance), offer continuing legal education programs on AML/CFT and the RBA and large law firms should be encouraged to conduct in-house training programs on AML/CFT and the RBA.

149. The overall RBA and the various methods available for training and education gives legal professionals flexibility regarding the frequency, delivery mechanisms and focus of such training. Legal professionals should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

a) tailored to the relevant staff responsibility (e.g. client contact or administration);

b) at the appropriate level of detail (e.g. considering the nature of services provided by the legal professional);

c) at a frequency suitable to the risk level of the type of work undertaken by the legal professional; and

d) used to assess staff knowledge of the information provided.

Higher-risk countries (R.19 and 23)

150. Consistent with R.19, legal professionals should apply enhanced CDD measures (also see box in paragraph 102 above), proportionate to the risks, to business relationships and transactions with clients from countries for which this is called for by the FATF.

Section IV- Guidance for supervisors

151. The RBA to AML/CFT aims to develop prevention or mitigation measures, which are commensurate with the risks identified. This applies to the way supervisory authorities allocate their resources. R.28 requires that legal professionals are subject to adequate AML/CFT regulation and supervision. Supervisors and SRBs have different roles across jurisdictions and this section should be read in the context of what is applicable for a specific jurisdiction. Whichever model of supervision (i.e. by a designated supervisor or a SRB) is adopted by a country, it should be effective.

152. In many jurisdictions, supervisors and SRBs take an active role in identifying ML/TF risks and may take a direct approach to regulating legal professionals' obligatory responsibilities both generally and with regards to AML/CFT. Supervisors or SRBs should identify the particularities of the sector, assess its risks, controls and procedures in order to efficiently allocate its resources. In particular, supervisors for legal professionals should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas.

153. Although a country may have a legal framework that does not fully accommodate the supervision of legal professionals in the manner described in this Section, the supervision of legal professionals in that country should nonetheless include as a minimum:

a) A requirement that legal professionals perform risk assessment at firm, client and transactional level.

b) A requirement that legal professionals perform appropriate risk-based CDD.

c) Procedures that ensure the system for licensing legal professionals prevents criminals from becoming legal professionals.

d) Procedures determined to ensure prompt investigation of legal professional misuse of client/ trust funds or alleged involvement in ML/TF schemes.

e) A requirement that legal professionals complete periodic continuing legal education in CDD and AML/CFT topics.

f) A requirement that legal professionals report suspicious transactions, comply with tipping-off and confidentiality requirements, internal controls requirements and higher-risk countries requirements.

g) A requirement that legal professionals adequately document risk assessment, CDD and other AML related decisions and processes undertaken.

Risk-based approach to supervision

154. R.28 requires that legal professionals are subject to adequate AML/CFT regulation and supervision for monitoring compliance. A RBA to AML/CFT means that the measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resources to areas of higher ML/TF risk. While it is each country's responsibility to ensure there is an adequate national framework in place in relation to regulation and supervision of legal professionals, any relevant supervisors and

SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.[43]

Supervisors and SRBs' role in supervision and monitoring

155. Countries can ensure that legal professionals are subject to effective oversight through the supervision performed by a SRB, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF. A SRB is a body representing a profession (e.g. legal professionals, notaries, other independent legal professionals, accountants or TCSPs) that has a role (either exclusive or in conjunction with other entities) in regulating the persons who are qualified to enter and practise in the profession. A SRB also may perform supervisory or monitoring functions (e.g. to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession).

156. Supervisors and SRBs should have appropriate powers to perform their supervisory functions (including powers to monitor and to impose effective, proportionate and dissuasive sanction), and adequate financial, human and technical resources. Supervisors and SRBs should determine the frequency and intensity of their supervisory or monitoring actions on a RBA, taking into account inherent ML/TF risks in the legal sector, and mitigation by legal professionals and their firms.

157. Countries should ensure that supervisors and SRBs are equipped in identifying and sanctioning non-compliance by its members. Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

158. Supervisors and SRBs should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas. Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives pertaining to the SRB's role in representing their members, while also being obligated to supervise them. If a SRB contains members of the supervised population, or represents those people, the relevant person should not continue to take part in the monitoring/ supervision of their practice/law firm to avoid conflicts of interest. This institutional conflict may be particularly relevant when it comes to enforcement, including sanctions, which should be sufficient to have a deterrent effect and also remove the benefits of non-compliance.

Background: national frameworks and understanding ML/TF risk- the role of countries

159. Countries should ensure that the extent to which a national framework allows legal professionals to apply a RBA should also reflect the nature, diversity and maturity of the sector, and its risk profile as well the ML/TF risks associated with individual legal professionals.

160. Access to information about ML/TF risks is essential for an effective RBA. Countries are required to take appropriate steps to identify and assess ML/TF risks on an ongoing basis in order to (a) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (b) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (c) make information

[43] See INR 28.1.

available for AML/CFT risk assessments conducted by legal professionals and the jurisdiction's national assessment of risk. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to competent authorities, SRBs and legal professionals.[44] In situations where some legal professionals have limited capacity to identify ML/TF risks, countries should work with the sector to understand their risks.

161. Supervisors and SRBs should, as applicable draw on a variety of sources to identify and assess ML/TF risks. These may include, but will not be limited to, the jurisdiction's national risk assessments, supra-national risk assessments, domestic or international typologies and supervisory expertise, as well as FIU feedback. The necessary information can also be obtained through appropriate information-sharing and collaboration among AML/CFT supervisors, when there are more than one for different sectors (legal professionals, accountants and TCSPs).

162. Competent authorities may also consider undertaking a targeted sectoral risk assessment to get a better understanding of the specific environment in which legal professionals operate in the country and the nature of services provided by them.

163. Supervisors and SRBs should understand the level of inherent risk including the nature and complexity of services provided by the legal professional. Supervisors and SRBs should also consider the type of services the legal professional is providing as well as its size and business model (e.g. whether it is a sole practitioner), corporate governance arrangements, financial and accounting information, delivery channels, client profiles, geographic location and countries of operation. Supervisors and SRBs should also consider the controls legal professionals have in place (e.g. the quality of the risk management policy, the functioning of the internal oversight functions and the quality of oversight of any outsourcing and subcontracting arrangements). Supervisors should note that under the RBA, particularly in the legal profession sector, given their diversity in scale, functions and number, there may be valid reasons for differences among risks and controls. There is therefore no one-size-fits-all approach. In evaluating the adequacy of their RBA, supervisors should take into consideration the circumstances of these differences.

164. Supervisors and SRBs should seek to ensure that their supervised populations are fully aware of, and compliant with measures to identify and verify a client, the client's source of wealth and funds where required, along with measures designed to ensure transparency of beneficial ownership, as these are cross-cutting issues that affect several aspects of AML/CFT.

165. To further understand the vulnerabilities associated with beneficial ownership, with a particular focus on the involvement of professional intermediaries, supervisors should stay abreast of research papers published by international bodies.[45] Useful reference include the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

166. Supervisors and SRBs should review their assessment of legal professionals' ML/TF risk profiles periodically, including when circumstances change materially or relevant new threats emerge and appropriately communicate this assessment to the legal professional community.

---

[44] See INR 1.3.

[45] Such as the FATF, the OECD, the WB, the IMF and the UNODC.

Mitigating and managing ML/TF risk

167. Supervisors and SRBs should take proportionate measures to mitigate and manage ML/TF risk. Supervisors and SRBs should determine the frequency and intensity of these measures based on their understanding of the inherent ML/TF risks. Supervisors and SRBs should consider the characteristics of the legal professionals, particularly their role as professional intermediaries. It is essential to have a clear understanding of the ML/TF risks: (a) present in the country; and (b) associated with the type of legal professionals and their clients, products and services.[46]

168. Supervisors and SRBs should take into account the risk profile of legal professionals when assessing the adequacy of internal controls, policies and procedures.[47]

169. Supervisors and SRBs should develop a means of identifying which legal professionals or classes of legal professionals are at the greatest risk of being used by criminals and communicate those findings to the legal professionals. This involves considering both the probability and impact of ML/TF risk.

170. Probability means the likelihood of ML/TF taking place as a consequence of the activity undertaken by legal professionals and the environment in which they operate. The risk can also vary depending on other factors:

a) service and product risk (the likelihood that products or services can be used for ML/TF);

b) client risk (the likelihood that clients' funds may have criminal origins);

c) nature of transactions (e.g. frequency, volume and counterparties);

d) geographical risk (whether the legal professional, its clients or other offices perform specified activities in riskier locations); and

e) other indicators of risk are based on a combination of objective factors and experience, such as the supervisor's wider work with the legal professional as well as information on legal professional's compliance history, complaints about the legal professional or about the quality of the legal professional's internal controls. Other such factors may include information from government/law enforcement sources, whistle-blowers or negative news reports in credible media, particularly those related to predicate offences for ML/TF or to financial crimes.

171. In adopting a RBA to supervision, supervisors may consider allocating supervised entities sharing similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of business, type of clients serviced and geographic areas of activities. The setting up of such groupings could allow supervisors to take a comprehensive view of the sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual firms. If the risk profile of a legal professional within a grouping changes, supervisors may reassess the supervisory approach, which may include removing the firm from the grouping.

[46] See INR 28.2.
[47] See INR 28.3

172. Supervisors and SRBs should also consider the impact, (i.e. the potential harm caused) if the legal professional or firm facilitates, unwittingly or otherwise, ML/TF. A small number of legal professionals may cause a high level of harm, including reputational harm to the profession. This can depend on:

a) size (i.e. turnover), number and type of clients, number of office locations, value of transactions, and

b) links or involvement with other businesses (which could affect the susceptibility to being involved in 'layering' activity, e.g. concealing the origin of the transaction with the purpose to legalise the asset).

173. Supervisors and SRBs should update the risk assessment on an ongoing basis. The result from the assessment will help determine the resources the supervisor will allocate to the supervision of the legal professionals.

174. Supervisors or SRBs should consider whether legal professionals meet the ongoing requirements for continued participation in the profession as well as assessments of competence and of fitness and character. This will include whether the legal professional meets expectations related to AML/CFT compliance. This will take place both when a supervised entity joins the profession, and on an ongoing basis thereafter.

175. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to differentiate among categories of legal professionals based on various factors such as their client base, countries they deal with and applicable AML/CFT controls. Other determinative factors may include (a) whether the legal professional conducts litigation or transactional business; (b) whether the clients of the legal professional's firm are in the private or public sector; or (c) whether the legal professional's business is internationally or domestically focused.

176. Supervisors and SRBs should acknowledge that in a risk-based regime, not all legal professionals will adopt identical AML/CFT controls and that an isolated incident where the legal professional is part of an illegal transaction unwittingly does not necessarily invalidate the integrity of a legal professional's AML/CFT controls. At the same time, legal professionals should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

Supervision of the RBA

Licensing or Registration

177. R.28 requires a country to ensure that regulated entities including legal professionals are subject to regulatory and supervisory measures to ensure compliance by the profession with AML/CFT requirements.

178. R.28 requires the supervisor or SRB to take the necessary measures to prevent criminals or their associates from being professionally accredited or holding or being the beneficial owner of a significant or controlling interest in an accredited legal professional entity (where this is permitted under national law and regulations) or holding a management function in a legal professional entity. This may be achieved through the evaluation of these persons through a "fit and proper" test.

179. A licensing or registration mechanism is one of the means to identify legal professionals to whom the regulatory and supervisory measures, including the "fit and

proper" test should be applied. It also enables the identification of the population of legal professionals, for the purposes of assessing and understanding the ML/TF risks for the country, and the action that should be taken to mitigate them in accordance with R.1. Not all jurisdictions take this approach, and the application and precise objectives of licensing and registration differ among the jurisdictions that do use these mechanisms.

180. Licensing or registration provides a supervisor or SRB with the means to fulfil a "gatekeeper" role over who can enter a profession in which many individuals will be required to undertake the specified activities set forth in R.22. Not all accredited legal professionals who are appropriately licensed or registered may be performing the specified activities under R.22. There is no requirement for separate licensing or registration of legal professionals on the basis of their practice areas under the FATF Recommendations. Supervisors and SRBs should ensure that their supervisory efforts are directed at legal professionals whose practices involve the specified activities under R.22. Licensing or registration should also ensure that upon qualification, legal professionals are subject to AML/CFT compliance monitoring.

181. As appropriate, the supervisor or SRB should actively identify individuals and businesses who should be supervised by using intelligence from other competent authorities (e.g. FIUs, company registry, or tax authority), information from financial institutions and DNFBPs, complaints by the public and open source information from advertisements and business and commercial registries, or any other sources that indicates that there are unsupervised individuals or businesses providing the specified activities under R.22.

182. Licensing or registration frameworks should define the activities that are subject to licensing or registration, prohibit unlicensed or unregistered individuals or businesses providing these activities and set out measures for both refusing licences or registrations and for removing "bad actors".

183. The terms "licensing" or "registration" are not interchangeable. Licensing regimes generally tend to operate over financial institutions and impose mandatory minimum requirements based upon Core Principles on issues such as capital, governance, and resourcing to manage and mitigate prudential, conduct as well as ML/TF risks on an on-going basis. Some jurisdictions have adopted similar licensing regimes for legal professionals, generally where legal professionals carry out trust and corporate services, to encompass aspects of conduct requirements in managing the higher level of ML/TF risks that have been identified in that sector.

184. A jurisdiction may have a registration framework over the entire DNFBP sector, including legal professionals or have a specific registration framework for each constituent of a DNFBP. Generally, a supervisor or SRB carries out the registration function.

185. The supervisor or SRB should ensure that requirements for licensing or registration and the process for applying are clear, objective, publicly available and consistently applied. Determination of the licence or registration should be objective and timely. A SRB could be responsible for both supervision and for representing the interest of its members. The SRB should ensure that registration decisions are taken separately and independently from its activities regarding member representation.

Fit and proper tests

186. A fit and proper test provides a possible mechanism for a supervisor or SRB to take the necessary measures to prevent criminals or their associates from owning, controlling or holding a

management function in a legal professional. Such tests are used in relation to legal professionals in some jurisdictions and may be used by supervisors or SRBs to ensure compliance with AML/CFT requirements.

187. In accordance with R.28, the supervisor or SRB should establish the integrity of every beneficial owner, controller and individual holding a management function in a legal professional.

188. In some jurisdictions, a "fit and proper test" forms a fundamental part of determining whether to license or register the applicant and whether on an ongoing basis the licensee or registrant (including its owners and controllers, where applicable) remains fit and proper to continue in that role. The initial assessment of an individual's fitness and propriety is a combination of obtaining information from the individual and corroborating elements of that information against independent credible sources to determine whether the individual is fit and proper to hold that role.

189. The process for determining fitness and propriety generally requires the applicant to complete a questionnaire. The questionnaire could gather personal identification information, residence and employment history, and require disclosure by the applicant of any convictions or adverse judgements, including pending prosecutions and convictions. Elements of this information should be corroborated to establish the bona fides of an individual. Such checks could include enquiries about the individual with law enforcement agencies and other supervisors, or screening the individual against independent electronic search databases. The personal data collected should be kept confidential.

190. The supervisor or SRB should also ensure that on an ongoing basis that those holding or being the beneficial owner of significant or controlling interest in and individuals holding management functions are fit and proper. A fit and proper test should apply to new owners, controllers and individuals holding a management function. The supervisor or SRB should consider reviewing the fitness and propriety of these individuals arising from any supervisory findings, receipt of information from other competent authorities; or open source information indicating significant adverse developments.

Guarding against "brass-plate" operations

191. The supervisor or SRB should ensure that its licensing or registration requirements require the applicant to have a meaningful relationship with the country. Depending on the circumstances, a business with only staff who do not possess the professional requirements of a legal professional might not be licensed or registered.

192. A supervisor or SRB should consider the ownership and control structure of the applicant to make a licensing or registration decision, where applicable. Factors to take into account could include consideration of where the beneficial owners and controllers reside and the type and quality of its management, including directors, managers and compliance officers.

193. The supervisor or SRB should consider whether the ownership and control structure of law firms unduly hinders its identification of the beneficial owners and controllers or presents obstacles to applying effective supervision.

Monitoring and supervision

194. Supervisors and SRBs should take measures to effectively monitor legal professionals providing specified legal services through on-site and off-site supervision. The nature of this monitoring will depend on the risk profiles prepared by the supervisor or SRB and the connected risk-based approach. Supervisors and SRBs may choose to adjust:

a) the level of checks required to perform their licensing/registration function: where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited, and approvals may be made on a review of basic documentation. Where the ML/TF risk associated with the sector is high, supervisors and SRBs may ask for additional information.

b) the type of on-site or off-site AML/CFT supervision: supervisors and SRBs may determine the correct mix of on-site and off-site supervision of legal professionals. Off-site supervision may involve analysis of annual independent audits and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identification of persons responsible for the filing. It may also include undertaking thematic reviews of the sector, making compulsory the periodic information returns from firms. Off-site supervision alone may not be appropriate in higher risk situations. On-site inspections may involve reviewing AML/CFT internal policies, controls and procedures, interviewing members of senior management, compliance officer and other relevant staff, considering gatekeeper's own risk assessments, spot checking CDD documents and supporting evidence, looking at reporting of ML/TF suspicions in relation to clients, legal professionals and other matters, which may be observed in the course of an on-site visit and where appropriate, sample testing of reporting obligations.

c) the frequency and nature of ongoing AML/CFT supervision: supervisors and SRBs should proactively adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from legal professionals' inclusion in thematic review samples).

d) the intensity of AML/CFT supervision: supervisors and SRBs should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of legal professionals' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the legal professionals' risk assessment, CDD, reporting and record-keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of Directors and AML/CFT assessment in particular lines of business.

195. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever

appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to legal professionals to enable them to enhance their RBA.

196. Record keeping and quality assurance are important, so that supervisors can document and test the reasons for significant decisions relating to AML/CFT supervision. Supervisors should have an appropriate information retention policy and be able to easily retrieve information while complying with the relevant data protection legislation. Record keeping is crucial and fundamental to the supervisors' work. Undertaking adequate quality assurance is also fundamental to the supervisory process to ensure decision-making/sanctioning is consistent across the supervised population.

Enforcement

197. R.28 requires supervisors or SRB to have adequate powers to perform their functions, including powers to monitor compliance by legal professionals. R.35 requires countries to have the power to impose sanctions, whether criminal, civil or administrative, on DNFBPs, to include legal professionals when providing the services outlined in R.22(d). Sanctions should be available for the directors and senior management of the firm when a legal professional fails to comply with requirements.

198. Supervisors and SRBs should use proportionate actions, including a range of supervisory interventions and corrective actions to ensure that any identified deficiencies are addressed in a timely manner. Sanctions may range from informal or written warning, censure and reprimand to punitive measures (including disbarment and criminal prosecutions where appropriate) for more egregious non-compliance, as identified weaknesses can have wider consequences. Generally, systemic breakdowns or significantly inadequate controls will result in more severe supervisory response.

199. Enforcement by supervisors and SRBs should be proportionate while having a deterrent effect. Supervisors and SRBs should have (or should delegate to those who have) sufficient resources to investigate and monitor non-compliance. Enforcement should aim to remove the benefits of non-compliance.

Guidance

200. Supervisors and SRBs should communicate their regulatory expectations. This should be done through a consultative process after meaningful engagement with relevant stakeholders, including legal professionals. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. This could include guidance to clarify the interpretation and application of professional privilege and secrecy principle in the context of the nature of services provided by legal professionals.

201. Guidance issued to legal professionals should also discuss ML/TF risk within their sector and outline ML/TF indicators (i.e. red flags) and methods of risk assessment to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways that are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction.

202. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the legal profession, which may cover operational and practical issues, and be more detailed and explanatory in nature. Training

events may also provide an effective means to ensure legal professionals awareness and compliance with AML/CFT responsibilities. Where supervisors cooperate to produce combined guidance across sectors, supervisors should ensure this guidance adequately addresses the diversity of roles that come within the guidance's remit, and that such guidance provides practical direction to all its intended recipients. The private sector guidance should be consistent with national legislation and with any guidelines issued by competent authorities with regard to the legal profession and be consistent with all other legal requirements and obligations.

203. Supervisors should consider communicating with other relevant domestic supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities across sectors (such as legal professionals, accountants and TCSPs). Multiple guidance should not create opportunities for regulatory arbitrage. Relevant supervisory authorities should consider preparing joint guidance in consultation with the relevant sectors, while recognising that in many jurisdictions legal professionals will consider that separate guidance targeted at the legal profession will be the most appropriate and effective form.

204. Information and guidance should be provided by supervisors in an up-to-date and accessible format. It could include sectoral guidance material, findings of thematic reviews, training events, newsletters, internet-based material, oral updates on supervisory visits, meetings and annual reports.

Training

205. Supervisors and SRBs should ensure that their staff, and other relevant employees are trained to assess the quality of ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of the AML/CFT policies, procedures and internal controls. It is recommended that the training has a practical basis/dimension. Supervisory staff should recognise that in implementing the RBA, legal professionals should make reasonable judgements for their particular services and activities. This may mean that no two legal professionals and no two firms are likely to adopt the same detailed practices.

206. Training should allow supervisory staff to form sound judgments about the quality of the risk assessments made by legal professionals and the adequacy and proportionality of AML/CFT controls of legal professionals. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Endorsements

207. Supervisors should avoid mandating the use of AML/CFT systems, tools or software of any third party commercial providers to avoid conflicts of interest in the effective supervision of firms.

Information exchange

208. Supervisors should encourage the information exchange between the public and private sector and within private sector (e.g. between financial institutions and legal professionals) is important for combating ML/TF. Information sharing and intelligence sharing arrangements between supervisors and public authorities (such as Financial

Intelligence Units and law enforcement), where applicable should be robust, secure and subject to compliance with national legal requirements.

209. The type of information that could be shared between the public and private sectors include:

a) ML/TF risk assessments;

b) Typologies (i.e. case studies) of how money launderers or terrorist financers have misused legal professionals;

c) feedback on STRs and other relevant reports;

d) targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with legal professionals as a class or individually; and

e) countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by R.6.

210. Domestic co-operation and information exchange between FIU and supervisors of legal professionals and among competent authorities including law enforcement, intelligence, FIU, tax authorities, supervisors and SRBs is also important for effective monitoring/supervision of the sector. Such co-operation and co-ordination may help avoid gaps and overlaps in supervision and ensure sharing of good practices and findings. Such intelligence should also inform a supervisor's risk-based approach to supervisory assurance. Intelligence about active misconduct investigations and completed cases between supervisors and law enforcement agencies should also be encouraged where appropriate. When sharing information, protocols and safeguards should be implemented in order to protect personal data.

211. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the legal sector, taking into account the multi-jurisdictional reach of many legal professionals.

Supervision of beneficial ownership and source of funds/wealth requirements

212. The FATF Recommendations require competent authorities to have access to adequate, accurate and timely information on the beneficial ownership and control of legal persons (R.24). In addition, countries must take measures to prevent the misuse of legal arrangements for ML/TF, in particular ensuring that there is adequate, accurate and timely information on express trusts (R.25). Implementation of the FATF Recommendations on beneficial ownership has proven challenging. As a result, the FATF developed the *FATF Guidance on Transparency and Beneficial Ownership* to assist countries in their implementation of R.24 and R.25, as well as R.1 as it relates to understanding the ML/TF risks of legal persons and legal arrangements. The FATF and Egmont Group also published the Report on Concealment of Beneficial Ownership in July 2018 which identified issues to help address the vulnerabilities associated with the concealment of beneficial ownership.

213. R.24 and R.25 require countries to have mechanisms to ensure that information provided to registries is accurate and updated on a timely basis and that beneficial ownership information is accurate and current. To determine the adequacy of a system for monitoring and ensuring compliance, countries should have regard to the risk of

AML/CFT in given businesses (i.e. if there is a proven higher risk then higher monitoring measures should be taken). Legal professionals must, however, be cautious in blindly relying on the information contained in registries. Ongoing monitoring is important during a relationship to detect unusual and potentially suspicious transactions as a result of a change in beneficial ownership, as registries are unlikely to provide such information on a dynamic basis.

214. Those responsible for company formation and the creation of legal arrangements fulfil a key gatekeeper role to the wider financial community through the activities they undertake in the formation of legal persons and legal arrangements or in their management and administration. The guidance in relation to beneficial ownership information in this section is intended for legal professionals who are involved in such arrangements by acting in the capacity of a formation agent, company director, company secretary, office for service, nominee or other similar capacity.

215. Legal professionals are also required to undertake and document adequate risk assessment of clients/transactions to fully understand the nature of the underlying clients' business activity. Evidence could include business plans/governance documents, financial statements and company registry filings.

216. As DNFBPs, legal professionals are required to apply CDD measures to beneficial owners of legal persons and legal arrangements to whom they are providing advice or formation services. In some countries, a legal professional may be required for registering a legal person and will be responsible for providing basic and/or beneficial ownership information to the registry. A number of countries have notarial systems where a notary will attest to the accuracy of registry filings.

217. In their capacity as company directors, trustees or foundation officials of these legal persons and legal arrangements, legal professionals often represent these legal persons and legal arrangements in their dealings with other financial institutions and DNFBPs that are providing banking or audit services to these types of client.

218. These financial institutions and other DNFBPs may request the CDD information collected and maintained by legal professionals, who because of their role as director or trustee, will act as the principal point of contact with the legal person or legal arrangement. These financial institutions and other DNFBPs may never meet the beneficial owners of the legal person or legal arrangement.

219. Under R.28, countries should ensure that legal professionals are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which includes identifying the beneficial owner/s and taking reasonable measures to verify them. R.24 and R.25, which deal with transparency of beneficial ownership of legal persons and legal arrangements, require countries to have mechanisms for ensuring that adequate, accurate and up-to-date information is available on a timely basis on these legal entities.

220. In accordance with R.28, legal professionals should be subject to risk-based supervision by a supervisor or SRB covering the beneficial ownership and record-keeping requirements of R.10 and R.11. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current basic and beneficial ownership information on legal persons and legal arrangements is maintained and will be available on a timely basis to competent authorities.

221. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which legal professionals have established to identify and record the beneficial owner. In addition, they should undertake sample testing of client records on a representative basis to gauge the effectiveness of the application of those measures and the accessibility of accurate beneficial ownership information.

222. During on-site and offsite inspections, the supervisor or SRB should examine the policies, procedures and controls that are in place for on-boarding of new clients to establish what information and documentation is required where the client is a natural person or legal person or arrangement. The supervisor or SRB should verify the adequacy of these procedures and controls to identify beneficial owners to understand the ownership and control structure of these legal persons and arrangements and to ascertain the business activity. For example, self-declaration on beneficial ownership provided by the client without any other mechanism to verify the information may not be adequate in all cases.

223. Sample testing of records will assist the supervisor or SRB in determining whether controls are effective for the accurate identification of beneficial ownership, accurate disclosure of that information to relevant parties and for establishing if that information is readily available. The extent of testing will be dependent on risk but the records selected should reflect the profile of the client base and include both new and existing clients.

224. The supervisor or SRB should consider the measures the legal professional has put in place for monitoring changes in the beneficial ownership of legal persons and legal arrangements to whom they provide services to ensure that beneficial ownership information is accurate and current and to determine how timely updated filings are made, where relevant to a registry.

225. During examinations, the supervisor or SRB should consider whether to verify the beneficial ownership information available on the records of the legal professional with that held by the relevant registry, if any. The supervisor or SRB may also consider information from other competent authorities such as FIUs, public reports and information from other financial institutions or DNFBPs, to verify the efficacy of the legal professional's controls.

Sources of funds and wealth

226. Legal professionals should be subject to risk-based supervision by a supervisor or SRB covering the requirements to identify and evidence the source of funds and source of wealth for higher risk clients to whom they provide services. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current information on sources of funds and wealth is properly evidenced and available on a timely basis to competent authorities. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which legal professionals have established to identify and record sources of wealth in arrangements.

Nominee arrangements

227. A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the beneficial owner.

228. A nominee shareholder is a natural or legal person who is officially recorded in the register of members and shareholders of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held on trust or through a custodial agreement.

229. In a number of countries, legal professionals act or arrange for another person (either an individual or corporate) to act as a director and act or arrange for another person (either an individual or corporate) to act as a nominee shareholder for another person as part of their professional services. In accordance with R.24, one of the mechanisms to ensure that nominee shareholders and directors are not misused is by subjecting these legal professionals to licensing and recording their status in company registries. Countries may rely on a combination of measures in this respect.

230. There are legitimate reasons for a legal professional to act as or provide directors to a legal person or act or provide nominee shareholders. These may include the settlement and safekeeping of shares in listed companies where post traded specialists act as nominee shareholders. However, nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of the person from whom they will take instructions from or whom they represent. They are sometimes referred to as "strawmen".

231. Nominee directors and nominee shareholders can create obstacles to identifying the true beneficial owner of a legal person, particularly where the status is not disclosed. This is because it will be the identity of the nominee that is disclosed in the corporate records of the legal person held by a registry and in the company records at its registered office. Company law in various countries does not recognise the status of a nominee director because in law it is the directors of the company who are liable for its activities and the directors have a duty to act in the best interest of the company.

232. The supervisor or SRB should be aware that undisclosed nominee arrangements may exist. They should consider whether undisclosed nominee arrangements would be identified and addressed during their on-site and offsite inspections and examination of the policies, procedures, controls and client records of the legal professional, including the CDD process and ongoing monitoring by the legal professional.

233. An undisclosed nominee arrangement may exist where there are the following (non-exhaustive) indicators:

a) the profile of a director or shareholder is inconsistent with the activities of the company;

b) the individual holds numerous appointments to unconnected companies;

c) a director's or shareholder's source of wealth is inconsistent with the value and nature of the assets within the company;

d) funds into and out of the company are sent to, or received from unidentified third party/ies;

e) the directors or shareholders are accustomed to acting on instruction of another person; and

f) requests or instructions are subject to minimal or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the director/s.

Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom a legal professional provides services

1. Taking a RBA, the amount of information that should be obtained by the legal professional will depend on whether the legal professional is establishing or administering the trust, company or other legal entity or is acting as or providing a trustee or director of the trust, company or other legal entity. In these cases, a legal professional will be required to understand the general purpose behind the structure and the source of funds in the structure in addition to being able to identify the beneficial owners and controlling persons. A legal professional who is providing other services (e.g. acting as registered office) to a trust, company or other legal entity will be required to obtain sufficient information to enable it to be able to identify the beneficial owners and controlling persons of the trust, company or other legal entity.

2. A legal professional that is not acting as trustee may, in appropriate circumstances, rely on a synopsis prepared by another legal professional or accountant or TCSP providing services to the trust or relevant extracts from the trust deed itself to enable the legal professional to identify the settlor, trustees, protector (if any), beneficiaries or natural persons exercising effective control. This is in addition to the requirement, where appropriate, to obtain evidence to verify the identity of such persons as discussed below.

In relation to a trust

3. As described above, depending on the services being provided to the trust, a legal professional should have policies and procedures in place to identify the following and verify their identity using reliable, independent source documents, data or information (provided that the legal professional's policies should enable it to disregard source documents, data or information that are perceived to be unreliable) as described in more detail below:

i. the settlor;

ii. the protector;

iii. the trustee(s), where the legal professional is not acting as trustee;

iv. the named beneficiaries or class of beneficiaries, and

v. any other natural person actually exercising effective control over the trust.

Settlor

a) A settlor is generally any person (or persons) by whom the trust is made. A person is a settlor if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the settlor must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration).

b) A settlor may or may not be named in the trust deed. Legal professionals should have policies and procedures in place to identify and verify the identity of the real economic settlor.

c) A legal professional establishing on behalf of a client or administering a trust, company or other legal entity or otherwise acting as or providing a trustee or director of a trustee, company or other legal entity should have policies and procedures in place (using a RBA) to identify the source of funds in the trust, company or other legal entity.

d) It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift or letter of wishes.

e) Where assets have been transferred to the trust from another trust, it will be necessary to obtain this information for both transferee and transferor trust.

Beneficiaries

a) Legal professionals should have policies and procedures in place, adopting a RBA to enable them to form a reasonable belief that they know the true identity of the beneficiaries of the trust, and taking reasonable measures to verify the identity of the beneficiaries, such that the legal professionals are satisfied that they know who the beneficiaries are. This does not require the legal professional to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the legal professionals should at least identify and verify the identity of beneficiaries who have current fixed rights to distributions of income or capital or who actually receive distributions from the trust (e.g. a life tenant).

b) Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), legal professionals should obtain information to enable them to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).

c) Where beneficiaries are identified by reference to a class (e.g. children and issue of a person) or where beneficiaries are minors under the law governing the trust, although legal professionals should satisfy themselves that these are the intended beneficiaries (e.g. by reference to the trust deed), they are not obliged to obtain additional information to verify the identity of the individual beneficiaries referred to in the class unless or until the trustees determine to make a distribution to such beneficiary.

d) In some trusts, named individuals only become beneficiaries on the happening of a particular contingency (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, a legal professional is not required to obtain additional information to verify the identity of such contingent beneficiaries unless or until the contingency is satisfied or until the trustees decide to make a distribution to such a beneficiary.

e) A legal professional who administers the trust or company or other legal entity owned by a trust or otherwise provides or acts as trustee or director to the trustee, company or other legal entity should have procedures in place so that there is a requirement to update the information provided if named beneficiaries are added or removed from the class of beneficiaries, or beneficiaries receive distributions or benefits for the first time after the

information has been provided, or there are other changes to the class of beneficiaries.

f) A legal professional is not obliged to obtain other information about beneficiaries other than to enable the legal professional to satisfy itself that it knows who the beneficiaries truly are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust is a PEP.

Natural person exercising effective control

a) A legal professional providing services to the trust should have procedures in place to identify any natural person exercising effective control over the trust.

b) For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:

   i. dispose of or invest (other than as an investment manager) trust property;

   ii. direct, make or approve trust distributions;

   iii. vary or terminate the trust;

   iv. add or remove a person as a beneficiary or to or from a class of beneficiaries; and/or

   v. appoint or remove trustees.

c) A legal professional who administers the trust or otherwise acts as trustee must, in addition, also obtain information to satisfy itself that it knows the identity of any other individual who has power to give another individual "control" over the trust; by conferring on such individual powers as described in paragraph (b) above.

Corporate settlors and beneficiaries

4. These examples are subject to the more general guidance on what information should be obtained by the legal professional to enable it to identify settlors and beneficiaries. It is not intended to suggest that a legal professional must obtain more information about a beneficiary that is an entity where it would not need to obtain such information if the beneficiary is an individual.

   a) In certain cases, the settlor, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, a legal professional should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to the entity.

   b) In the case of a settlor which is a legal entity, a legal professional should satisfy itself that it has sufficient information to understand the purpose behind the formation of the trust by the entity. For example, a company may establish a trust for the benefit of its employees or a legal entity may act as nominee for an individual settlor or on the instructions of an individual who has provided funds to the legal entity for this purpose. In the case of a legal entity acting as nominee for an individual settlor or on the instructions of an individual, the legal professional should take steps to satisfy itself as to the identity of the economic settlor of the trust (i.e. the person who has provided funds to the

legal entity to enable it to settle funds into the trust) and the controlling persons in relation to the legal entity at the time the assets were settled into trust. If the corporate settlor retains powers over the trust (e.g. a power of revocation), the legal professional should satisfy itself that it knows the current beneficial owners and controlling persons of the corporate settlor and understands the reason for the change in ownership or control.

c) In the case of a beneficiary which is an entity (e.g. a charitable trust or company), a legal professional should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, the legal professional should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate trustee

a) Where a legal professional is not itself acting as trustee, it is necessary for the legal professional to obtain information to enable it to identify and verify the identity of the trustee (s) and, where the trustee is a corporate trustee, identify the corporate entity, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity.

b) Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the legal professional should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. The legal professional can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the website of the body that regulates the trustee and of the regulated trustee itself).

c) It is not uncommon for families to set up trust companies to act for trusts for the benefit of that family. These are typically called private trust companies and may have a restricted trust licence that enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, the legal professional should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, the legal professional does not need to obtain detailed information to identify the directors or controlling persons of that entity that acts as shareholder of the private trust company.

Individual and Corporate protector

a) Where a legal professional is not itself acting as a protector and a protector has been appointed, the legal professionals should obtain information to identify and verify the identity of the protector.

b) Where the protector is a legal entity, the legal professional should obtain sufficient information that it can satisfy itself who is the controlling person and beneficial owner of the protector, and take reasonable measure to verify their identity.

c) Where the protector is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the legal professional should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. The legal professional can rely on external evidence, such as information in the public domain to satisfy itself as to the beneficial owner of the regulated protector (e.g. the website of the body that regulates the protector and of the regulated protector itself).

Annex 2: Sources of further information

1. Various sources of information exist that may help governments and legal professionals in their development of a RBA. Although not an exhaustive list, this Annex highlights a number of useful web-links that governments and legal professionals may wish to draw upon. They provide additional sources of information, and further assistance might also be obtained from other information sources such as AML/CFT assessments.

Legislation and Court Decisions

2. The rulings by the ECJ of June 26th, 2007 by the Belgium Constitution Court of January 23rd 2008 and the French Conseil d'État of April 10th, 2008 confirmed that AML/CFT regulation cannot require or permit the breach of the legal professional's duty of professional secrecy when performing the essential activities of the profession.

3. The Court of First Instance in the Joined Cases T-125/03 &T-253/03 Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v Commission of the European Communities has restated the ruling in the AM&S case that professional secrecy "meets the need to ensure that every person must be able, without constraint, to consult a legal professional whose profession entails the giving of independent legal advice to all those in need of it (AM&S, paragraph 18). That principle is thus closely linked to the concept of the legal professional's role as collaborating in the administration of justice by the courts (AM&S, paragraph 24).

4. In Judgement of the Court (Grand Chamber) of 26 June 2007 in Case C-305/05 in a question referred for a preliminary ruling, the Court holds that "the obligations of information and of cooperation with the authorities responsible for combating money laundering [...] and imposed on legal professionals by Article 2a(5) of Directive 91/30848, account being taken of the second subparagraph of Article 6(3)49 thereof, do not infringe the right to a fair trial as guaranteed by Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 6(2) EU". The Court reaches this conclusion by considering that: (i) obligations of information and cooperation apply to legal professionals only in so far as they advise their client in the preparation or execution of certain transactions; (ii) as soon as the legal professional acting in connection with a transaction is called upon for assistance in defending the client or in representing him before the courts, or for advice as to the manner of instituting or avoiding judicial proceedings, that

[48] Article 2a(5) of Directive 91/308 listed the specified transactional activities in whose performance legal professionals were to be considered as obliged entities.

[49] According to which "Member States shall not be obliged to apply the obligations laid down in paragraph 1 to notaries, independent legal professionals, auditors, external accountants and tax advisors with regard to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning, judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings".

legal professional is exempt from the obligations of information and cooperation, regardless of whether the information has been received or obtained before, during or after the proceedings. An exemption of that kind safeguards the right of the client to a fair trial; (iii) the requirements relating to the right to a fair trial do not preclude the obligations of information and cooperation from being imposed on legal professionals acting specifically in connection with the specified activities, in cases where the second subparagraph of Article 6(3) of that directive does not apply, where those obligations are justified by the need to combat money laundering effectively, in view of its evident influence on the rise of organised crime"[50].

5. **Michaud v. France case of 6 December 2012**. This case concerned the obligation on French legal professionals to report their suspicions regarding possible ML activities by their clients. Among other things, the applicant, a member of the Paris Bar and the Bar Council, submitted that this obligation, which resulted from the transposition of European directives, was in conflict with Article 8 of the European Convention on Human Rights, which protects the confidentiality of lawyer-client relations.

6. The European Court of Human Rights in its judgement held that there had been no violation of Article 8 of the Convention. While stressing the importance of the confidentiality of lawyer-client relations and of legal professional privilege, it considered, however, that the obligation to report suspicions pursued the legitimate aim of prevention of disorder or crime, since it was intended to combat ML and related criminal offences, and that it was necessary in pursuit of that aim. The Court held that the obligation to report suspicions, as implemented in France, did not interfere disproportionately with legal professional privilege, since legal professionals were not subject to the above requirement when defending litigants and the legislation had put in place a filter to protect professional privilege, thus ensuring that legal professionals did not submit their reports directly to the authorities, but to the president of their Bar association.

7. Directive (EU) 2015/849 (AMLD) provides:

   - Art. 2 AMLD: 1. This Directive shall apply to the following obliged entities: […] (3) the following natural or legal persons acting in the exercise of their professional activities: […] (b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the: (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets; (iii) opening or management of bank, savings or securities accounts (iv) organisation of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of trusts, companies, foundations, or similar structures;

8. Art. 34(2): "Member States shall not apply the obligations laid down in Article 33(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors ***only to the strict extent that such exemption*** relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of

[50] http://curia.europa.eu/juris/liste.jsf?language=en&num=C-305/05

defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings"[51].

9. In the United States there is a "crime-fraud" exception to attorney-client privilege. See, e.g. Am. Law Institute, Restatement of the Law Third, Restatement of the Law Governing Lawyers §82 Client Crime or Fraud (2000). As the U.S. Supreme Court observed, "[i]t is the purpose of the crime-fraud exception to the attorney-client privilege to assure that the 'seal of secrecy' … between legal professional and client does not extend to communications 'made for the purpose of getting advice for the commission of a fraud.'" *United States v. Zolin*, 491 U.S. 554, 562 (1989) (internal citation omitted). Before determining whether this exception applies, there must be a showing of "a factual basis adequate to support a good faith belief by a reasonable person that *in camera* review of the materials may reveal evidence to establish a claim that the crime-fraud exception applies." *Id.* at 572. Under case law in the U.S. further developing this principle, the crime-fraud exception can apply even where the attorney acts innocently—"the lawyers' innocence does not preserve the attorney-client privilege against the crime-fraud exception. The privilege is the client's, so it is the client's knowledge and intentions that are of paramount concern to the application of the crime-fraud exception; the attorney need know nothing about the client's ongoing or planned illicit activity for the exception to apply." *United States v. Chen*, 99 F.3d 1495, 1504 (9th Cir. 1996) (internal quotations omitted). Under these principles, persons (both legal and natural) have been obliged to disclose pursuant to subpoenas or other legal process factual information that otherwise would have been subject to attorney-client privilege. *See, e.g. In re Grand Jury*, 705 F.3d 133, 155-61 (3d Cir. 2012).

Guidance on the Risk-based Approach

1. Law Society of Ireland: www.lawsociety.ie[52].
2. Law Society of England and Wales: www.lawsociety.org.uk
3. Law Society of Hong Kong: www.hklawsoc.org.hk
4. Organisme d'autoréglementation de la Fédération Suisse des Avocats et de la Fédération Suisse des Notaires (SRO SAV/SNV): home page: snv.ch/www.sro-sav-snv.ch/fr/02_beitritt/01_regelwerke.htm/02_Reglement.pdf (art.41 to 46)
5. The Netherlands Bar Association: www.advocatenorde.nl
6. The Royal Dutch Notarial Society: www.notaris.nl
7. The American Bar Association Voluntary Good Practices Guidance for Legal professionals to Detect and Combat Money Laundering and Terrorist Financing, published 23 April 2010, available on the ABA website: www.americanbar.org.

[51] Article 33(1) of the Directive refers to reporting STRs to the FIU

[52] AML guidance and other AML resources available to solicitors in Ireland by logging into the members area www.lawsociety.ie/aml

8. The American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 463 on the Voluntary Good Practices Guidance, published 23 May, 2013, available on the ABA website: www.americanbar.org.
9. A Lawyer's Guide to Detecting and Preventing Money Laundering, collaborative publication of the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, published October 2014, available on the IBA website: www.ibanet.org.
10. The FATF Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, 2013, Chapters 4 and 5.
11. Comparative research published by the Solicitors Regulation Authority about ML/TF vulnerabilities observed by the SRA in England and Wales.
12. Comparative Guidance for the legal sector in England and Wales, published by the Legal Sector Affinity Group and approved by HM Treasury.

Other sources of information to help assist countries' and legal professionals' risk assessment of countries and cross-border activities

10. In determining the levels of risks associated with particular country or cross border activity, legal professionals and governments may draw on a range of publicly available information sources. These may include reports that detail observance of international standards and codes, specific risk ratings associated with illicit activity, corruption surveys and levels of international co-operation. A non-exhaustive list is as follows:

    i. IMF and World Bank Reports on observance of international standards and codes (Financial Sector Assessment Programme)

       WB reports:
       http://documents.worldbank.org/curated/en/docsearch/document-type/904559

       a. IMF: www.imf.org/external/NP/rosc/rosc.aspx

    ii. OECD Sub Group of Country Risk Classification (a list of country of risk classifications published after each meeting) www.oecd.org/trade/topics/export-credits/arrangement-and-sector-understandings/financing-terms-and-conditions/country-risk-classification/

    iii. Egmont Group of financial intelligence units that participate in regular information exchange and the sharing of good practice www.egmontgroup.org/

    iv. Signatory to the United Nations Convention against Transnational Organized Crime www.unodc.org/unodc/crime_cicp_signatures_convention.html

    v. The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury economic and trade, Sanctions Programmes www.ustreas.gov/offices/enforcement/ofac/programs/index.shtml

vi. Consolidated list of persons, groups and entities subject to EU Financial Sanctions: https://data.europa.eu/euodp/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions

vii. Joint Guidelines of the European Supervisory Authorities (ESA) on anti-money laundering risk and counter terrorist financing https://esas-joint-committee.europa.eu/Publications/Guidelines

Annex 3: Glossary of terminology

Beneficial Owner

Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Competent Authorities

Competent authorities refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency and bearer negotiable instruments (BNIs); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.

Core Principles

Core Principles refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

Designated Non-Financial Businesses and Professions (DNFBPs)

Designated non-financial businesses and professions means:

a) Casinos (which also includes internet and ship based casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the FATF Recommendations, and which as a business, provide any of the following services to third parties:

   - Acting as a formation agent of legal persons;
   - Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

Express Trust

Express trust refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts that come into being through the operation of the law and that do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).

FATF Recommendations

Refers to the FATF 40 Recommendations.

Legal Person

Legal person refers to any entities other than natural persons that can establish a permanent client relationship with a legal professional or otherwise own property. This can include bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Legal Professional

In this Guidance, the term *"Legal professional"* refers to lawyers, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Foreign and *domestic PEPs* are individuals who are or have been entrusted by a foreign country or domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Red Flags

Any fact or set of facts or circumstances that, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A *"red flag"* may be used as a short hand for any indicator of risk that puts an investigating legal professional on notice that further checks or other appropriate safeguarding actions will be required. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, as a client may be able to provide a legitimate explanation. Red flag indicators should assist legal professionals in applying a risk-based approach to their CDD requirements. Where there are a number

of red flag indicators, it is more like4ly that a legal professional should have a suspicion that ML or TF is occurring.

Self-regulatory body (SRB)

A *SRB* is a body that represents a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons who are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

Supervisors

Supervisors refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("financial supervisors") and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

Annex 4: Supervisory practices for implementation of the RBA

Ireland

AML/CFT Compliance Monitoring in Ireland

The Law Society of Ireland is the educational, representative and regulatory body of the solicitors' profession in Ireland. In addition to the statutory functions it exercises under the Solicitors Acts, the Society is also the competent authority for the monitoring of solicitors for the purposes of compliance with Ireland's anti-money laundering and counter-terrorist financing laws under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended.

The Society uses a risk-based system when choosing firms for inspection in addition to conducting a number of random inspections. For many years, firms have been chosen for inspection on the basis of pre-determined risk factors which trigger an accounts inspection. These risk factors include:

- complaints by the public
- previous investigation experience
- the contents of the firm's annual reporting accountant's report
- delays in complying with filing obligations in relation to accountants reports and practicing certificates
- professional indemnity insurance issues
- judgement debts
- media reports
- notifications of concern by government authorities including An Garda Síochána and the Revenue Commissioners

AML/CFT compliance checks are carried out in conjunction with the Society's financial regulation of solicitors' firms. When AML/CFT deficiencies are discovered, targeted standalone checks are implemented until any deficiencies are satisfactorily removed. The process available to compel compliance and used in the past is outlined below.

- If a solicitor fails to implement procedures to combat ML/TF, a report is submitted to the Regulation of Practice Committee who will require the solicitor to provide it with a copy of their new written AML/CFT procedures and evidence that those procedures have been communicated to all staff and will be implemented in full.
- Where it is suspected that a solicitor has committed a substantive offence of ML/TF or failed to fulfil reporting obligations, the matter is referred to the Money Laundering Reporting Committee of the Law Society for appropriate action.
- The experience of the Law Society to date has been that the failure to implement AML/CFT procedures tends to reflect a failure of the solicitor to implement satisfactory procedures to ensure compliance with the

Solicitors Act, in particular the provisions of the Solicitors Accounts Regulations. When a solicitor fails to implement satisfactory procedures to ensure compliance with the Solicitors Accounts Regulations and with the Solicitors (ML and TF) Regulations, the Society will re-investigate the firm until such time that satisfactory procedures have been put in place. If the solicitor does not implement satisfactory procedures, the matter may be referred to the Solicitors Disciplinary Tribunal.

- If it comes to the attention of the Law Society that a solicitor has been engaged in dishonesty particularly in relation to clients' monies (which may occur in parallel with activity suspected to be related to ML/TF), a number of sanctions can be applied, including:
  - An application to the President of the High Court for an Order immediately suspending that solicitor from practice.
  - An application for an Order that no bank shall make any payment from any bank account held by that solicitor or under that solicitor's control.
  - An application for an Order that any documents held by the solicitor be immediately delivered to the Law Society or its nominee.
- In addition to supervision, the Law Society also engages in a range of other AML/CFT outreach and engagement activities including:
  - Awareness raising via a dedicated AML web resource hub, eZine articles, Gazette and email alerts
  - The development of AML Guidance Notes - these are comprehensive notes covering all AML/CFT obligations and ML/TF risks, which follow a question and answer format for ease of reference. They also contain a dedicated chapter providing a non-exhaustive list of indicators of potential suspicious circumstances.
  - In November 2018, supplementary guidance was provided to solicitors to help with new obligations which transpose 4AMLD. Topics covered include how to conduct a Business Risk Assessment, update Policies, Controls and Procedures, and carry out Customer Risk Assessments and 4AMLD changes to CDD measures.
  - Tailored guidance via an Anti-Money Laundering Helpline. This helpline receives queries from solicitors about AML on a daily basis and provides real-time specific guidance. The helpline provides a vital confidential support service to solicitors when navigating potential red flags and deciding whether or not to proceed with a legal service. The Society's guidance is to document their thought process with a particular emphasis on the risk of committing the substantive offence of money laundering should they provide a legal service which may exhibit red flags. In this way, the service can help prevent unwitting facilitation of money laundering by solicitors.
  - AML Education is provided to trainee solicitors attending qualifying courses in the Law Society. In addition, for qualified solicitors, AML modules feature on the Law Society's Diploma and CPD courses. Throughout 2017, for example, the Society delivered extensive AML training across the country and online through a total of 9 seminars with 2 379 attendees.

- CPD Regulations 2015 (S.I. No. 480/2015) require firms to appoint an AML Compliance Partner (failure to do so will mean that each partner in the firm will be designated as an AML Compliance Partner). The AML Compliance Partner must annually undertake a minimum of 3 hours training in regulatory matters, of which at least 2 hours shall be accounting and AML compliance. Training during 2017 has had a measurable impact on the awareness of solicitors of their AML obligations and ML/TF risks evidenced by increased demand for AML guidance in the days following an AML seminar.

France

The CARPA is a verification and regulation system under the responsibility of the Bar Council in France. It applies to all handling of funds received by lawyers on behalf of their clients. It conducts verification under the authority of the Chairman of the Bar Council and has a role in the fight against ML/TF. TRACFIN, the French FIU has an interest in the CARPA, guaranteeing the traceability of all financial flows. The rules of the CARPA system are as follows:

Any handling of funds made by a lawyer must be related to a legal or judicial act.

Any handling of funds made by a lawyer on behalf of his clients must be routed through CARPA (with the sole exception that trusts do not enter into the scope of intervention of CARPA in the current state of the law).

The bank account is opened in the name of CARPA, in which the funds received by the lawyers are deposited on behalf of their clients.

A lawyer cannot receive funds or give instructions to pay them to the beneficiaries without the prior verification of CARPA exercised under the authority and the responsibility of the Bar Council and of the Chairman of the Bar Council. The verifications concern, in particular:

i. the nature and the description of the case;

ii. the origin of the funds;

iii. the destination of the funds;

iv. the actual beneficiary of the transaction; and

v. the connection between the financial payment and the legal or judicial transaction carried out by the lawyer in the framework of his professional activity.

CARPA can reject a transaction if it cannot verify the above elements.

The CARPA is not a financial institution and is backed by a bank. As the CARPA is under the authority of the Bar Council and the Chairman of the Bar Council, lawyers have the obligation to provide the necessary explanations for the CARPA to operate without being able to rely upon professional secrecy (which would apply if they were dealing with a bank). The controls thus exercised by the CARPA on the one hand and by its bank

on the other intersect in a complementary way with regard to professional secrecy.

Malaysia

AML/CFT Supervisory Practices of Legal Professionals in Malaysia

A. Fit and Proper Requirements – Self-Regulatory Bodies (SRBs)

In Malaysia, the legal professionals are regulated under the Legal Profession Act 1976, Advocate Ordinance Sabah 1953 and Advocate Ordinance Sarawak 1953, respectively. Prior to admission to the Bar, they are subject to appropriate market entry controls in which they are required to fulfil the "fit and proper" requirements under their respective governing legislation. Practising certificates will be subsequently issued by the High Court of Malaya and High Court of Sabah and Sarawak in conjunction with the respective SRBs for legal professionals, i.e. Bar Council Malaysia (BC) and Sabah Law Society (SLS) as the SRBs, as well as Advocates Association of Sarawak (AAS).

B. AML/CFT Risk-based Supervision – Bank Negara Malaysia (BNM)

Under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), BNM is the designated supervisory authority for the AML/CFT supervision of the Designated Non-Financial Businesses and Professions (DNFBPs) & Other Financial Institutions in Malaysia, including legal professionals.

BNM adopts a risk-based approach supervision on legal professionals, in which the differentiation is guided by the outcome of the National Risk Assessment (NRA) and the application of Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF), as follows:

i. National Risk Assessment (NRA) 2017

Malaysia's third iteration of the NRA in 2017 comprising assessment of ML/TF inherent risk and overall control effectiveness had stipulated the legal professionals' net ML and TF risks as **"MEDIUM HIGH"** and **"MEDIUM"** level, respectively, as exacerbated by the sector's marginal control, as follows:

ML		TF	
Inherent Risk	Medium	Inherent Risk	Low
Control	Marginal	Control	Marginal
Net Risk	Medium High	Net Risk	Medium

ii. Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF)

D'SuRF encapsulates end-to-end governance and supervisory process, risk-based application of supervisory tools. In line with the ML/TF rating of the sector and the application of D'SuRF, the frequency and intensity of monitoring on legal professionals are guided accordingly to include a range of supervisory tools, as follows:

On-site Examination

Firms are selected based on a robust selection process under the D'SuRF, which is in line with the risk profile of the reporting institutions (RIs). The on-site examination is in-depth, with assessments covering the RIs' inherent risk and quality of risk management.

In applying RBA, BNM imposes post-onsite follow-up measures for RIs with heightened risks. This includes requiring the RI to submit proposals to BNM on planned measures to rectify any supervisory issues and progress report until full rectification. The D'SuRF sets the deadline for both submissions. The follow-up measures have been imposed on a number of legal firms selected for on-site examination, highlighting the higher risk of the sector and consistent with the most recent NRA results.

Off-site Monitoring and Supervisory Outreach Activities

Apart from on-site examinations, BNM employs a range of off-site monitoring and supervisory outreach activities, aimed to elevate awareness and guide the implementation of the AMLA requirements by legal professionals. These off-site tools are also deployed according to the RBA, whereby the intensity and frequency for the legal professions is relatively higher compared to other sectors. Among the off-site monitoring, includes the submission of Data and Compliance Reports and internal audit reports. In addition, BNM and the relevant SRBs conduct periodic nationwide AML/CFT outreach and awareness programmes.

Spain

General Council of the Notariat of Spain – Money Laundering Centralised Prevention Body

On 28/12/2005 the Spanish General Council of the Notariat established, pursuant to Ministerial Order 2963/2005, of 20 September 2005, regulating the Centralised Prevention Body, a body specialising in the self-regulation of notarial organisation, as permitted by the INR.23 "*Countries may allow lawyers, notaries, other legal professionals and independent accountants to send their STRs to their appropriate self-regulatory organisations, provided that there are adequate forms of cooperation between these organisations and the FIU*."

This Body takes on certain obligations in the name of notaries:

- Transaction's analysis.

- Communication of suspicious transactions to the FIU.
- Preparation of sector risk analysis
- Preparation of risk-based AML/TF Internal Policies and Procedures.
- Definition of risk indicators for the notarial sector.
- Training of notaries and employees.
- Supervision of the fulfilment of AML/CTF obligations by notaries.

It intersects between the FIU and notaries, with the generic mission of intensifying collaboration between the notariat and authorities in fight against ML/TF. It has drawn up guides, manuals, FAQ documents, best practice documents; prepared in-house databases to improve the application of CDD at notary offices; resolved more than 7 000 consultations from notary offices; designed on-line training programmes; developed in-person training courses for notaries and employees; established a single matrix of common risk indicators; conducted a sectoral risk analysis; implemented remote supervision of all notary offices and in-person supervision at over 80 notarial practices, among other activities.

The AML system used by Spain's notaries represents a considerable advance for Public Authorities, which thanks to its implementation now have access to:

- A new source of valuable information: notarial indexes (a single database with information on all the public instruments and policies notarised and witnessed in the country). This information, processed in an integrated and automated manner to detect potential ML/TF operations
- A body with AML specialists operating the database, who manage the database, analyse and report to the FIU high-risk operations on behalf of notaries and who can analyse not only the transactions of each notary office (as would be the case if there were no centralised body) but all notary offices together.

The system also offers advantages for notaries, who can delegate the management of (and in practice are relieved from) some of their duties (analysing and, where applicable, reporting operations with evidence of ML/TF, training, internal procedures, etc.) to a team of experts working on their behalf.

General Council of the Notariat of Spain – Practices for Due Diligence: Beneficial Ownership Database

On 24 March 2012, the General Council of the Notariat resolved to set up the "Beneficial Ownership Database" ("Base de Datos de Titular Real", or "BDTR") personal data filing system, and in compliance with data protection regulations published this resolution in the Official State Gazette on 28 April 2012.

The resolution allowed for information to be accessed:

- By notaries, as they are subject to AML obligations.
- By the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (Spanish FIU) to fulfil the tasks entrusted to the Service.
- By the court, taxation, law enforcement and administrative authorities responsible for the prevention and investigation of money laundering.
- By other parties subject to Prevention of Money Laundering Act 10/2010, of 28 April 2010, on the terms set out therein.

Article 6 of Royal Decree 304/2014, of 5 May, approving the Regulation of Prevention of Money Laundering and Terrorist Financing Act 10/2010, of 28 April, established in Spanish law that "*for fulfilment of the obligation to identify and verify the identity of the beneficial owner established in this article, the parties subject to this Act may access the database of beneficial ownership of the General Council of the Notariat …*"

As a result, not only notaries but also all parties subject to AML requirements may consult the BDTR to facilitate compliance with Due Diligence obligations. This thus allows the FIU and Law Enforcement Agencies to obtain information on owners with a percentage of less than 25% (full corporate regime) at Spanish private limited liability companies, on any given date. They may also request information on which companies a natural person owns (reverse beneficial ownership) on any given date.

Two levels of information quality is ensured:

- Information based on a statement to a public official (foreign companies, foundations, associations, Spanish corporations).
- Information verified in accordance with the sale and purchase transaction of the shares of Spanish Private Limited Liability Companies.

The General Council of the Notariat has established agreements with associations of parties subject to AML obligations (banks, savings banks, investment firms, auditors, lawyers, lottery agencies, credit institutions,

casinos, etc.) and has provided the information called for in more than 2 000 000 requests made to these applicants.

UK

Supervisory Approach of the Solicitors Regulation Authority

The Solicitors Regulation Authority (SRA) regulates solicitors and their firms, as well as other lawyers and non-lawyer managers working in law firms across England and Wales. The SRA also regulates those working as registered European lawyers or registered foreign lawyers. The SRA seeks to protect the public by ensuring that solicitors meet high standards and by acting when risks are identified. With regards to the Money Laundering Regulations, two thirds of firms that the SRA supervises (67%) offer services that fall within scope, the two main categories being acting as an independent legal professional or acting as a trust or company services provider

There are significant barriers to entry to the profession. Requirements include having a qualifying law degree, followed by the Legal Practice Course and then a two-year period of recognised training incorporating the Professional Skills Course. Character and suitability test is also conducted before admission to the roll of solicitors. The SRA requires firms to obtain approval of owners and managers. Firms are required to have Compliance Officers of Legal Practice (COLPs) and Compliance Officers of Financial Administration (COFAs) approved by the SRA. They should have sufficient seniority and independence. Firms are also required to declare whether they are doing work within scope of the Money Laundering Regulations. Those firms in scope of the Regulations must submit an additional application form to declare any individual who is applying to register as a beneficial owner, officer or manager (BOOM).

Risk-based approach

The SRA carries out both qualitative and quantitative risk assessment of how the regulated community is exposed to ML/TF. Each firm is given a risk rating, which informs the supervisory approach of the SRA. Supervisory activities fall into two broad categories: i) reactive work (responding to concerns and breaches); and ii) proactive work (e.g. engaging with firms to prevent breaches, identify potential breaches, explore risks, enhance risk understanding and provide evidence of poor and good behaviours). The SRA uses the information/intelligence that it receives to build a firm's profile. The assessment takes into account the specific breach alleged, the severity of the allegation, the quality of the information and their ability to investigate. Information is coded and then RAG rated (red, amber or green, with red being the most severe). Reports received are risk assessed and conduct matters are created for

matters assessed as high or medium. Those with an AML/CFT angle often leads to an onsite investigation where the main issues are considered, and a fact-based report produced.

Enforcement: The SRA has a number of enforcement tools. This includes letter of advice, finding and warning, reprimand, severe reprimand and rebuke, based on the gravity of violation. The SRA also has powers to impose fines on individuals and firms. In cases of serious misconduct, the SRA can refer a case to the Solicitors Disciplinary Tribunal, which can impose higher fines and also has powers to suspend or strike off. The SRA has the power to disqualify individuals from involvement in specific roles in certain types of firms. It can also prosecute for information offences or acting as a bogus firm and can revoke authorisations or withdraw approvals. The SRA can also prevent non-lawyers from working within legal businesses.

US

Fit and Proper requirements: Lawyers[53] in the United States

The discussion below describes the fit and proper requirements in the US, which is the country with the largest number of lawyers subject to an alternative supervisory system.

The highest court of the state in which a lawyer is licensed is responsible for adopting the version of the Model Rules of Professional Conduct applicable in that state and for enforcing the duties of lawyers under those rules. State bar associations or independent agencies created by court rules serve as licensing, regulatory, and disciplinary agencies of the court.

The US system regulates lawyers throughout their careers and includes rigorous controls on lawyers. These controls begin with the rules on the bar admission and are designed, among other things, to prevent criminals from becoming or controlling lawyers and to detect effectively any breaches that might occur.

Entry Requirements: Legal education in the US is a post graduate program, not an undergraduate program and most US jurisdictions require their bar examination applicants to have attended an ABA-approved law school. The US has a unified legal profession, which means that US lawyers who perform "transactional" legal work need to be licensed by state supreme courts and their disciplinary agencies, as do those lawyers who litigate cases in front of a court tribunal. As part of the mandatory licensing process, prospective lawyers are subject to a series

[53] The term "Lawyers" is intentionally used in this discussion of the situation in the US as opposed to legal professionals as the requirements described do not extend to all legal professionals within the US.

of requirements to ensure they possess the necessary character and fitness to sit for the bar examination and to practice law. Applicants to US law schools need to disclose any criminal convictions or other encounters with the legal system.

Ongoing Requirements: US lawyers must renew their licenses annually. The requirements for renewal include mandatory compliance with rules of professional conduct, mandatory rules about accounts involving client funds, and additional rules that vary from state to state and include matters such as mandatory continuing education requirements, random audits of client trust accounts, and programs designed to identify and assist lawyers with substance abuse and mental health issues. US lawyers have mandatory obligations to report wrongdoing by other lawyers and failure to comply subject a lawyer to discipline. Many states require lawyers to self-report criminal convictions to the lawyer disciplinary agency.

Annex 5: Examples of Red flags highlighting suspicious activities or transactions for legal professionals[54]

a) The transaction is unusual, e.g.:
   - the type of operation being notarised is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting;
   - the transactions are unusual because of their size, nature, frequency, or manner of execution;
   - there are remarkable and highly significant differences between the declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional;
   - legal person or arrangement, including NPOs, that request services for purposes or transactions, which are not compatible with those declared or not typical for those organisations.
   - the transaction involves a disproportional amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.

b) The customer or third party is contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly, without logical explanation.

c) The source of funds is unusual:
   - third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation;
   - funds received from or sent to a foreign country when there is no apparent connection between the country and the client;
   - funds received from or sent to high-risk countries.

d) The client is using multiple bank accounts or foreign accounts without good reason.

e) Private expenditure is funded by a company, business or government.

f) Selecting the method of payment has been deferred to a date very close to the time of notarisation, in a jurisdiction where the method of payment is usually included in the contract, particularly if no guarantee securing the payment is established, without a logical explanation.

g) An unusually short repayment period has been set without logical explanation.

h) Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.

[54] See also the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership, July 2018, Annex E – Indicators of concealed beneficial ownership.

i) The asset is purchased with cash and then rapidly used as collateral for a loan.

j) There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested that are not appropriate for the common practice used for the ordered transaction.

k) Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification.

l) The collateral being provided for the transaction is currently located in a high-risk country.

m) There has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation.

n) There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk.

o) The company receives an injection of capital or assets in kind that is excessively high in comparison with the business, size or market value of the company performing, with no logical explanation.

p) There is an excessively high or low price attached to the securities transferred, with regard to any circumstance indicating such an excess (e.g. volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation.

q) Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the customer or the possible group of companies to which it belongs or other justifiable reasons.

Annex 6: Members of the RBA Drafting Group

FATF Members and observers	Office	Country/Institution
Sarah Wheeler (Co-chair)	Office for Professional Body AML Supervision (OPBAS), FCA	UK
Sandra Garcia (Co-chair)	Department of Treasury	USA
Erik Kiefel	FinCen	
Helena Landstedt and Josefin Lind	County Administrative Board for Stockholm	Sweden
Charlene Davidson	Department of Finance	Canada
Viviana Garza Salazar	Central Bank of Mexico	Mexico
Fiona Crocker	Guernsey Financial Services Commission	Group of International Finance Centre Supervisors (GIFCS)
Ms Janice Tan	Accounting and Regulatory Authority	Singapore
Adi Comeriner Peled	Ministry of Justice	Israel
Richard Walker	Financial Crime and Regulatory Policy, Policy & Resources Committee	Guernsey
Selda van Goor	Central Bank of Netherlands	Netherlands
Natalie Limbasan	Legal Department	OECD

Accountants		
Member	**Office**	**Institution**
Michelle Giddings (Co-chair)	Professional Standards	Institute of Chartered Accountants of England & Wales
Amir Ghandar	Public Policy & Regulation	International Federation of Accountants

Legal professionals and Notaries		
Member	**Office**	**Institution**
Stephen Revell (Co-chair)	Freshfields Bruckhaus Deringer	International Bar Association
Keily Blair	Economic Crime, Regulatory Disputes department	PWC, UK
Mahmood Lone	Regulatory issues and complex cross-border disputes	Allen & Overy LLP, UK
Amy Bell	Law Society's Task Force on ML	Law Society, UK
William Clark	ABA's Task Force on Gatekeeper Regulation and the Profession	American Bar Association (ABA)
Didier de Montmollin	Founder	DGE Avocats, Switzerland
Ignacio Gomá Lanzón	CNUE's Anti-Money Laundering working group	Council of the Notariats of the European Union (CNUE)
Alexander Winkler	Notary office	Austria
Rupert Manhart	Anti-money laundering Committee	Council of Bars and Law Societies of Europe
Silvina Capello	UINL External consultant for AML/CFT issues	International Union of Notariats (UINL)

FATF Members and observers	Office	Country/Institution
	TCSPs	
Member	**Office**	**Institution**
John Riches (Co-chair) and Samantha Morgan	RMW Law LLP	Society of Trust and Estate Practitioners (STEP)
Emily Deane	Technical Counsel	
Paul Hodgson	Butterfield Trust (Guernsey) Ltd	The Guernsey Association of Trustees
Michael Betley	Trust Corporation International	
Paula Reid	A&L Goodbody	A&L Goodbody, Ireland

Appendix U:

FATF, *Concealment of Beneficial Ownership* (Paris: FATF, 2018)

Concealment of Beneficial Ownership

July 2018

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The goal of the Egmont Group of Financial Intelligence Units (Egmont Group) is to provide a forum for financial intelligence unites (FIUs) around the world to improve cooperation in the fight against money laundering and the financing of terrorism and to foster the implementation of domestic programs in this field.

For more information about the Egmont Group, please visit the website: **www.egmontgroup.org**

Citing reference:

FATF – Egmont Group (2018), *Concealment of Beneficial Ownership* , FATF, Paris, France, www.fatf-gafi.org/publications/methodandtrends/documents/concealment-beneficial-ownership.html

TABLE OF CONTENTS

ACRONYMS

ACRA	Singapore Accounting and Corporate Regulatory Authority
AEOI	Automatic Exchange of Information for Tax Purposes
AML/CFT	Anti-money laundering and counter-terrorist financing
APG	Asia Pacific Group
ATM	Automatic teller machine
BVI	British Virgin Islands
CDD	Customer due diligence
CFTC	United States Commodity Futures Trading Commission
CSP	Corporate service provider
DNFBPs	Designated non-financial businesses and professions
DOJ	United States Department of Justice
EOIR	Standards on exchange of information for tax purposes: the Exchange of Information on Request
EUR	Euro
FATCA	United States Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FATF TREIN	FATF Training and Research Institute
FinTech	Financial technology
FIU	Financial intelligence unit
GIFCS	Group of International Finance Centre Supervisors
IMF	International Monetary Fund
IP	Internet protocol
KYC	Know your customer
LLC	Limited liability companies
LPP	Legal professional privilege
LTD	Private company limited by shares
MLRO	Money Laundering Reporting Officer

ML/TF	Money laundering and terrorist financing
MSB	Money service business
OCCRP	Organised Crime and Corruption Reporting Project
OECD	Organisation for Economic Co-operation and Development
OFC	Offshore financial centres
PEP	Politically exposed person
RegTech	Regulatory technology
SRBs	Self-regulating bodies
STR	Suspicious transaction report
TBML	Trade-based money laundering
TCSP	Trust and company service provider
US	United States of America
USD	United States dollars
VPN	Virtual private network

EXECUTIVE SUMMARY

1. Criminals employ a range of techniques and mechanisms to obscure their ownership and control of illicitly obtained assets. Identifying the true beneficial owner(s) or individual(s) exercising control represents a significant challenge for prosecutors, law enforcement agencies, and intelligence practitioners across the globe. **Schemes designed to obscure beneficial ownership often employ a "hide-in-plain sight" strategy**, leveraging global trade and commerce infrastructures to appear legitimate. However, visibility does not equate to transparency, and many of the tools that were designed to encourage business growth and development, such as limited liability corporations and nominee directorship services, can be used to facilitate money laundering, tax evasion, and corruption. The globalisation of trade and communications has only increased this threat, and countries now face the challenge of enforcing national laws in a borderless commercial environment.

Legal arrangements – refers to express trusts or other similar legal arrangements.
Legal persons – refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property.

2. This joint FATF Egmont Group report takes a global view assessing how legal persons, legal arrangements and professional intermediaries can help criminals conceal wealth and illicit assets. The purpose of the report is to help national authorities including FIUs, financial institutions and other professional service providers in understanding the nature of the risks that they face.

3. Analysis of 106 case studies demonstrates that **legal persons, principally shell companies, are a key feature in schemes designed to disguise beneficial ownership**, while **front companies and bearer shares** are less frequently exploited.

4. **Individuals and groups seeking to conceal the ownership of assets are most likely to exercise control over those assets via a combination of direct and indirect control**, rather than strictly one or the other. In a majority of cases, the beneficial owner used a combination of layering and direct ownership chains, as well as professional intermediaries and third parties exercising control on their behalf. In a limited number of cases, the beneficial owner exercised *only* indirect control and rarely retained direct control through a complicated structure without involving an intermediary. This demonstrates that, in many cases, the beneficial owner will maintain some level of direct control in a scheme, but will rarely do so without also involving an intermediary or "straw man" (informal

Shell company – incorporated company with no independent operations, significant assets, ongoing business activities, or employees.
Front company – fully functioning company with the characteristics of a legitimate business, serving to disguise and obscure illicit financial activity.
Shelf company –incorporated company with inactive shareholders, directors, and secretary and is left dormant for a longer period even if a customer relationship has already been established.

nominee shareholders and directors, such as spouses, children, extended family, and other personal or business associates).

5. **Nominee directors and shareholders, particularly informal nominees (or "straw men"), are a key vulnerability**, and were identified in a large majority of case studies assessed for this report. The role of the nominee, in many cases, is to protect or conceal the identity of the beneficial owner and controller of a company or asset. A nominee can help overcome jurisdictional controls on company ownership and circumvent directorship bans imposed by courts and government authorities. While the appointment of nominees is lawful in most countries, the ongoing merits of this practice are questionable in the context of the significant money laundering and terrorist financing vulnerabilities associated with their use.

Specialist and professional intermediaries

6. **The use of specialists and professional intermediaries is a key feature** of schemes designed to conceal beneficial ownership, particularly in cases where the proceeds of crime are significant. The majority of the case studies involved professional intermediaries. While it was not always explicitly stated in the case studies, approximately half of all intermediaries involved were assessed as having been complicit in their involvement. This demonstrates that complicity is not necessary to facilitate a scheme designed to obscure beneficial ownership, and that **professionals can be unwitting or negligent in their involvement**. This serves to highlight the importance of effective regulation of designated non-financial businesses and professions, and the need for increased awareness amongst professional service sectors. Nevertheless, law enforcement experience in some jurisdictions indicates that professional intermediaries are more likely to be complicit than unwittingly involved in money laundering cases.

- In the case study sample available for this report, **trust and company service providers (TCSPs)** represented the highest proportion of professional intermediaries involved in the establishment of legal persons, legal arrangements, and bank accounts. The TCSP sector was also significantly more likely to provide nominee, directorship, and other company management services to their clients, provide services to other professionals on behalf of third-party clients, and provide services to clients based internationally. However, despite their significant involvement in the establishment and management of these arrangements, TCSPs appear less likely to be the architect of schemes designed to obscure beneficial ownership. TCSPs that were assessed as having been complicit in their involvement were more likely to have been wilfully blind than fully complicit, or may have also provided legal, accounting, or other financial services. This suggests that the role of TCSPs is more likely to be transactional in nature, operating at the behest of a client or other intermediary, who are often based in another country. It also demonstrates that, **while TCSPs appear to be less likely to be the masterminds of schemes designed to obscure beneficial ownership**, **the services provided by TCSPs are vulnerable to exploitation by criminals and other professional intermediaries involved in these schemes**.

- **Accounting professionals** were the least represented sector in the cases analysed for this report; however, they were significantly more likely to be complicit in their involvement when compared to legal professionals and TCSPs. The accounting profession demonstrated the least direct involvement in the establishment of legal persons, legal arrangements, or banking relationships, which suggests that the key role of the accounting profession in the construction of schemes designed to disguise beneficial ownership is the provision of expert advice. Accounting professionals represented the highest proportion of scheme designers and promoters in the case studies, and were more likely to promote their own scheme to prospective clients than to simply facilitate a scheme designed by their client. They were also the only professional sector that was not identified as having provided services to another professional intermediary on behalf of a third-party client. **It is likely that the financial acumen of the accounting profession, and the ease with which accountants can identify suspicious financial activities, limit their vulnerability to being unwittingly exploited to facilitate the concealment of beneficial ownership**. It also suggests that criminals and complicit professionals may be unwilling to involve an accounting professional unless their complicity can be assured in advance.
- In comparison to other professional intermediary sectors, **the role of legal professionals in the facilitation of schemes designed to disguise beneficial ownership, varies depending on the situation.**
    - Legal professionals were more involved in the establishment of legal persons, legal arrangements, and bank accounts when compared with accountants, but less so when compared to TCSPs. The same was also true for the provision of nominee and directorship services.
    - Lawyers were the most likely of the three professions to be involved in the acquisition of real estate as a means of laundering the proceeds of crime and obscuring beneficial ownership.
    - Legal trust accounts and client accounts were also more frequently used as a means of disguising beneficial ownership, although the accounting profession also exhibited a similar proportion of this concealment technique. Legal professional privilege was also identified as a barrier to the successful recovery of beneficial ownership information.
    - In the case studies analysed for this report, where legal professionals were involved, there were a number of cases where legal professionals appeared to be unwitting or negligent in their involvement. This suggests that, despite their reasonably high level of involvement in the establishment of legal persons and arrangements, **legal professionals are not sufficiently aware of their inherent money laundering and terrorism financing vulnerabilities**. It is likely that this is exacerbated by the low level of regulation imposed on legal professionals in many countries.

7. Analysis indicates that **the services of both lawyers and accountants are rarely required to facilitate the same money laundering scheme – the involvement of one is typically sufficient**. TCSPs were present in almost all cases

that involved intermediaries from multiple sectors, and few cases demonstrated the use of both a lawyer and an accountant. Of the cases that involved multiple intermediaries from the same sector, the TCSP sector represented the overwhelming majority of these instances. When multiple TCSPs were exploited in a single scheme, almost all of the cases involved TCSPs in multiple jurisdictions. This reflects the role of TCSPs in establishing and managing local companies on behalf of foreign clients. Conversely, in instances where multiple legal or accounting professionals were used, most cases involved the use of multiple lawyers/accountants in the same jurisdiction, and most of these intermediaries were unwittingly involved. This suggests that, in instances where multiple lawyers or accountants are utilised to facilitate a scheme, criminal clients may be attempting to avoid suspicion by limiting their engagements with any single professional.

8. A lack of awareness and education of money laundering (ML)/ terrorist financing (TF) risks among professionals inhibits the identification of ML/TF red flags. This increases their vulnerability to being exploited by clients seeking to misuse otherwise legitimate services for ML/TF purposes. The case studies for this report identified that only four intermediaries involved in these schemes identified and reported suspicious activity in line with the FATF Standards. All of these cases were from countries that regulate designated non-financial businesses and professions (DNFBPs) under an anti-money laundering/counter-terrorist financing (AML/CFT) legal framework.

Anti-money laundering obligations and supervision

9. Seventeen per cent of jurisdictions that participated in the FATF's Horizontal Study of supervision and enforcement of beneficial ownership obligations do not impose any AML/CFT obligations or AML/CFT supervision on any DNFBPs whatsoever, despite this being a requirement of the FATF Standards. In some cases, this is the result of resistance to regulation from the relevant sectors or professions; in other cases, it may represent an "unfinished" aspect of the AML/CFT system which has not yet been implemented. The lack of supervision in these countries is a major vulnerability, and **professionals operating in countries that have not implemented appropriate regulations for DNFBPs represent an unregulated "back-door" into the global financial system**.

10. A country with a weak AML/CFT regime will exacerbate the vulnerabilities of legal persons, legal arrangements, and professional intermediaries. Key requirements of the FATF Standards, such as Immediate Outcomes 4 and 5, and Recommendations 10, 11, 12, 22, 23, 24, 25 and 28, amongst others, all relate to the risk profile of legal persons, arrangements, and intermediaries in a given jurisdiction. However, other inter-jurisdictional variables, such as trade and finance routes, are also influential with respect to the vulnerabilities and challenges associated with beneficial ownership. These vulnerabilities differ across jurisdictions and therefore cannot be definitively assessed at a global level. Competent authorities, financial institutions and DNFBPs should be mindful of the jurisdictional vulnerabilities that affect their country/business when assessing risk.

11. Schemes designed to obscure beneficial ownership often rely on a "hide in-plain-sight" strategy. This significantly impairs the ability of financial institutions, professional intermediaries, and competent authorities to identify suspicious

activities designed to obscure beneficial ownership and facilitate crime. At the same time, the FATF Standards and, by extension, much of the global AML/CFT infrastructure, centre upon the identification and reporting of suspicious activities by financial institutions and DNFBPs. Many of the case studies analysed for this report identified that information held by financial institutions was invaluable to the investigation of crime, and those countries that require the reporting of other transactions (such as threshold and cross-border transactions) indicated that these threshold-based reports were instrumental to the identification of irregular financial activities.

12. As the global economy becomes increasingly interconnected, and the sovereignty of financial borders dissipates, it is important to ensure that authorities have access to the appropriate information required to effectively deliver their mandate, whether it be suspicious transaction reporting submitted by reporting entities or other types of information, such as threshold and cross-border reporting. Furthermore, the FATF standards provide scope for countries to use several mechanisms to enable timely access to beneficial ownership information, and some countries have recently implemented, or are currently implementing, registers of beneficial ownership information as a mechanism to enable them to do so. Systems combining one or more approaches to ensure availability and accuracy of basic and beneficial ownership information may be more effective than systems that rely on a single approach. Some jurisdictions consider the availability of beneficial ownership registers assist competent authorities access up-to-date and accurate information, including for verifying information obtained from other sources.

Issues for consideration

13. As a result of the analysis and consultations that underpin it, this report identifies a number of issues to help address the vulnerabilities associated with the concealment of beneficial ownership, including:

- Consideration of the role of nominees including measures that may limit their misuse.
- The need for regulation of professional intermediaries in line with the FATF Standards, and the importance of efforts to educate professionals on ML and TF vulnerabilities to enhance awareness and help mitigate the vulnerabilities associated with the concealment of beneficial ownership.
- Further work to identify possible solutions or measures to prevent the misuse of legal professional privilege (LPP) to conceal beneficial ownership information, including through the provision of enhanced training and guidance material for legal professionals.
- Ensuring financial intelligence units have access to the widest possible range of financial information.
- Increased sharing of relevant information and transaction records to support global efforts to improve the transparency of beneficial ownership.
- Further work to understand what can be done to improve the quality and timeliness of the cross-border sharing of information, including through mutual legal assistance.

- Ensuring, for countries that make use of registers of beneficial ownership, and for all countries' company registers, that there is sufficient resource and expertise associated with their maintenance. This is to ensure that the information recorded in the register is adequate, accurate, and up-to-date, and can be accessed in a timely manner.
- The need for countries to consider and articulate the vulnerabilities and threats relating to domestic and foreign legal persons and arrangements, the domestic and foreign intermediaries involved in their establishment, and the means by which criminals may exploit them to facilitate ML and other criminality.

14. A broad theme underlying all of these issues is information, including possible ways to improve the reliability, access and mechanisms to share that information more effectively at domestic and international levels. In some instances, these issues aim to inform responses by individual governments in taking further action; other issues identify areas for further research and engagement.

INTRODUCTION

15. Over the past three decades, the dramatic convergence of international trade and global financial systems, as well as the rise of the internet and other forms of communication technologies, has opened new opportunities for criminals to misuse company and business structures to conceal anomalous financial flows and criminality. Far from operating in a shady, hidden criminal economy, criminals disguise their activities as legitimate corporate trade to hide illicit funds within the enormous volume of transactions that cross the globe every day. However, visibility does not equate to transparency, and criminals use a multitude of tools, including shell companies[1], trusts, other legal arrangements, nominees, and professional intermediaries, to conceal the true intent of their activities and beneficial ownership[2] associated with them.

16. The ownership and control of illicit assets, and the use of legal structures to conceal them, has been the subject of increased global attention in recent years. The leak of confidential information from two large international law firms responsible for the establishment of complex international corporate structures in 2015 and 2017[3] has increased public awareness of the way in which legal structures can be used to conceal wealth and illicit assets.

17. The ability of countries to prevent the misuse of legal persons and legal arrangements, and the ways in which they are being misused, have been the subject of numerous discussion papers and research projects over the last decade or longer. Studies have been published by international bodies, including the Organisation for Economic Co-operation and Development (OECD), the World Bank, the United Nations Office on Drugs and Crime, and the Financial Action Task Force (FATF). Collectively, these reports provide a wealth of knowledge on the abuse of corporate structures to facilitate corruption and money laundering; however, the FATF and Egmont Group of Financial Intelligence Units (Egmont Group) identified the need for further analysis of the vulnerabilities associated with beneficial ownership, with a particular

Legal arrangements – refers to express trusts or other similar legal arrangements.
Legal persons – refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property.

See also Section 1.

1 For the purpose of this paper, "shell companies" are considered to be companies that are incorporated but which have no independent operations, significant assets, ongoing business activities, or employees.

2 'Beneficial ownership' or 'beneficial owner' refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. See also the section 'Definition of Beneficial Owner'.

3 From Panama-based law firm Mossack Fonseca, in 2015, and Bermuda-based law firm, Appleby, in 2017.

focus on the involvement of professional intermediaries, to guide global responses. This report attempts to address that need.

18. The publication takes a macro-level, global view of inherent vulnerabilities and is designed to support further risk analysis by governments, financial institutions, and other professional service providers. In undertaking further risk analysis, countries and private sector professionals should consider how the geopolitical and economic environment, as well as their own risk mitigation strategies, will affect the vulnerabilities associated with legal structures and the intermediary sectors that facilitate their formation and management.

METHODOLOGY

19. This project was co-sponsored by the FATF and Egmont Group. The project drew upon the unique and complementary capabilities of the FATF and Egmont Group to try to better understand the vulnerabilities linked to the concealment of beneficial ownership and the misuse of professional service providers. Led by Australia, Germany and France, the project team included experts from: Argentina, Canada, India, Israel, Italy, the Netherlands, New Zealand, the Russian Federation, Singapore, Switzerland, the United Kingdom, the United States, the Asia Pacific Group (APG) members, Bangladesh and Nepal, the Secretariat of the Inter-Governmental Action Group Against Money Laundering in West Africa (GIABA), the Group of International Finance Centre Supervisors (GIFCS), the Middle East and North Africa FATF-style regional body (MENAFATF) member, Egypt, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), the International Monetary Fund (IMF), the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes (OECD Global Forum), the World Bank, and the FATF Training and Research Institute (FATF TREIN).

20. In preparing this report, the project team analysed typologies studies, intelligence assessments, mutual evaluation reports, and academic reports published by a range of academics, international bodies, and governments. A detailed list of the public sources used is included in Annex A. In addition to these public reports, the project leads analysed intelligence reports produced by financial intelligence units (FIUs), criminal intelligence and law enforcement agencies, and other competent authorities to identify emerging trends and methods being exploited by criminals. In many cases, these reports are not available publicly, and only desensitised information has been used in this report.

21. An intelligence exchange workshop was conducted during the FATF Joint Experts Meeting, which was hosted by the Russian Federation in Moscow in April 2017, during which 13 delegations[4] presented case studies and intelligence insights relating to the concealment of beneficial ownership. A session was also held with the private sector, including representatives from banks, law societies, and TCSPs, which helped the project team to better understand their practices and challenges with regard to issues of beneficial ownership.

22. As part of a process of targeted private sector consultation, the project team sought comments from 12 international organisations and associations representing a spectrum of the private sector with a particular interest in the topic. The organisations represented global financial institutions, DNFBPs, data providers, FinTech and RegTech firms, and non-government organisations. The project team received comments from the Financial Transparency Coalition; the Institute of International Finance; the International Banking Federation; the International Federation of Accountants; the International RegTech Association; the International

[4] These 13 were Indonesia, Italy, Israel, Kyrgyz Republic, the Netherlands, Poland, Russia, Spain, Sudan, Switzerland, Venezuela, Europol, and the European Commission.

Union of Notaries; the Society of Trust and Estate Practitioners; the Wolfsberg Group; and from the International Bar Association's Anti-Money Laundering and Sanctions Expert Working Group. These comments included additional information on vulnerabilities, additional risk indicators, and methods for identifying beneficial ownership.

23. The primary sources of information for this report were the case studies[5] provided by FATF, the Egmont Group, and FSRB members. FATF TREIN undertook an analysis of the 106 case studies and typologies submitted by 34 jurisdictions. This is a relatively small sample of countries, and is weighted towards a few jurisdictions that provided a larger number of cases[6]. FATF TREIN's analysis was limited to the information known to the competent authorities and the information then communicated in the case summaries. In some cases, information relating to the money laundering scheme (the predicate offence or the location of the ultimate beneficial owner) was apparently not known by the competent authorities. In other cases, the information was not communicated in the case summary (for example, the type of legal person) or was anonymised (for example, the jurisdiction from which services were provided).

24. Despite these inherent limitations in the data, the case descriptions are substantially more detailed than those that can be found in recently published Mutual Evaluation Reports (MERs). Additionally, the cases, where the dates were identified, were generally recent, ranging from 2010 to 2017. The average sum of money laundered in each case, across all cases reviewed for this report, was in excess of USD 500 million.

25. This report has focused on the vulnerabilities and techniques of misuse associated with the concealment of beneficial ownership posed by legal persons, legal arrangements, and the professional intermediaries commonly involved in their establishment. It does not cover the threats posed by criminals and how these may differ among predicate offences, how different predicate offences may affect the methods used to obscure the beneficial owner, or the consequences associated with the residual risk. The report considers common techniques used by criminals to conceal beneficial ownership, and the environmental characteristics that contribute to the vulnerabilities posed by these legal structures and intermediaries. No effort has been made to provide a definitive list of high-risk jurisdictions based on these environmental risks, as numerous variables specific to particular jurisdictions make such a task untenable on a global level.

Horizontal Study of Enforcement and Supervision

26. In 2016-17, the FATF undertook a horizontal study on the enforcement and supervision of beneficial ownership obligations. The purpose of the study was to understand how beneficial ownership requirements were being supervised, in

[5] The case studies provided by law enforcement agencies and FIUs are focused on the various techniques, trends and methods used by criminals to conceal beneficial ownership.

[6] For example, the Netherlands submitted 19 cases for analysis, while Egypt submitted eight and Australia and the United States both submitted seven.

particular among key gatekeeper professions such as lawyers and TCSPs, as well as the role of registries in establishing and managing companies. The Horizontal Study was based on a survey of 64 jurisdictions, including 23 FATF members, who volunteered to provide information. The results of this analysis are attached at Annex B to this report and, where relevant, references to that study are provided throughout the publication.

DEFINITION OF BENEFICIAL OWNER

27. The FATF standards define "beneficial owner" as the "*natural person(s) who ultimately*[7] *own(s) or* control*(s) a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement*"[8] [9]. This definition differs from the definitions of "beneficiary" and "beneficiaries", which can include both natural and legal persons and arrangements, and often relate to:

- the recipients of charitable, humanitarian, or other types of assistance through the services of an NPO[10], or
- the person(s) entitled to the benefit of a trust arrangement[11] or insurance policy[12].

28. The distinction between "beneficial owner" and "beneficiary" relies on the concept of "ultimate" control or benefit, which refers to the *natural person* who ultimately controls or benefits from an asset or transaction through direct or indirect means. Importantly, a "beneficial owner" must always be a natural person, as a legal person cannot exert "ultimate" control over an asset. This is due to the fact that legal persons are always controlled, directly or indirectly, by natural persons. Therefore, while a legal person or arrangement can be the beneficiary of an asset or transaction, determining the beneficial owner requires the discovery of the natural person(s) who ultimately control or benefit from the legal person or arrangement.

29. The concept of ultimate benefit and control is also central to distinguishing "beneficial" ownership from "legal" ownership. The legal owner of an asset is the natural or legal person or arrangement that holds the legal title of that asset; however, legal ownership is not always essential in order to exert control over, or benefit from, an asset, particularly when the asset is held in trust or owned by a legal person. It is therefore essential to determine the natural person who controls an asset, rather than the legal owner of that asset.

30. Determining ultimate control can be problematic, and is often the principal challenge of determining beneficial ownership. In the context of a company, control can be exerted by shareholders, directors, and senior management. While shareholders are generally considered to exert the greatest level of control over a

---

7 Reference to "ultimately owns or controls" and "ultimate effective control" indicates situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

8 This definition should also apply to beneficial owner of a beneficiary under a life or other investment-linked insurance policy.

9 FATF, 2012a: p. 113.

10 *Ibid,* p. 59.

11 *Ibid,* p. 113.

12 *Ibid,* p. 62.

company, due to their ability to dismiss directors and other senior staff and because they stand to benefit from the profits of the company, the role of directors and senior management cannot be overlooked. In the context of trusts, the trustee exerts control over an asset but is legally bound to act in the interests of the beneficiary, who generally cannot exercise any control over the trust. The settlor and protector of the trust may also continue to exert some level of control or influence over the trust, despite having relinquished legal ownership of the asset to the trustee for the benefit of the beneficiary. This can complicate any efforts to determine who should be considered the beneficial owner and can necessitate further efforts to determine the true nature of the trust relationship.

31. Control can also be exerted via third parties, including professional intermediaries, family members, associates, nominees, and other natural persons who have been recruited or coerced to act on behalf of the ultimate beneficial owner. The use of nominees and other third parties can complicate efforts to identify the ultimate beneficial owner of an asset or transaction, as the beneficial owner may not be recorded in formal company or trust records in many jurisdictions. While it is important for competent authorities to have the ability to understand the identity of the natural person controlling an asset, it is also important for competent authorities to understand who benefits from it.

32. Further guidance on the definition of "beneficial owner" is available in the *FATF Guidance on Transparency and Beneficial Ownership*[13].

13 FATF, 2014: p. 8.

STRUCTURE OF THE REPORT

33. The report is divided into four sections, which are designed to analyse the separate aspects that contribute to the concealment of beneficial ownership. The sections are arranged as follows:

- **Section 1** briefly outlines the **main characteristics of various legal persons and arrangements**. By analysing the case studies provided in support of this report, as well as the experiences of law enforcement agencies and FIUs in various countries, this section of the report provides an overview of the general features and functions of legal persons and arrangements that make them vulnerable to misuse for the purposes of concealing beneficial ownership.
- **Section 2** provides an overview of the **methods and techniques** commonly used to conceal beneficial ownership. The purpose of this section is to analyse how beneficial ownership is disguised using a range of legal structures, intermediaries, and fraudulent activities. The following three key methods are assessed in this section: generating complex ownership and control structures, obscuring the relationship between the asset and the beneficial owner, and falsifying activities. These methods can involve a range of techniques, the assessment of which will form a foundation for the assessment of vulnerabilities associated with legal persons, arrangements, and intermediaries in later sections of the report.
- **Section 3** analyses key **professional intermediary sectors** involved in the establishment and management of legal persons and arrangements, namely the legal, accounting, and TCSP sectors, and is the focus of this report. This section provides an overview of the principal role of these intermediary sectors in the establishment of legal structures, the services they provide that are commonly exploited by criminals, and other features which make these professionals vulnerable to exploitation. The purpose of this assessment is to determine how professional intermediaries are being exploited, wittingly and unwittingly, to affect schemes and methods designed to obscure beneficial ownership in order to inform risk assessments and mitigation strategies.
- **Section 4** provides an overview of key **environmental vulnerabilities**, including jurisdictional vulnerabilities and vulnerable business practices, which contribute to the vulnerabilities associated with the legal persons, legal arrangements, and professional intermediaries assessed in the rest of the report. The section does not attempt to provide a definitive list of high-risk jurisdictions, as jurisdictional risks will differ from country to country. Rather, the purpose of this section is to support risk analysis activities performed by FIUs, financial services providers, and professional intermediaries.

34. In analysing the main characteristics leading to misuse of legal persons and legal arrangements, the inherent vulnerabilities associated with professional intermediaries, and the environmental vulnerabilities that may facilitate their

appearance, this report identifies a number of issues for consideration. A broad theme underlying these issues is information, including possible ways to improve the reliability, access and mechanisms to share that information more effectively at domestic and international levels. In some instances, these issues for consideration aim to inform responses by individual governments in taking further action; other issues identify areas for further research and engagement.

SECTION 1 — MISUSE OF LEGAL PERSONS AND ARRANGEMENTS

35. Legal persons and arrangements play an important role in global commerce and trade, and are the cornerstone of modern economies. For the most part, legal persons and arrangements serve legitimate, lawful, and meaningful purposes. However, the unique legal status of legal persons and arrangements also lend themselves to complex schemes designed to conceal the true beneficial owners and, in many respects, concealing the real reason for holding assets and conducting related transactions. Legal persons can lend legitimacy to unlawful activities, hide the involvement of key stakeholders and controlling parties, and generally frustrate criminal investigations domestically and internationally. Whilst acknowledging the legitimate role of legal persons and arrangements, this section will briefly introduce the characteristics of various types of legal persons and arrangements, and how they are exploited to facilitate crime and conceal beneficial ownership.

36. It is important to note that the information in this section is designed to assist financial institutions and professional intermediaries in analysing risk. It is not intended to suggest that any particular form of legal person or arrangement to be considered high-risk or low-risk by default. Private sector entities are encouraged to apply a risk-based approach to customers and transactions on a case-by-case basis.

Legal persons

37. Seen from a global perspective, there are numerous different kinds of legal persons that exist under a multitude of different company laws, making it difficult for law enforcement to trace assets held by legal persons across numerous countries. Legal persons, specifically companies, are prominent features of most schemes and structures designed to obscure beneficial ownership. Almost all of the cases analysed for this report involved at least one company. The separation of legal and natural personalities offered by companies is a key feature influencing this popularity.

38. Given the broad range of legal persons in existence across the globe, an analysis of the similarities and differences among forms of legal persons would have exceeded the scope of this project. Furthermore, most of the case studies did not provide specific insights into the types and legal peculiarities of the legal persons used in the money laundering schemes. As such, the report has focused on broader characteristics of legal persons, and has not endeavoured to assess all of the specific forms available. One of the factors that might contribute to a higher frequency of misuse of a particular type of legal person is the absence of accurate and up-to-date information on its ownership and management, which, as evidenced by the Horizontal Study[14], remains a challenge in many jurisdictions.

39. A categorization of legal persons must differentiate between partnerships on the one hand and corporations or capital companies, in the sense of trading

[14] See, in particular, Question 3 of the Horizontal Study at Annex B.

companies, on the other. In a general **partnership**, ownership and control are exercised by all partners specified in the partnership contract. In that regard, the ability to misuse a general partnership to disguise beneficial ownership is significantly reduced, as management is exercised immediately by the partners and there is no legal segregation between the natural persons and an independent legal person. The same can be said of general partners of a limited partnership; however, limited partners can benefit from a certain degree of anonymity by acting solely as an investing partner regardless of their actual role in the partnership. However, due to their limited liability, limited partners generally have only limited control over the partnership.

40. In contrast to partnerships, the capital participation of shareholders is the focus of **capital companies**, not their "personality". Unlike partnerships, capital companies are always a separate legal entity, and are often controlled and owned through shares, which can be transferred and sold regularly without affecting the existence of the capital company itself. The hybrid construction of limited liability companies (LLCs) (or private company limited by shares (LTD)) and foundations differ from capital companies and are outlined in further detail below.

41. The main feature of a company is the strict separation of the natural person investing in and owning the company by shares and the legal personality of the company itself. A company's legal personality allows it to conduct business and own assets under its own name, assuming all rights and being liable for all debts and obligations it enters into. This legal structure allows a natural person to take part in business without disclosure of their personal identity[15]. Even though shareholders own the company, usually they are not actively involved in management functions, but instead elect or appoint a board of directors to manage the company in a fiduciary capacity[16].

42. Private companies, such as **limited liability companies** (LLC)[17], are restricted in different ways (they may have a limited number of shareholders, require notarization for the transfer of shares, etc.) depending on the jurisdiction in which they are established. LLCs combine elements of partnerships and companies. While differing slightly from country to country, the primary concepts are the same. Unlike publicly traded companies, they do not offer their interests to the public, and are therefore generally subject to less stringent reporting and oversight regimes. Shares in a limited liability company cannot be publicly offered and traded, and

15 Securities laws may provide for transparency to a certain degree, such as through notification requirements for stock-listed companies if the shareholder exceeds a certain amounts of shares.

16 Van der Does de Willebois, E. et al. (2011: p. 162) claim that companies are the most misused corporate vehicle documented in the study. While the study focuses on corruption, it discusses in detail how corporate vehicles can be used to disguise of ownership and control.

17 The term "limited liability company" here is intended to encompass the various forms of this kind of company in several jurisdictions (e.g. LLC in US; Pvt Ltd. in UK, Ireland, India, Hong Kong; GmbH in Germany, Austria, Liechtenstein; BV in the Netherlands; SARL in France).

often some limitations apply to the transfer of shares. While members can manage a LLC directly, this function is usually performed by managers or directors. The governing rules on ownership and control rights are determined by a contract, which may not be publicly available. The contract gives the members a high degree of freedom in determining the division of ownership and control among the members,[18] thus allowing latitude to exploit nominees and obscure true ownership and control arrangements in order to obscure beneficial ownership.

43. **Foundations** are separate legal entities with no owners or shareholders and are generally managed by a board of directors. Foundations are generally restricted to the provision of a service for public benefit, although several jurisdictions allow foundations to be established to fulfil private purposes (private foundations[19]). Safeguards usually exist to ensure that a foundation is sufficiently independent from its founder; however, foundations are vulnerable to exploitation for money laundering purposes, particularly when laws allow the founder to exert control over the foundation. Only a small number of the cases analysed for this report involved the use of a foundation.

44. As previously stated, this report has not drawn any specific conclusions on the vulnerabilities of specific forms of legal person, as cases provided did not contain sufficient information on the types of legal persons used in financial crimes to allow conclusions to be drawn. However, it can be stated that almost all of the cases analysed for this report involved the use of a company, which indicates that these vehicles are significantly attractive for misuse. Furthermore, only a small number of cases involved a foundation, and a very small number of the case studies involved a partnership to obscure beneficial ownership.

45. A range of characteristics have been identified which allow legal persons to be exploited by criminals to conceal beneficial ownership. Many of these – including the use of shell, shelf[20] [21], and front companies[22], the construction of complex chains

18 Van der Does de Willebois, E. et al., 2011: p. 164.

19 Private foundations pursue not-for-profit activities on behalf of their members or founders. The structure can be found in many countries including Germany, Bulgaria, Panama, the Netherlands, and Sweden. A private foundation is usually funded by an individual or small group of individuals. It has legal personality by virtue of a written act and through recognition of its status by the supervisory authority. The initial registration of a foundation established to fulfil private purposes is usually faster and less demanding than the process required for a public foundation. Accounting requirements are also more straightforward, and maintenance and administration costs also tend to be lower.

20 For the purpose of this paper, a "shelf company" is considered to be an incorporated company that has inactive shareholders, directors, and secretary and is left dormant for a longer period even if a customer relationship has already been established.

21 As *shelf companies* can also be considered a type of *shell company*, particularly following their sale or transfer of ownership, it is possible that jurisdictions referred to former shelf companies as shell companies when providing case studies.

22 For the purpose of this paper, a "front company" is considered to be a fully functioning company with all the characteristics of a legitimate business, which ultimately serves to disguise and obscure the illicit financial activity being conducted. Front companies are often cash intensive businesses.

of ownership using multiple legal persons, the splitting of assets and company administration across different countries, and the use of formal and informal nominees – have been analysed in Sections 2 and 4 of this report.

Legal arrangements

46. One way to translate a fiduciary relationship into a legal agreement, especially in common law countries, is the settlement of a trust. Although there is no universal definition, from a functional point a view a trust can be said to separate the legal property, administration, and economic benefit of an asset[23].

47. **Trusts** can be used to achieve varying objectives, including:

- transferring the administration of an asset to a third party to organise an inheritance
- protecting assets for children, classes of family members or vulnerable adults
- managing in common an asset for a pool of corporations (like syndicated loans in corporate banking, where a lead lender originates and administrates the loan for the other secondary lenders, who are only signing the loan agreement)
- financing charity through an intermediary gathering funds
- investing money with the view to finance an important expense in the future (e.g. education fees or retirement).

48. While trusts are sometimes a source of misunderstanding between common law and civil law experts, they have spread across countries of both legal traditions. Although they have a long and established history under common law, they are a more ambiguous concept in civil law countries; however, it is worth noting that similar "trust-like" legal arrangements exist in some civil law countries, presenting the same structure or functions, like the "*fiducie*" in some civil law countries (although this latter type of legal arrangement cannot be used to facilitate a legacy)[24].

---

[23] The FATF Recommendations makes use of Article 2 of the Hague Convention on the Law Applicable to Trusts and on their Recognition (the Hague Trust Convention) when considering how to define a trust. Key characteristics of a trust according to the Hague Trust Convention include the separation of the assets from the trustee's estate, the title of the assets stand in the name of the trustee or in the name of another person on behalf of the trustee, and the provision of power to the trustee to manage the assets in accordance the terms of the trust.

[24] Trusts developed in common law countries, but it is important to note that civil law countries which do not recognize trusts have often put in place different mechanisms to fulfil the same functions as trusts. For instance, from a European perspective, one can consider that the widely developed "life insurance" contract uses the same principles as a trust, where a settlor asks a trustee to administer funds on behalf of a third party (the beneficiary).

49. The Horizontal Study found that 60% of responding jurisdictions provided for the creation of trusts or other similar legal arrangements under their domestic laws[25]. A further 21% of responses were from jurisdictions which are not the source of law for legal arrangements, but which give some recognition to foreign legal arrangements and permit foreign legal arrangements to be created or administered by gatekeepers or others within their jurisdiction (e.g. under the Hague Trust Convention). Finally, 19% of responses indicated they do not recognise (e.g. in courts or in their tax system) any legal arrangements, whether based on domestic or foreign law.

50. Apart from the intent to separate legal and beneficial ownership, it is not clear precisely why criminals exploit trusts in money laundering schemes. There may be a multiplicity of reasons which will vary on a case-by-case basis. Criminals may exploit the secrecy provisions inherent in certain legal arrangements to prevent competent authorities from exerting authority to unravel the true ownership structure. This is particularly likely when schemes involve a foreign trust. Indeed, the use of foreign trusts might convey risks of unlawful practices owing to criminals making the most of the differing treatment of these legal arrangements by tax authorities and of the potential lack of coordination between them. From the cases analysed for this report, criminals used foreign jurisdictions in broadly the same proportions when establishing legal persons and legal arrangements.

51. The complexity and expense of establishing legal arrangements may limit their use when compared to the prolific exploitation of legal persons by criminals. The benefits associated with the use of legal arrangements, principally the separation of legal and beneficial ownership, might not be sufficiently significant to merit the additional investment when compared to the cost, availability and characteristics of legal persons. The relative frequency of the use of legal arrangements in the cases analysed for this report (approximately one-quarter of all cases) may be due to the fact that many of the cases involved sophisticated predicate offences that yielded significant proceeds and thus warranted the additional investment.

25 See, in particular, Question 2 of the Horizontal Study at Annex B.

SECTION 2 — TECHNIQUES USED TO OBSCURE BENEFICIAL OWNERSHIP

52. Criminals employ a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common mechanisms/techniques have been compiled by FATF in previous studies, including the 2014 *FATF Guidance on Transparency and Beneficial Ownership*. According to the FATF guidance report[26] beneficial ownership information is commonly obscured through the use of:

- shell companies[27], especially in cases where foreign ownership is spread across jurisdictions
- complex ownership and control structures
- bearer shares and bearer share warrants
- unrestricted use of legal persons as directors
- formal nominee shareholders and directors where the identity of the nominator is undisclosed
- informal nominee shareholders and directors, such as close associates and family
- trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets
- intermediaries in forming legal persons, including professional intermediaries.

53. Additional techniques and mechanisms which were not explored in the FATF's previous guidance include the use of shelf companies[28] and front companies[29], misleading naming conventions, false loans and invoices, and declaring numerous beneficiaries. Overall, the key techniques used by criminals to obscure beneficial ownership can be categorised within three broad methods:

26 FATF, 2014: p. 6.

27 For the purpose of this paper, "shell companies" are considered to be companies that are incorporated but which have no independent operations, significant assets, ongoing business activities, or employees.

28 For the purpose of this paper, a "shelf company" is considered to be an incorporated company that has inactive shareholders, directors, and secretary and is left dormant for a longer period even if a customer relationship has already been established.

29 For the purpose of this paper, a "front company" is considered to be a fully functioning company with all characteristics of a legitimate business that is usually cash intensive.

- **generating complex ownership and control structures** through the use of legal persons and legal arrangements, particularly when established across multiple jurisdictions
- **using individuals and financial instruments to obscure the relationship between the beneficial owner and the asset**, including bearer shares, nominees, and professional intermediaries, and
- **falsifying activities** through the use of false loans, false invoices, and misleading naming conventions.

54. These methods and techniques are outlined in greater detail below in order to contextualise the role of legal persons, arrangements, and professional intermediaries in disguising beneficial ownership.

Generating complex ownership and control structures

55. A key method used to disguise beneficial ownership involves the use of legal persons and arrangements to distance the beneficial owner from an asset through complex chains of ownership. Adding numerous layers of ownership between an asset and the beneficial owner in different jurisdictions, and using different types of legal structures, can prevent detection and frustrate investigations.

56. More than half of the case studies submitted in support of this report made use of complicated ownership structures, whereby control was affected through a combination of direct and indirect control. These complex structures were achieved through the establishment of chains of ownership, which often involved a number of legal persons and arrangements across multiple countries, distancing the beneficial owner from the assets of the primary corporate vehicle. In only a small number of cases did the beneficial owner retain legal ownership through a complicated structure without using an intermediary. The Russian case study below (Case Study 88) demonstrates how complex ownership structures, involving numerous foreign companies and bank accounts, were used to disguise the beneficial ownership of embezzled public funds and other proceeds of crime.

57. There are few restrictions on the establishment of chains of ownership within and across jurisdictions.[30] Legal persons are allowed to own shares in companies established in any country, while many countries also allow legal persons to be registered as the directors of companies. Shell companies and front companies feature prominently in most complex structures identified by FIUs and other competent authorities, while trusts and other legal arrangements are less frequently identified.

58. Complex ownership and control structures are not, in and of themselves, unlawful. Often, these corporate structures serve legitimate purposes and facilitate a wide range of commercial activities, entrepreneurial ventures, and the management of personal finances. Advances in communications technology, ease of travel, and other effects of globalisation are increasing the accessibility of global finance and business centres to all population segments, beyond large corporations and high net

30 Van der Does de Willebois, E. et al., 2011: p. 53.

worth individuals. Complex ownership structures can simplify business transactions for companies that regularly trade transnationally, provide services to international clients, or conduct parts of a company's operations (such as manufacturing or research and development) in another country. Often complex control structures are used by family businesses, by government-owned or operated public or commercial business ventures, and by publicly traded companies to structure their affairs. In these instances, a financial institution, legal/accounting professional, or other service provider will be in a position to readily ascertain the beneficial ownership of the structure. These structures are generally transparent to relevant authorities and present minimal vulnerabilities for disguising beneficial ownership.

59. Despite the legitimacy of many complex ownership and control structures, these structures can also be used to obscure beneficial ownership, avoid taxation obligations, conceal wealth, and launder the proceeds of crime. Complex structures are also used in fraudulent investment schemes, phoenix activity[31], false invoicing, and other types of fraud. The majority of case studies that involved tax evasion, fraudulent investment schemes and fraud as predicate offences also utilised complex structures to conceal beneficial ownership.

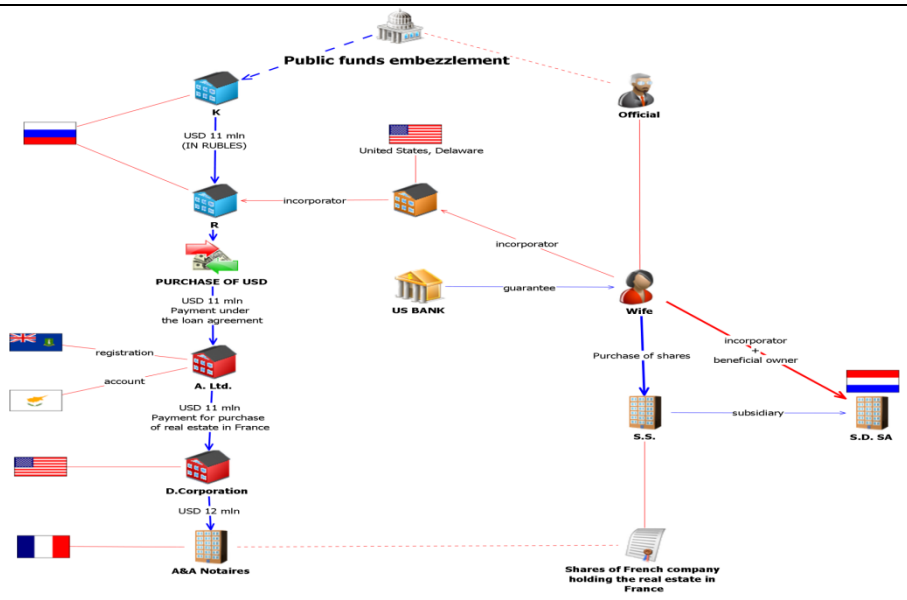
60. The use of numerous legal persons or arrangements within a single legal structure, as well as the use of numerous bank accounts and nominee directors, can significantly impair efforts by FIUs, other competent authorities, and financial institutions to identify and verify the beneficial owner. This is further frustrated when legal ownership structures span numerous jurisdictions. Despite concerted efforts by many countries to improve the sharing of financial intelligence and company information, mutual legal assistance and other forms of bilateral or multilateral information requests are often slow to action or complicated by various legal hurdles. Law enforcement agencies and FIUs report that, following lengthy information-sharing processes with international counterparts, the information received often demonstrates that the company of interest is owned by another legal person or arrangement in another country. The Horizontal Study demonstrated that there are considerable challenges in ensuring accurate and up-to-date information on legal persons in many jurisdictions[32]. As a result, the greater the number of companies and countries involved in a corporate structure, the greater the challenges associated with discovering the ultimate beneficial owner in a timely manner.

31 Illegal phoenix activity is the creation of a new company to continue the business of a company that has been deliberately liquidated to avoid paying its debts, including taxes, creditors and employee entitlements.

32 See, in particular, Question 3 of the Horizontal Study at Annex B.

Case Study 88 – Russia

Embezzled public funds worth RUB 300 million (Russian rubles) (USD 11 million) were transferred from the account of Company K to the account of Company R. Company R, a Delaware corporation, was owned and managed by the Russian wife of the suspect, a state official. The same day, Company R transferred USD 11 million as a loan to an account of Company A (BVI) held by a Cypriot bank. Company A then transferred more than USD 11 million to the Company D (US) to purchase real estate in France. Company D transferred more than USD 12 million to a French Notaries Bureau. Information from the FIU of Luxembourg showed that one of the US banks acted as a guarantor for the suspect's wife in a transaction to purchase of shares of a French company – and the holder of the real estate. The transaction was conducted via an S.S. company – a French subsidiary of a Luxembourg S.D. SA., incorporated and owned by the same individual. Analysis showed that these two chains were interrelated and the real estate was purchased with the proceeds of public funds embezzled for the benefit of the state official's wife.



Shell and Shelf Companies

61. The 2014 *FATF Guidance on Transparency and Beneficial Ownership* defined **shell companies** to be "*companies that are incorporated but which have no significant operations or related assets*"[33]. The FATF's 2013 report, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, used a similar definition[34] in its description of the use of shell companies as a technique to place or layer illicit funds. As outlined in the 2013 report, shell companies can serve

33 FATF, 2014: p. 6.

34 FATF, 2013: p. 55.

legitimate purposes, such as serving as a transaction vehicle for company mergers or protecting a corporate name from being used by another party.

62. Despite their legitimate uses, shell companies are the most common type of legal person used in schemes and structures designed to obscure beneficial ownership. Of the case studies analysed for this report, more than half specifically referred to the use of shell companies; however, it is likely that the actual figure is higher, as many countries are likely to have referred to legal persons in a general sense, rather than specifying the nature of the company involved. Shell companies can be used in complex structures involving the distribution of assets across multiple companies in multiple jurisdictions. When these structures are used for illicit purposes, money may flow through multiple layers of shell companies before finally being withdrawn in cash or transferred to its final destination internationally. Of the cases that included shell companies, the majority included a corporation located in a foreign jurisdiction.

63. Shell companies can be difficult to detect, as their incorporation is often no different from companies formed for other purposes; however, there are a number of characteristics and indicators that may indicate that a company is a shell, including the use of only a post-box address, a lack of personnel (or only a single person as a staff member), and a lack of payments in taxes and/or social benefit payments. Furthermore, many shell companies do not have a physical presence, and are geographically anchored through the use of TCSPs and nominee directors whose role in the management and direction of the shell company is limited. This is a particular problem with shell companies and presents a meaningful vulnerability that should be considered when doing business with companies that exhibit characteristics of being a shell company.

64. The use of shell companies in complex corporate structures designed to disguise beneficial ownership is a consistent and enduring technique used by criminal groups, corrupt individuals, and complicit professionals. The increased availability of shell companies to foreign nationals, which has been made possible by the growth of global communications and the convergence of international trade markets, has exacerbated this issue.

65. As with shell companies, **shelf companies** serve legitimate purposes. In theory, shelf companies allow investors, or people planning a new undertaking, the possibility of securing a company structure within hours to serve a time-sensitive need. Where shelf companies have already been in operation for a number of years, the new owner can use this history to help secure business relationships or lines of credit; some shelf companies may already have established customer relationships with financial institutions, facilitating access to the international financial system.

66. When the shelf company is sold, the inactive shareholders transfer their shares to the purchaser, and the directors submit their resignations. As part of the transfer, the purchaser may receive the company's credit history, if it is available. Occasionally, the company directors will continue to function as nominees, particularly when the shelf company is established and sold by a TCSP. In these cases, the only apparent change in the company is a change of ownership. However, the change of ownership will only be apparent if it is properly recorded in company registries. This is often "overlooked" in cases where shelf companies are used to disguise beneficial ownership. Law enforcement agencies and FIUs have reported

that the failure to properly record the change of ownership following the sale of a shelf company is a concern.

67. Despite the theoretical use of shelf companies in the concealment of beneficial ownership, only two of the case studies analysed for this report included specific references to the use of shelf companies. The prevalence of shelf companies in schemes designed to obscure beneficial ownership is, therefore, unknown. It is possible that the use of shelf companies to obscure beneficial ownership is higher than demonstrated in the case studies in this report, as some shelf companies are likely to have been referred to as "shell companies" in the case studies. It is also likely that the value of shelf companies resides predominantly in the pre-existence of nominee directors and shareholders. Though convenient, many TCSPs will offer nominee services to newly established shell companies, making shelf companies less necessary.

Case Study 19 – Ecuador
Public officials in Ecuador, along with relatives and individuals connected to law firms, created a series of shelf companies in several countries for the purpose of receiving bribe payments. The bribe payments were effected through individuals with links to companies that provide goods and services to a public institution in the oil sector. To send the payments, and to hide the real beneficiaries of the transfers, the suppliers created companies in Panama, Hong Kong, British Virgin Islands, Bahamas, Uruguay, and the US.

Case Study 26 – Egypt
The accused created six British Virgin Island shell companies and used the bank accounts of these shell companies to launder the proceeds of crime of a total amount of more than EGP 1 billion (Egyptian pounds). The predicate offence was "illegal earning". The six shell companies all had a nominee shareholder.

Front company

68. A "front company" is a fully functioning company, with assets, income, expenses. It also exhibits other characteristics associated with the operation of a legitimate business. Any functioning company can be a front company, but the most common form of front company is one that operates in the customer service industry (such as a restaurant, night club, or salon) as these businesses commonly handle cash. Front companies can be exploited to launder the proceeds of crime through the integration of illegitimate funds with legitimate income, often by disguising the illegitimate funds as cash sales made during the course of business. When this is done, these funds can then be deposited into the company's bank account and used by the beneficial owner (if the beneficial owner is also the business owner) or they may pay false expenses in order to transfer the money to the true beneficial owner. Unlike many money laundering operations, where criminals attempt to conceal their illicit wealth and may also attempt to avoid paying

tax on that wealth, criminals who use front companies will occasionally pay company tax on the illicit income to further legitimise the wealth. One case study from Australia (Case Study 2) demonstrates how a front company was used to disguise the proceeds of crime as employee salary payments through the use of a transport company and a third-party salary payment service provider.

69. While front companies have obvious applications to the concealment of illicit wealth more generally, they also conceal the beneficial ownership of that wealth at the placement stage of the laundering process. In the normal course of business, company income is essentially the transfer of money and value from one beneficial owner (the customer) to a second beneficial owner (the business owner). When a front company is used to launder illicit wealth, the "customer" is often the business owner or a close associate. However, company records will record the transfer as having originated from a customer interaction, thereby concealing the business owner or associate as the originating beneficial owner. Over a quarter of the case studies submitted in support of this report involved the use of front companies.

70. Front companies are not always cash-intensive businesses. With today's digitised and transnational economy, front companies can take the form of anything that is expected to generate income from multiple sources. Front companies can also be established to commit fraud, where the company appears to offer a service or perform a function that it does not offer or perform in order to defraud investors and embezzle public funds, or to obscure the beneficial owner of an asset as part of a complex ownership structure, as demonstrated by one case from the US (Case Study 99 below).

71. Financial institutions have also identified instances where informal nominees are solicited by crime groups to establish front companies as a means of circumventing due diligence, money laundering controls or sanctions[35]. This situation arises when a crime group, which is already operating a company, seeks to access the financial system by arranging for an employee to set up an otherwise legitimate operating company in another jurisdiction, where that employee may or may not be an owner of the new company, but does control it typically as an officer. In this situation, the due diligence performed on the new company would not typically identify the indirect connection to the original company, which is hidden, and the new company would act as a front company by engaging in transactions and accessing the financial system in a way that the hidden company could not.

72. While front companies were less prevalent than shell companies in the case studies, it does appear that the use of front companies is a popular technique for the concealment of beneficial ownership and illicit wealth[36]. Although front companies are occasionally directly owned and operated by the beneficial owner, their steady stream of legitimate income serves to conceal the beneficiary of the income itself. For this reason, criminals will continue to exploit front companies to conceal beneficial ownership and integrate illicit wealth.

35 See section 3 for further information.

36 Over a quarter of the case studies submitted in support of this report involved the use of front companies.

Case Study 2 – Australia

An Australian drug syndicate used multiple money laundering methods to launder more than AUD 1 million worth of proceeds of crime. Trust accounts, a front company, high-value goods and real estate were used to launder the profits from cannabis sales. The syndicate also misused the services of two professional facilitators (an accountant and solicitor) to facilitate its criminal activity.

One of the four money laundering methods utilised by the syndicate involved the transfer of illicit wealth to syndicate members in the guise of legitimate wage earnings. The syndicate members employed a company that specialised in processing wages to pay them a wage from their new transport company. Members of the syndicate deposited the cash proceeds of the cannabis sales into the transport company's account. From this account the funds were transferred to the wage processing company. The wage processing company then paid these funds to the syndicate members, seemingly as legitimate wages. Syndicate members were paid an annual wage of around AUD 100 000.

Case Study 99 – United States

U.S. authorities identified front companies used to conceal the ownership of certain U.S. assets by Bank Melli, which was previously designated by US authorities for providing financial services to entities involved in Iran's nuclear and ballistic missile program. Bank Melli was also subject to a call for enhanced vigilance in UNSCR 1803. The Department of Justice (DOJ) obtained the forfeiture of substantial assets controlled by the Government of Iran. These assets included a 36-story office tower in Manhattan at 650 5th Avenue having an appraised value of more than USD 500 million, other properties, and several million dollars in cash. The ownership of the office tower was split between Bank Melli (40%) and the Alavi Foundation (60%), which provided services to the Iranian government, such as transferring funds from the office tower to Bank Melli.

Splitting company incorporation and asset administration over different countries

73. The ability of legal persons to establish and administer banking relationships in different countries is another vulnerability commonly exploited to obscure beneficial ownership. Keeping accounts abroad is an important and legitimate aspect of conducting business in an international market; however it is often difficult for banks to conduct robust customer due diligence on foreign companies. Moreover, the splitting of assets and company incorporation can impede investigation of the business objective of the company and its ownership and control structure, the purpose of transactions, and, most notably, the clarification of the company´s beneficial owner.

74. A large number of cases involved the splitting of company incorporation and asset administration over different countries. In most cases, shell companies were

used to open bank accounts in foreign jurisdictions. In some instances, several accounts were opened in different countries for companies incorporated in foreign jurisdictions, enabling rapid movement of funds over numerous frontiers. This impedes law enforcement efforts to trace the assets.

Case Study 76 – Netherlands
International company A headquartered in The Netherlands paid corruption funds to a government employee via letter box companies. An international company was registered in an international jurisdiction, with a government employee listed as the beneficial owner but with nominee shareholders and directors. Payments were made via a Dutch bank account of a subsidiary of the international company to an account of the international company in Estonia and via an enterprise registered in Hong Kong, after which these funds were paid into bank accounts in a foreign jurisdiction and from there to a Luxembourg bank account of the international company. Bribes were also paid to charities that were directly associated with government employees. In order to account for the bribes, false invoices were entered in the accounting records.

Trusts and other legal arrangements

75. Trusts and other legal arrangements can be used to enhance anonymity by adding an additional layer of complexity through the separation of the legal and beneficial ownership of an asset. In a trust, the legal title and control of an asset are separated from the equitable interests in the asset. This means that different persons might own, benefit from, and control the trust, depending on the applicable trust law and the provisions of the document establishing the trust (for example, the trust deed). In some countries, trust law allows for the settlor and beneficiary (and sometimes even the trustee) to be the same person. Trust deeds also vary and may contain provisions that affect where ultimate control over the trust assets lies, including clauses under which the settlor reserves certain powers - such as the power to revoke the trust and have the trust assets returned, as was possibly the initial intention of the corrupt individual in the Cayman Islands case below (Case Study 14). Other vulnerable features include directed trust arrangements, general or special powers of appointment exercisable by the settlor, and loans repayable on demand to the trust (by the settlor or others). Trusts and other legal arrangements were identified in approximately one-quarter of the case studies analysed for this report. Most of the examples involved common law express trusts, with two making use of a civil law *fiducie*.

76. The enhanced anonymity offered by trusts and trust-like legal arrangements can provide significant benefits to a criminal operation, and can present challenges to financial transparency. The ability to separate legal ownership from beneficial ownership presents a range of challenges for authorities and service providers seeking to determine beneficial ownership; it can also pose a number of risks to the criminals who utilise them. Legal arrangements require the criminal to relinquish legal ownership and control of the asset to a trustee to manage the benefit (or title) of the asset. The introduction of a trustee may pose a vulnerability to the criminal

operation, for instance if the trustee is not complicit, or if control over the trustee is not guaranteed.

77. Whereas the situation of criminals setting up a complex structure involving multiple trusts seems relatively rare (Case Study 42, below, provides one rare circumstance), the combination of a trust interacting with at least one company appears more frequently in the case studies. Almost all of the cases that involved the use of a legal arrangement also involved a company or other legal person. This demonstrates that trusts and similar legal arrangement are rarely used in isolation to hold assets and obscure beneficial ownership, but generally form part of a wider scheme; it might also show that schemes that only involve a trust may be more difficult for authorities to identify. The interaction of the trust with other legal persons adds an additional layer of complexity and helps frustrate efforts to discover beneficial ownership. As further demonstrated by the outcomes of the Horizontal Study[37], information on legal arrangements is rarely available, or is subject to significant challenges with regard to its relevance and accuracy. Case Study 13 from the Cayman Islands (included below), is a good example of this method being used to generate complexity through transfers between a company and a trust.

78. In the cases analysed for this report, legal arrangements were rarely found to hold the actual proceeds of crime. Their role in most schemes was to build additional layers of complexity and further anonymise transactions. When chosen as part of a multi-level ownership structure, trusts appear to enter a company's shareholder register in place of the beneficial owner, thereby disguising the beneficial owner of the shares. Approximately half of the cases that involved a legal arrangement also involved shares, which was proportionally higher when compared to the entire sample population. One case study from Australia (Case Study 2) involved a crime syndicate that created bank accounts held in trust, as well as investment companies, as part of its money laundering scheme, and instructed an accountant to use cash from the proceeds of cannabis sales to purchase shares in the name of the trust accounts and investment companies. The purpose of the trust in this arrangement was to further distance the assets (the shares) from the beneficial owners.

79. Although not as common as the use of legal persons, the frequency of the use of trusts and other legal arrangements is not insignificant. It is possible that, despite the benefits associated with trusts and other legal arrangements, which offer significant opportunities to enhance anonymity by providing a partition between the legal and beneficial ownership of the property, the complexity and expenses associated with establishing and managing a legal arrangement may make them less attractive to criminals. It is also possible that the use of legal arrangements may increase the difficulty of investigating and identifying the beneficial owner, thereby explaining their relatively low prevalence in the case study sample.

[37] See, in particular, Questions 2 and 3 of the Horizontal Study.

Case Study 42 – Italy

The Nucleo Polizia of Milan conducted a preventive seizure of funds traceable to a single family, which were held in the Channel Islands, for a total value of EUR 1.3 billion. The assets were concealed through a complex network of trusts. Multiple trust accounts hid the beneficiaries of assets consisting of public debt securities and cash. The investigation established that between 1996 and 2006 the subjects placed their assets in Dutch and Luxembourg companies through complex corporate operations and by transferring them to different trusts in the Channel Islands. Subsequently, the funds were legally repatriated through a tax amnesty in December 2009. The investigation identified chartered accountants who had, over time, facilitated the concealment of funds through trusts with the aim of facilitating laundering and reinvestment.

Case Study 13 – Cayman Islands

Mr. A established a Cayman Islands revocable trust, with himself as settlor and a local TCSP acting as trustee. Mr. A also arranged for the incorporation of a Cayman Islands company known as 'Company B', with the local TCSP also acting as the registered office.

The TCSP became aware of allegations relating to Mr. A and his involvement in an oil and gas contract scam which also involved members of a foreign government. Over a two-year period, the TCSP reported that the trust and underlying company had received numerous transfers of funds and property from what was now deemed to be questionable sources, which in turn heightened its suspicions and prompted an STR. An analysis of the trust accounts revealed outgoing funds to individuals named in numerous media reports who allegedly took part in the kickback scandal. In response to a request, the foreign jurisdiction confirmed that Mr. A was being investigated for money laundering and corruption of government officials.

Using individuals and financial instruments to obscure the relationship between the beneficial owner and the asset

80. In addition to the generation of complex ownership and control structures, criminals often employ additional techniques to further obscure the relationship between them and their assets. As a methodology, obscuring the relationship between the beneficial owner and an asset differs from the generation of complex ownership and control structures in that, rather than aiming to create distance via legal complexity, it attempts to create a false or misleading picture of the true ownership and control structure. Techniques most often used to achieve this include the use of formal and informal nominees and professional intermediaries. Other techniques, such as the use of bearer shares and the declaration of numerous beneficiaries, have also been identified, but appear to be less common.

Bearer shares and bearer share warrants

81. Bearer shares are company shares that exist in certificate form and are legally owned by the person that has physical possession of the bearer share certificate at any given time. Ownership and control of bearer shares can be exchanged anonymously between parties by way of physical exchange alone, as no record of the exchange needs to be documented or reported.

82. Due to the inability to accurately ascertain and monitor the owner of a bearer share at any given time, determining beneficial ownership of legal persons controlled by bearer shares is nearly impossible. For this reason, bearer shares and bearer share warrants have historically been recognised as posing a significant money laundering risk, particularly in relation to the concealment of beneficial ownership. This risk is reflected in Recommendation 24 of the FATF Standards, which requires member countries to take measures to prevent the misuse of bearer shares and bearer share warrants.

83. In most jurisdictions, bearer shares have been reformed or eliminated altogether through the dematerialisation of the bearer share certificate into a computerised register or ledger of shares. Even in jurisdictions where bearer shares are still permitted by law, the financial sector has taken measures to limit their effectiveness, often by requiring them to be placed into trust prior to the commencement of a client relationship. Other jurisdictions have implemented measures that require an intermediary to facilitate the transfer of bearer shares to make the transfer lawful[38]. As a result, the prevalence and use of bearer shares and bearer share warrants have markedly declined in recent years. Of the case studies submitted in support of this report, only four involved the use of bearer shares. However, this may also be due to the immense challenge of identifying the beneficial owner of bearer shares, the near impossibility of which may limit the number of cases involving their use.

Formal nominee shareholders and directors

84. A nominee shareholder is the registered owner of shares held for the benefit of another person. A nominee director is a director appointed to the board of a company to represent the interests of his/her appointer on that board. Legally, nominees are responsible for the operation of the company, and accept the legal

[38] Of the 50 jurisdictions assessed against the 2012 FATF Recommendations at April 2018, 45 jurisdictions either do not have bearer shares or bearer share warrants in circulation, or do not have them in existence. Five jurisdictions do not have restrictions on bearer shares but it is unclear whether there are bearer shares and/or bearer share warrants in circulation. Among the 45 jurisdictions, 17 prohibit bearer shares and/or bearer share warrants, 15 require existing bearer shares and/or share warrants to be converted into registered shares where they exist, five require them to be held with a regulated financial institution or professional intermediary, two require shareholders with a controlling interest to notify the company and the company to record their identity, one country has a range of the previously mentioned options and five do not have bearer shares and/or bearer share warrants.

obligations associated with company directorship or ownership in the country in which the company is incorporated. However, in some cases a nominee may hold the position of director or shareholder in name only on behalf of someone else. These arrangements may be controlled by a trust arrangement or civil contract between the nominee and actual director or shareholder.

85. The use of nominee shareholders and directors is a common phenomenon that occurs in most countries. In some countries there is also formal recognition in law of certain scenarios in which nominee arrangements are permitted (such as in relation to publicly traded companies). Nominees are utilised in a number of scenarios, including to shield the nominator from public disclosure requirements or to meet legal requirements of the country in which the company is incorporated (such as requirements for companies to have a director residing domestically). A range of service providers are known to offer **formal nominee services**, including legal and accounting professionals, TCSPs, and professional nominees (people who rent their identification information to companies for nominee purposes only, but provide no additional services to the company). The vulnerabilities associated with the provision of nominee services by lawyers, accountants and TCSPs are outlined in greater detail in Section 3 of this report. One New Zealand case study (Case Study 81 below) demonstrates how a TCSP provided nominee directorship services for over 1 000 companies registered in New Zealand on behalf of foreign clients. Authorities suspect that at least 73 of these companies facilitated crimes in foreign jurisdictions, including the smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and money laundering.

86. While the use of nominees is lawful (or at least not unlawful) in most jurisdictions, nominees have been used to disguise ownership and control, or to circumvent laws designed to manage foreign business ownership and foreign trade. FIUs and law enforcement agencies also report the use of nominee services by known criminals and individuals who have been prohibited from serving as a director of a company due to previous malfeasance. As a result, the availability and use of formal nominee services are vulnerable to exploitation for the purposes of disguising beneficial ownership. Of the case studies analysed for this report, just under half of the cases involved formal nominees. The presence of nominee directors and shareholders in company records can also affect law enforcement investigations by delaying the identification of the beneficial owner, or by creating false links between companies that share nominees.

87. These vulnerabilities are reflected in Recommendation 24 of the FATF standards, which states that countries should take measures to prevent the misuse of nominee shares and nominee directors.

Case Study 81 – New Zealand

Companies registered in New Zealand by a Vanuatu-based TCSP operated by New Zealand citizens were suspected of acting as shell companies that facilitated crime in foreign jurisdictions. The TCSP acted as nominee shareholders and provided nominee directors who resided in jurisdictions such as Vanuatu, Panama and the Seychelles.

The TCSP also provided a New Zealand-based nominee director to satisfy the legal requirement to have a New Zealand resident director and address. In the case of Company A, the employee recruited to act as a director likely had no knowledge of the activities taking place, as they had no previous involvement in any of the TCSP activities.

By 2010, the TCSP had registered approximately 2 000 companies in New Zealand on behalf of clients in foreign jurisdictions. The address, in Auckland, was used as the registered office for most of the companies. Authorities suspect that at least 73 of these companies facilitated crimes in foreign jurisdictions, included the smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and money laundering.

Informal Nominee Shareholders and Directors

88. Informal nominee shareholders and directors perform the same function as formal nominee service providers; however, their connection with the true director, shareholder, or beneficial owner is often of a personal, rather than of a professional, nature. Informal nominees identified by law enforcement commonly include spouses, children, extended family, business associates (who are being controlled by the actual owner or controller of the company), and other personal associates otherwise unrelated to the beneficial owner's business interests. Indeed, the relationship between an informal nominee and the actual owner or controller of a company or shares can vary significantly. Law enforcement agencies and FIUs have reported instances where foreign students and tourists have been convinced or coerced into establishing companies on behalf of third parties, sometimes in exchange for nominal payments or other personal benefits. These individuals are recorded as directors or controlling shareholders of these companies; however, they are rarely involved in the operation of the company post-formation. Of the case studies analysed for this report, just under half involved informal nominees.

89. Unlike formal nominee arrangements, informal nominee arrangements will rarely be governed by a contractual agreement. Furthermore, while formal nominees will always seek to insulate themselves from the activities of the legal person or arrangement, informal nominees are more likely to profess to be the beneficial owner of the legal person or arrangement in an effort to maintain the fiction created by the true beneficial owner. For this reason, informal nominees are often referred to as "straw" or "front" men. One Russian case study (Case Study 87 below) demonstrates how the ownership of companies used to facilitate fraud against a government contract was passed from the suspect (Mr. X.) to a number of different "straw men", including Mr. X's daughter. At least one of the informal

nominees received a salary in return; however, they did not perform the role of a professional nominee and were unaware of the activities of the company. The purpose of passing ownership of the companies to informal nominees was to further distance the companies from Mr. X, who was related to the man responsible for the project in the public department.

90. There are significant risks associated with acting as an informal nominee, as they are ultimately legally responsible for the activities of the company and will often lack the resources or expertise required to distance themselves from any legal obligations or repercussions. Furthermore, informal nominees are unable to utilise protections such as client confidentiality or legal professional privilege, which are available to some formal service providers. As a result, informal nominees are more susceptible to law enforcement investigations. That being said, informal nominees who have never previously come to law enforcement attention or whose association with the true beneficial owner or controller is indirect (e.g. not a relative or business associate) are often difficult to identify by financial institutions and some competent authorities.

91. A related phenomenon reported by some law enforcement agencies is the use of stolen identities to establish legal persons. In these instances, the victim of the identity theft is ostensibly an informal nominee for the legal person, albeit without their knowledge or consent. Law enforcement agencies have also identified situations where companies have been registered to informal nominees who have previously sold their identification details to a third party. These informal nominees are often incentivised to sell their identification details due to financial hardship. In these instances, the informal nominee also has no visibility of the company their details are recorded against; however, they may not necessarily be *victims* of identity fraud. One New Zealand case study (Case Study 80 below) demonstrates how bank accounts held in the names of students were used to receive laundered funds from foreign bank accounts to purchase properties. Another New Zealand case (Case Study 77) demonstrates how lower-income individuals can be manipulated into selling their identification information to professional money launderers, who then use them to establish companies and bank accounts.

92. While the cases analysed for this report demonstrated an approximately equal distribution between the use of formal and informal nominees, law enforcement and FIU experience indicates that criminals, particularly those with limited resources, will favour the use of informal nominees rather than formal nominee service providers. Often these informal nominees are family members, particularly spouses, who are frequently complicit with the beneficial owner's criminal activities. The reliance on familial nominees may stem from the ease with which the true beneficial owner can control and manage their activities.

Case Study 77 – New Zealand

A New Zealand shell company was set up by a New Zealand TCSP based in Vanuatu. The shell company was registered on behalf of an unknown overseas client and nominees were used to hide the identity of the beneficial owners. The actual business of the shell company was not apparent and was not indicated by the company name. The address listed on the companies' register was the same virtual office in Auckland as the TCSP. The nominee director resided in Seychelles, and the nominee shareholder was a nominee shareholding company owned by the TCSP. The nominee shareholding company was itself substantially a shell company and had been used as the nominee shareholder for hundreds of other shell companies registered by the TCSP.

News reports indicated that a power of attorney document transferred the directorship to a Russian national who had sold his passport details, with a bank account opened in Latvia. When journalists from the Organised Crime and Corruption Reporting Project (OCCRP) made contact with the Russian national, the man revealed he was unaware of the New Zealand company or its bank accounts. His identity, which he had sold, had been used without his knowledge. Furthermore, a former officer of the Russian tax police told journalists that hundreds of law firms specialise in establishing ready-made shell companies for their clients, who want to remain anonymous. Usually, these law firms rely on disadvantaged individuals who sell them passport details for approximately USD 100–300.

Trade transactions were conducted with several Ukrainian companies including a state-owned weapons trader. The contracts were then cancelled after the funds had been transferred and refunds were made to different third-party international companies. Transactions were also made with three other New Zealand shell companies registered by the same TCSP, using the same nominee director, nominee shareholder and virtual office address as the shell company. News reports indicated that all four shell companies had been involved in laundering USD 40 million for the Sinaloa drug cartel based in Mexico.

Case Study 80 – New Zealand

Shell companies based in Panama, Belize, and the UK with nominee shareholders and directors were used to open Latvian bank accounts to conduct hundreds of millions of dollars' worth of international payments. The majority of transactions were payments being made on behalf of Vietnamese entities for imported goods, or payments to Vietnamese expats living overseas on behalf of purportedly Vietnam-based senders. This distinct Vietnamese connection indicated the accounts might have been controlled or administered from within Vietnam. New Zealand bank accounts, which were held by students or by fruit wholesalers and exporters, were used to receive funds

transferred from bank accounts in Latvia, Cambodia and China. More than 15 New Zealand properties were purchased with the funds, all of which were facilitated through New Zealand law firms. Information suggested that the Latvian accounts were also being "topped up" by other shell company bank accounts based in international jurisdictions, indicating a co-ordinated layering process being undertaken.

Case Study 87 – Russia

A state customer concluded contracts on research work and the development of a special software with Contractor #1 and Contractor #2. Analysis of financial transactions showed that these contractors did not conduct any research activities themselves, but transferred budgetary funds to subcontractors with real scientific laboratories among them. The majority of funds from Contractor #1 was sent to its subcontractor, who channelled funds to a shadow financial scheme consisting of multiple layers of shell companies. The funds were finally withdrawn in cash. The majority of funds from Contractor #2 was sent to a real estate company that invested these funds into its business activity, acquired luxury cars and granted zero-interest rate loans to a number of individuals.

Analysis of ownership data, address registry information, an air tickets booking database, financial transactions and law enforcement data showed that Contractor #2 was previously owned by Mr. X, before the ownership was passed to straw men uninvolved with the scheme. The real estate company was formerly owned by Mr. X, before the ownership was transferred to his daughter. Contractor #1 was owned by straw men who had no idea about the company's business activities and received instructions from Mr. X. These straw men received a "salary" from the company's account. The director of the state customer's department responsible for research activities was a brother of Mr. X. A daughter of the state customer department's director acquired expensive real estate using cash that was deposited in advance in her account. The woman who had joint flights with Mr. X acquired expensive real estate using cash that was in advance deposited into her account in advance.

Declaring Numerous Beneficiaries

93. In some instances, the declaration of numerous beneficiaries on one account is used to confuse financial institutions and conceal the true nature of transactions undertaken through that account. FIUs and financial institutions have reported cases where large numbers of customers have been declared as beneficiaries on a single bank account in such a way that the bank has difficulty establishing which transaction was made on behalf of which beneficiary. In the instances where this has occurred, it is unclear whether the controller of the transactions was listed as a beneficiary. Regardless, the use of a single account to co-mingle transactions from a large number of beneficiaries poses a challenge when determining the ultimate

beneficial owner, and when attempting to follow the chain of suspicious transactions.

Case Study 38 – Israel

This scheme was used to hide funds from social engineering fraud and other criminal offenses. The cover story for the criminal offenses was international trade – funds from merchants in Europe and the US that were sending payments to suppliers in East Asia. The suspect, the owner of a registered MSB, operated a second, unregistered MSB. The suspect used several natural persons as his contact points in East Asia, who in turn contacted local TCSPs for the purpose of setting up international companies and opening bank accounts. Local straw-men were registered as the shareholders of the new international companies established for the scheme. In addition, shareholders were registered based on passports provided by the suspect's contact persons mentioned above. The registered addresses of the companies were in East Asia. Bank accounts were opened in the same East Asia countries where the offices were located.

Some of the funds were transferred to Israel to an account opened by the suspect. More than 60 beneficiaries were declared to the bank as beneficiaries, in such a way that the bank had difficulty in establishing which transaction was made on behalf of which beneficiary. The funds were sent from the companies set up by the suspect but the receiving bank did not know that these companies were actually under the suspects' control.

Use of Professional Intermediaries in Forming and Managing Legal Persons and Arrangements

94. The use of specialists and professional intermediaries, including lawyers, accountants, and TCSPs, is a key feature of the money laundering and broader organised crime environment. Professional service providers significantly enhance the capacity of criminals to engage in sophisticated money laundering schemes to conceal, accumulate and move volumes of illicit wealth. As a result, professional intermediaries have been assessed as posing a high money laundering risk in most countries.

95. The vulnerabilities posed by professional intermediaries are outlined in greater detail in Section 3 of this report.

Falsifying activities

96. Unlike the generation of complex ownership and control structures and the concealment of the relationship between the beneficial owner and an asset, which can serve both legitimate and illicit purposes, some techniques used to hide beneficial ownership are purely criminal. These techniques are designed to falsify activities to commit a crime via deception. The use of false loans and invoices to fraudulently disguise the beneficial ownership of a transaction is the most common

of these techniques, but others, such as the manipulation of company prospectuses and annual reports, have also been identified, though infrequently.

Use of False Loans and Invoices

97. A common means of disguising the beneficial owner of wealth and assets is through the use of false loans. This method, which is often referred to as a "loan-back" or "round-robin" scheme, principally involves money being sent to companies which are owned or controlled by, or on behalf of, the same individual, and returned in the guise of a loan. These schemes generally operate following two key steps:

- *Payment of business invoices*: the individual or business pays an invoice or series of invoices to a company (which is often located in another country) that is controlled/beneficially owned by them, or to an associate or professional intermediary operating on their behalf. The funds may be sent via numerous legal persons in the guise of legitimate business transactions, but will ultimately pool in the account of an international company that is operating in the interests of the beneficial owner of the company that paid the initial invoice. The purpose of this stage is to reduce the taxable income of the originating company or individual by increasing their (seemingly legitimate) business expenses.
- *Third-party loan*: once the funds have been pooled in the accounts of the international company, they are returned to the original company/individual, or a close family relation (commonly a spouse or child) or associate, in the form of a private loan. Occasionally these loans will be accompanied by false loan documents, but often the loan is recorded only in the description of the bank transfer. The purpose of this step is to return the wealth to the beneficial owner in a manner that is exempt from income taxation.

98. Loan-back schemes can involve the payment of interest, which may be used as a further means of channelling money into international bank accounts and reducing domestic tax obligations (as demonstrated in Case Study 7 from Australia). These schemes do not have to involve interest payments – there may be no actual obligation for the beneficial owner to repay the false loan. Regardless of the mechanics of the loan arrangement, the scheme serves the purpose of disguising the fact that the lender and borrower are beneficially owned by the same natural person.

99. Loan-back schemes are sometimes promoted and facilitated by professional service providers. In these instances, the international company used in the loan structure is controlled by the scheme promoter, who receives a portion of the laundered funds as payment for facilitating the scheme. This also serves the purpose of separating the beneficial ownership of the funds and decreasing the likelihood of detection. One case study from Australia (Case Study 6 below) demonstrates one such scheme operated by an Australian accountant via companies controlled by him or his associates in Hong Kong and the BVI.

Case Study 6 – Australia
Investigating authorities identified that suspect A operated an import business in Australia and was a participant in a tax evasion scheme operated by an accountant. Suspect A and his wife were directors and shareholders of an Australian company (company 1). Suspect A was also a director and shareholder of another Australian company (company 2). An associate of suspect A was the co-director of company 2. Authorities identified that the accountant controlled company 3, which was registered in Hong Kong and operated a bank account in Australia. This company was used to issue false invoices to companies 1 and 2. Over a five-and-a-half-year period company 3 issued false invoices to companies 1 and 2 for supposed "brokering services." Suspect A paid the false invoices, which totalled more than AUD 2 million, by directing companies 1 and 2 to pay company 3. The funds paid to company 3, less the accountant's 10% fee, were returned to suspect A and individuals associated with him.

Manipulation of a company´s prospectus, annual report etc.

100. While identity fraud is a common typology for natural persons to disguise their true identity, it is also possible to disguise the true activity and purpose of legal persons. One of the cases analysed for this report (Case Study 14) demonstrated how the manipulation of the financial status of a company through the inclusion of false and misleading information in the company prospectus and annual report allowed it to qualify for a listing on the stock exchange in the country of registration. While this measure was intended to improve the reputation and the economic activities of the company, it also led to a situation in which that company may have been subject to reduced customer due diligence obligations. Many AML/CFT regimes allow simplified due diligence measures for corporate entities that are listed on organised and regulated markets, since they are already subject to certain transparency requirements. Therefore, the ability for criminals to list a company on a stock exchange in a manipulative way can support future activities designed to obscure beneficial ownership, including the use of the company as a "front company".

Case Study 14 – Cayman Islands
The managing director of an overseas company issued a prospectus which contained misleading and false information within the company's annual report. He overstated the company's group revenue by 275%. This information was provided to that country's securities commission as part of the company's proposal for listing on their stock exchange. The managing director established a revocable trust and underlying company in the Cayman Islands. He then opened an overseas bank account in the name of the Cayman Islands company for which he held the power of attorney, allowing him to trade in the account. This

structure was devised to hide the managing director's trading in the overseas company and to hide assets derived from his illegal activities. The Cayman Islands company held over USD 1 million in this bank account. The Financial Reporting Authority (FRA) made an onward disclosure to the FIU of the foreign national's home country. The foreign national has been charged in his home country with three counts of providing misleading and false information.

SECTION 3 — VULNERABILITIES OF PROFESSIONAL INTERMEDIARIES

101. Professional intermediaries, including lawyers, accountants, and TCSPs, play an important role in modern society. For the most part, these professionals operate with integrity and in accordance with national and international laws. However, the reputation of these professional intermediaries also makes them the target of criminals and corrupt actors, and may result in some professionals becoming involved in the concealment of beneficial ownership for criminal purposes, either through coercion or corruption, or through negligence or a failure to identify suspicious activities. This section provides an overview of the vulnerabilities of professional intermediaries, and how they are exploited to conceal beneficial ownership.

102. The use of specialists and professional intermediaries, including lawyers, accountants, and TCSPs, is a key feature of the money laundering and broader organised crime environment. Criminals use professionals to obtain specialist advice and skills in complex financial, business, company, and tax matters to disguise the true ownership or source of their assets. Operating through or behind a professional adviser provides a veneer of legitimacy to criminal activities and, where complex structures are established, creates distance between criminal entities and their illicit wealth. The majority of the case studies analysed for this report involved a professional intermediary.

103. Although there are unique elements to each jurisdiction's legal system, the broad description of the role of professional intermediaries can be divided into four general categories[39]:

- systems in which legal persons can be established without the involvement of professional intermediaries
- systems in which professional intermediaries (other than notaries) are required
- notarial systems
- systems in which the company registrar tests the accuracy of filings or takes on the CDD obligations of the professional intermediary.[40]

104. Criminals may employ the services of numerous professional intermediaries simultaneously, with each professional playing a separate but crucial role in the criminal enterprise. Of the case studies submitted in support of this report, more than one-third involved the use of more than one professional services sector, and a similar number of cases involved multiple intermediaries in the same sector. Of the cases that involved more than one professional intermediary, TCSPs represented the

39 As assessed in the Horizontal Study at Annex B; see in particular Question 1.

40 Hybrids of these systems are also possible.

large majority of cases, while legal professionals (including civil notaries) were also common; however, the representation of accounting professionals in cases involving numerous professional intermediaries was rare.

105. Of the cases that involved multiple intermediaries from the same sector, the TCSP sector represented the overwhelming majority of these instances. When multiple TCSPs were exploited in a single scheme, almost all of the cases involved TCSPs in multiple jurisdictions. This is reflective of the role of TCSPs in establishing and managing local companies on behalf of foreign clients. Conversely, in instances where multiple legal or accounting professionals were used, the majority of cases involved the use of multiple lawyers/accountants in the same jurisdiction. Additionally, approximately half of the cases involved unwitting or negligent intermediaries. This indicates that, in instances where multiple lawyers or accountants are utilised to facilitate a scheme, it is likely that the criminal clients are attempting to avoid suspicion by limiting their engagements with any single professional. However, the small number of cases available makes it difficult to make a definitive assessment.

106. The increasingly global nature of organised crime and the finance sector has driven demand for the advice and services of professional intermediaries who can operate across, or have professional connections within, numerous international jurisdictions. As a result, criminal groups have been known to be connected with multiple intermediaries across multiple countries. Analysis of the case studies identified that a majority of intermediaries were operating on behalf of international clients.

107. The FATF Standards require DNFBPs, including lawyers, notaries, accountants, and TCSPs, to perform CDD, maintain CDD and transaction records, and submit suspicious transaction reports. These obligations came into effect when the standards were revised in 2003; however, many countries have not yet implemented them in law[41]. Of those countries that have implemented obligations on DNFBPs, many have not implemented those obligations effectively via appropriate supervision and monitoring[42]. This was also confirmed by the findings of the Horizontal Study[43]. As such, professional intermediaries are often subject to limited AML/CFT obligations.

41 Of the 50 jurisdictions that have been assessed against the 2012 FATF Recommendations at April 2018, 34 jurisdictions have major or moderate shortcomings in their measures for Recommendation 22 on DNFBPs' applying customer due diligence, and 30 have major or moderate shortcomings for Recommendation 23 on the other measures that DNFBPs need to take, including the reporting of suspicious transactions. 36 jurisdictions have major or moderate shortcomings in their mechanisms for regulating and supervising DNFBPs under Recommendation 28.

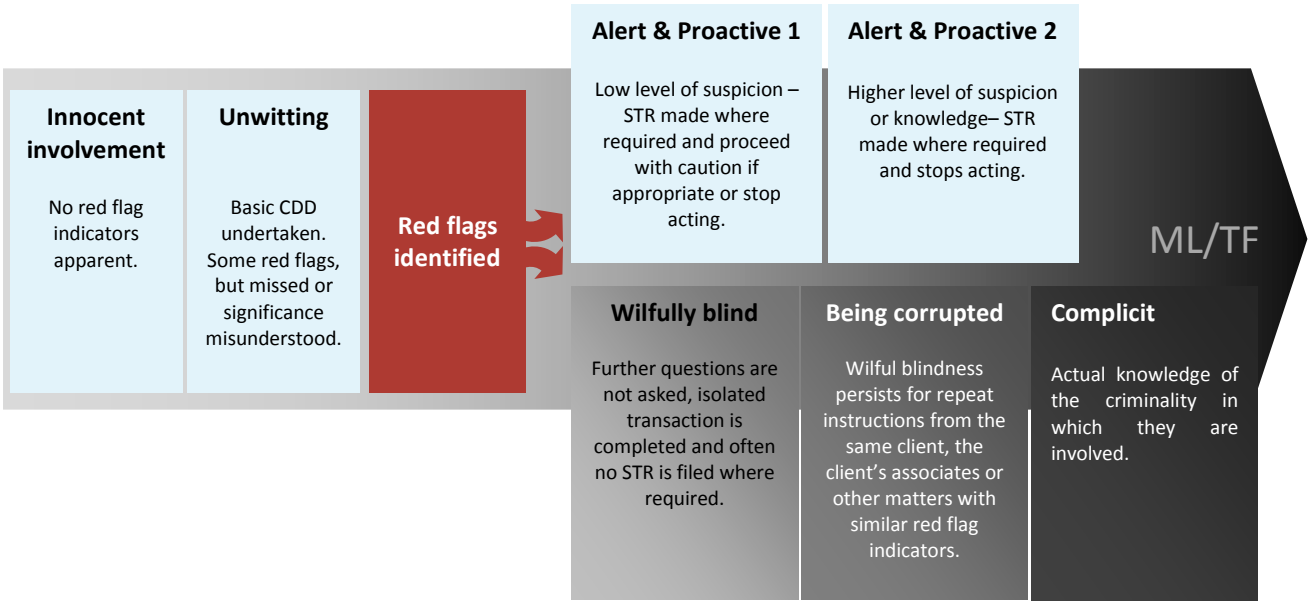
42 Of the 11 jurisdictions that have been assessed as having minor or no shortcomings in their mechanisms for regulating and supervising DNFBPs, 8 are not supervising, monitoring and regulating DNFBPs appropriately.

43 See, in particular, Questions 4-6 of the Horizontal Study at Annex B.

Continuum of complicity

108. In its 2013 report, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, the FATF assessed that the involvement of legal professionals in money laundering could not be described simply as either "complicit" or "unwitting", but tended to follow a continuum from "innocent involvement" to "complicit" (see Figure 1, below). [44]

Figure 1. **FATF Assessment of the Involvement of Legal Professional in ML/TF**[45]



109. This "**continuum of complicity**" can be equally applied to all professional intermediary sectors, and is not unique to the legal profession.

110. While it is widely acknowledged[46] [47] [48] that professional intermediaries can act as enablers of money laundering and terrorism financing, little is understood about how these intermediaries are sourced or recruited, and the degree to which intermediaries are innocently, negligently or complicity involved. It is likely that this intelligence gap is exacerbated by various factors, including:

---

44 FATF, 2013: p. 5.

45 Of the 11 jurisdictions that have been assessed as having minor or no shortcomings in their mechanisms for regulating and supervising DNFBPs, 8 are not supervising, monitoring and regulating DNFBPs appropriately.

46 Van der Does de Willebois, E. et al., 2011.

47 ACIC, 2017.

48 OECD, 2001.

- The limited AML/CFT obligations imposed on DNFBPs in many countries due to partial compliance or non-compliance with Recommendations 22 and 23, as well as the ineffective implementation of AML/CFT obligations in some countries.
- A reluctance by professional intermediaries to comply with their AML/CFT obligations due to perceived conflicts with their duty to their client, or their obligations to protect client confidentiality and legal professional privilege.
- The fact that professional intermediaries are often not the primary targets of law enforcement investigations, and details pertaining to their activities are not universally recorded on law enforcement indices.

111. This means that, despite the role of professional facilitators in enabling serious and organised crime, it is not possible to accurately quantify the degree to which they are involved, or their level of complicity, with any certainty. This report has analysed the case studies provided by 34 participating countries, and has attempted to draw conclusions on the complicity of professional intermediaries based on the information provided.

112. Approximately one-third of all cases were assessed as involving a complicit professional intermediary. Of the cases where intermediaries were assessed as being complicit, the majority were assessed as having designed the scheme themselves and promoted it to potential clients (predominantly as an effective tax minimisation method). In these instances, the professional intermediary was often the subject of the primary investigation.

113. Of the three professional sectors analysed, the accounting profession was most likely to be complicit in their involvement in schemes designed to conceal beneficial ownership. Moreover, both legal and accounting professionals were more likely to be the designer of the scheme, rather than simply a complicit intermediary in a scheme designed by another party or the client themselves. However, unlike accounting professionals, legal professionals were more likely to be unwittingly or wilfully blind in their involvement in the scheme. It is likely that the financial acumen of the accounting profession, and the ease with which accountants can identify suspicious activities indicative of money laundering or other financial criminality, may limit their unwitting involvement in these schemes. It may also be indicative of the nature of the case studies provided, which often involved the predicate offences of tax evasion and fraud, many of which were orchestrated by corrupt professionals.

114. The value and utility of an intermediary's professional services to a money laundering scheme is not strictly contingent on the complicity of the intermediary. An innocent, unwitting or negligent intermediary can be as valuable as a complicit intermediary if their services result in a desirable outcome for their criminal client. This is particularly true in the context of disguising beneficial ownership, as many of the services offered by professional intermediaries, such as the establishment of legal persons and arrangements, are commonplace and not necessarily indicative of corruption or criminality. Law enforcement agencies in some jurisdictions observed that more money laundering related investigations involved complicit professional intermediaries relative to unwitting intermediaries.

OVERVIEW OF COMMONLY EXPLOITED INTERMEDIARIES

115. This section provides an overview of the legal, accounting, and TCSP sectors. The purpose of this information is to contextualise the sectors commonly exploited by criminals to establish complex ownership structures and otherwise assist in the concealment of beneficial ownership information.

Legal Professionals

116. The legal sector is a large and multifaceted industry that provides a range of services to a broad spectrum of clients. Despite the presence of large domestic and multinational law firms in some countries, the legal sector is principally characterised by small business enterprises. Sole practitioners or partnerships with minimal additional non-partner staff represent the majority of the legal sector in most countries. This low level of market share concentration is in contrast to the banking sector, which is often dominated by a smaller number of large domestic and international banks.

117. While large and medium-sized law firms will offer a broad range of services, most law firms specialise in only one service segment, such as commercial law, personal legal services, or criminal law. Often, law firms that specialise in large-scale and international commercial law will employ a higher number of non-partner staff due to the complexity and resource intensive nature of large corporate issues. However, the choice to offer specialised services often does not preclude a law firm from providing services in other areas of law[49]. As such, firms which specialise in personal and family law matters may also be involved in commercial law matters and the establishment of companies and businesses.

118. The legal sector has historically demonstrated a low level of industry globalisation, with a majority of law firms servicing local clientele. This reflects the small-business nature of the sector and the desire of clients to deal with a local law firm. However, greater access to information and communication technologies, as well as an increasing market for transnational legal services has prompted large law firms to expand into the global market to pursue growth opportunities. Many major law firms are actively pursuing strategies to merge or establish relationships with international law firms to increase their presence in key international markets.

119. The legal sector in most countries is required to maintain a membership with a professional body, such as a law society or bar association. These professional bodies impose strict rules and codes of conduct on their members, and often serve as self-regulating bodies in countries where legal professionals are subject to AML/CFT oversight. Rules imposed by professional bodies operate in addition to

[49] Some exceptions exist in countries where lawyers are subject to more than one model of licencing or industry oversight.

overarching legislative obligations, and can result in severe financial or professional sanctions if breached.

120. The notarial sector differs from the legal sector in many countries, particularly civil law countries. In some civil law countries, notaries do not represent parties to a contract and are not intermediaries in the same sense as legal professionals. Many notaries do not maintain long-term client relationships, and instead are obliged to be impartial and independent, advising the parties of a contract on equal terms. Unlike legal professionals in private practice, many notaries carry duties as public office holders. These obligations of fairness and the public office duties will influence the scope of what the notary must do to assess the risk of money laundering.

Role in the Establishment and Management of Legal Persons and Arrangements

121. Legal representation is commonly sought in most countries to facilitate the establishment of companies and other legal persons and arrangements. In cases where legal representation is not strictly required, their legal expertise will often be engaged as a precautionary measure to ensure the lawful establishment of a legal person or arrangement, particularly in instances where a foreign jurisdiction is involved.

122. Large law firms that operate across numerous jurisdictions play an important role in the establishment of legal persons in one country of operation on behalf of a client in another country of operation. Often, multinational law firms will seek to establish branches, merge with existing firms, or establish agent relationships with smaller firms in financial hubs and trade centres. As such, they offer opportunities to facilitate the development of transnational company structures in support of legitimate global business ventures. It is also possible for their expertise in setting up cross-border structures to be utilised to conceal the beneficial ownership of illicit assets.

123. In the absence of an international presence, law firms will utilise professional associations and global alliance networks to effectively operate across international borders. These networks of otherwise independent law firms enable clients to seamlessly access the services of affiliated law firms in international markets. While formal membership-based alliances often operate under an association code of conduct, this does not necessarily include a compulsory AML/CFT compliance program, and not every member firm will be subject to AML/CFT regulation (see footnote 40 and 41).

124. Of the case studies analysed for this report, one-third specifically referred to the involvement of legal professionals (including notaries)[50]. It is likely that some of the case studies involving TCSPs actually involved lawyers or TCSPs with legal

[50] Of the cases that involved legal professionals, 25 cases referred to the involvement of lawyers, five referred to the involvement of notaries, and four referred to the involvement of both.

qualifications. The use of the term TCSP as a catch-all term for professionals involved in company establishment has been identified as a possible reporting issue throughout this project.

125. Where the involvement and activities of legal professionals could be assessed, the majority were found to have been working on behalf of a direct client. A small number were assessed as providing services to another professional intermediary on behalf of a third-party client.

Accountants

126. Like the legal sector, the accounting sector is a large industry that provides services and advice to a range of clients. The range of services offered by the accounting sector is more focused in comparison to the legal sector, with audit, tax, and advisory services representing the vast majority of business.

127. The accountancy sector has a moderate level of industry globalisation due to the presence of large multinational accounting firms. The level of globalisation is increasing through the acquisition of smaller firms by larger multinationals. However, despite the industry globalisation being more pronounced than the legal sector, and the larger market share held by large multinational accounting firms, the accounting sector, like the legal service sector, is characterised by small enterprises and sole proprietors.

128. The majority of accounting enterprises, including sole proprietors and enterprises employing fewer than 20 people, typically service individuals or small businesses, while the large multinational firms tend to service large companies and public sector authorities.

129. Much like the legal sector, accounting professionals who join an accredited accounting body are governed by a code of ethics. However, unlike the legal sector, accounting professionals in many countries are not required to maintain a membership to any independent oversight body[51]. As a result of this dynamic, and the significant number of sole proprietors in operation, it is difficult to monitor the accounting sector's awareness of AML/CFT risks and its adherence to AML/CFT obligations. Like the legal sector, FIUs and regulatory bodies where they perform a supervisory function face a number of challenges in accurately and effectively supervising the sector.

Role in the Establishment and Management of Legal Persons and Arrangements

130. The primary role of accounting professionals in the establishment of legal persons and arrangements is the provision of expert advice on business structures, asset management, and taxation obligations domestically and internationally. In many countries, accountants are the first professional consulted by small businesses

[51] For example see the Mutual Evaluation reports of Andorra, Bahamas, Bhutan, Denmark, Ireland, Mexico and Slovenia, available from www.fatf-gafi.org.

and individuals when seeking general business advice and advice on regulatory and compliance matters. Where services are not within their competence, accountants advise on an appropriate source of further assistance, or procure the services of an appropriate professional on behalf of their client.

131. In most countries, accountants are authorised to establish companies on behalf of their clients; however, the majority of accounting firms only provide services to established businesses, or advise on proposed business structures, and will not become directly involved in the establishment of legal persons themselves. This is largely due to the small nature of most accounting firms, and the low level of globalisation that these firms exhibit. Those accounting firms that do offer company establishment services are also likely to maintain a significant financial management role in the company, including being a signatory on accounts held by that company. Analysis of the role of accounting professionals in the case studies identified that only one was involved in the establishment of legal persons or arrangements in their own country of operation, and three were involved in the establishment of legal persons in a foreign jurisdiction.

132. As with the legal sector, accounting firms that operate across multiple jurisdictions generally leverage their global presence to offer company establishment and management services. However, the number of accounting firms with a global footprint is low in comparison to the legal sector, and, as a result, smaller firms often rely on professional associations and alliance networks to service transnational clients. Alternatively, small firms will act as an intermediary between clients and service providers based in overseas jurisdictions, including accountants, lawyers, and TCSPs. The majority of accounting professionals identified in the case studies were assessed as having facilitated international activities on behalf of their client.

133. Due to the contractual nature of trusts and other legal arrangements, accountancy professionals are rarely relied upon to establish a trust. Accounting professionals will advise clients on trust arrangements and may assist clients by acting as a settlor, trustee, or protector of a trust arrangement. Unlike the legal sector, the accounting sector places few restrictions on accountants maintaining these positions in a legal arrangement. However, in the case studies provided in support of this project, only one accountant offered directorship/trustee services to their client.

134. The accounting profession was the least represented sector in the cases analysed for this report. It is likely that some case studies referred to accountants as a TCSP, or that only the TCSP was recorded in the case study despite the involvement of other intermediaries, which has been identified as a possible reporting issue throughout this project. In cases where an accounting professional was identified, almost half involved both accounting professionals and professionals from another intermediary sector (such as the legal and TCSP sectors); a small number involved multiple accounting professionals in one scheme.

135. All accounting professionals identified in the case studies were assessed as working on behalf of a direct client. This indicates that accounting professionals are

less likely to be approached by other intermediaries to fulfil a scheme designed to conceal beneficial ownership.

136. The expertise of accounting professionals means that most practitioners will be capable of identifying suspicious and high-risk activities conducted by their clients. As a result, accounting professionals are less susceptible to innocent and unwitting exploitation relative to legal professionals and TCSPs. Law enforcement agencies, FIUs, and other competent authorities have identified numerous instances in which accounting professionals have been complicit in criminality, or have orchestrated fraudulent investment or tax avoidance schemes. Analysis of the case studies identified that a significant majority of accounting professionals were complicit in their involvement, and over half were responsible for designing and promoting the scheme as a means of minimising their clients' taxation obligations.

Trust and Company Service Providers

137. In comparison to the legal and accounting sectors, the TCSP sector (excluding legal and accounting professionals who provide company formation and management services) is difficult to describe or quantify. The TCSP sector varies significantly across jurisdictions. In some countries, the TCSP sector is robust and well-established, exhibiting some of the characteristics of other highly regulated industry sectors, including government registration, professional body oversight, and AML/CFT regulation. In other countries, the role of TCSPs is less clearly defined, and government and industry oversight is less robust. Company formation and trust services are provided by a range of market participants from numerous sectors, including the finance, legal, and accounting sectors, as well as stand-alone service providers that specialise in these services, but that do not offer financial, legal, or accounting services.

138. The FATF standards defines *"trust and company services providers"* to include any service provider that carries out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- providing a registered office, business address or accommodation, correspondence, or administrative address for a company, a partnership or any other legal person or arrangement
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

139. Much of the literature available on TCSPs encapsulates all service providers who provide the above services, regardless of whether they represent their core

business or an ancillary service only. For the purposes of this report, the terms "TCSP" and "TCSP sector" exclude professionals operating in the legal and accounting sectors. Input provided to this report by the Group of International Finance Centre Supervisors (GIFCS) demonstrates that, in countries with a highly active and well-established TCSP sector, the market is dominated by a large number of small businesses with no significantly large players dominating the sector. A relatively small proportion of TCSPs operating in these jurisdictions are accounting or legal firms or subsidiaries of an accounting or legal firm.

140. As a sector, TCSPs are particularly well established and defined in low-tax jurisdictions, such as those that are members of GIFCS, where they play a far more active role in company establishment and management. The majority of GIFCS members require their TCSPs and underlying shareholder controllers and key persons (director, partner, Money Laundering Reporting Officer (MLRO), and compliance officer) to be fit and proper. In determining this, authorities consider integrity, competence (including mandatory requirements for key persons occupying executive roles in the TCSP to hold a relevant professional qualification and undertake continuous personal development) and financial soundness. Other GIFCS members strongly encourage key persons occupying executive roles to hold relevant qualifications. The requirement to hold a professional qualification does not generally apply to a shareholder controller unless they are occupying a director, manager or compliance role in the TCSP, although they would be subject to all other aspects of the aforementioned fit and proper test. These requirements mirror some of the requirements imposed on other professional intermediary sectors, such as the legal and accounting sectors, and could serve as a valuable model for professionalising the TCSP sector in countries where the sector is less clearly defined.

Role in the Establishment and Management of Legal Persons and Arrangements

141. Due to the varying nature of the international TCSP sector, the degree of involvement of TCSPs in the establishment of legal persons and arrangements differs across jurisdictions. In most countries, the role of TCSPs is limited to the incorporation and registration of a company or other legal person and does not extend to the provision of strategic business or financial advice. TCSPs were identified in over one-third of the case studies analysed for this report, and represented the largest proportion of professional intermediaries involved in the cases. TCSPs were also more likely to be involved in cases involving multiple professional intermediaries. However, it is likely that this number includes other professionals (legal and accounting) which have been referred to broadly as TCSPs.

142. TCSPs provide a low-cost means of engaging in international business sectors, often providing services to international clients or other international professional service providers on behalf of foreign nationals. While legal and accounting professionals also offer these services, the lower fees associated with TCSPs make them a useful resource for small to medium-sized businesses. In comparison to other sectors, the TCSP sector appears to exhibit a very low level of market globalisation, with most TCSPs providing services only in the country in which they operate. The majority of TCSPs involved in the case studies were

assessed as providing services to customers based in an overseas jurisdiction, and were involved in establishing legal persons and/or arrangements locally.

143. In addition to establishing legal persons and arrangements, some TCSPs offer complete company packages, which include company incorporation and registration, as well as bank accounts in the country of incorporation. More than half of TCSPs were assessed as having opened bank accounts on behalf of their clients, most of whom resided overseas. In these instances, TCSPs perform an intermediary service between the client and a financial institution, and will be responsible for facilitating CDD activities. Most TCSPs also offer trustee, protector, directorship, and virtual/registered office services, particularly in jurisdictions that require companies to appoint a domestic resident as a director. Almost all of the TCSPs identified in the case studies provided directorship, trustee, nominee, or virtual office services to their client.

144. In recent years, TCSPs have taken advantage of the online environment to offer services to clients virtually, without the need for face-to-face engagement. While some of these TCSPs require clients to meet with an intermediary in their country of residence to complete CDD obligations, many others rely only on documentation provided virtually by the client. The provision of online and virtual services makes the effectiveness of AML/CFT activities more challenging, in particular the ability for TCSPs to accurately perform CDD to identify the ultimate beneficial owner of the legal person or arrangement.

145. TCSPs are also commonly involved in the establishment or administration of legal persons and arrangements on behalf of other professional service providers, particularly those operating in another jurisdiction or on behalf of foreign clients. One-third of the case studies specifically referred to TCSPs providing services to other professional intermediaries (lawyers and accountants) on behalf of third-party clients. Furthermore, analysis of the cases identified that approximately half of the TCSPs involved were unwitting in their involvement. This suggests that the role of TCSPs is more likely to be transactional in nature, operating at the behest of a client or other intermediary, and that TCSPs are less likely to be the masterminds of schemes designed to obscure beneficial ownership. TCSPs that were assessed as having been complicit in their involvement were more likely to have been wilfully blind than fully complicit, or may have been wrongly classified as a TCSP.

Other Intermediaries

146. Due to its focus on legal persons and arrangements, this report has predominantly analysed the services offered by lawyers, accountants, and TCSPs; however, other intermediaries are also known to be involved in activities designed to obscure beneficial ownership. Law enforcement and private sector representatives reported the existence of "full service" real estate firms, which provide a full range of intermediary functions, including creating shell and shelf companies, providing corporate officers, closing transactions with lawyers, and identifying properties (price range, risk profiles, etc.). These firms reportedly work with developers to enable fraud where strong early sales are essential to generating additional financing. Detailed analysis of this phenomenon was not possible in this

report; however, real estate professionals who provide any of the services covered in section XI of this report would face similar vulnerabilities as other professional intermediaries.

147. In addition to the professional intermediaries listed above, FIUs and law enforcement authorities have identified other intermediaries who are not professional service providers, and who do not perform services as described in recommendation 22 of the FATF Standards, but who are nonetheless involved in assisting clients with the establishment of complex legal structures. These individuals, who are sometimes referred to as "business finders", are often responsible for finding other professional intermediaries capable of (and willing to) establish the legal persons and arrangements necessary to achieve their client's desired legal structure. Due to their role as an intermediary between a client and a third-party professional, they are not actively involved in the formation of a legal person, and are therefore outside of the regulated population as described under Recommendation 22 of the FATF standards.

148. The role of these "business finders" is not well understood. Law enforcement experience of these business finders relates principally to individuals who cater specifically to criminal clients – in other words, professional money laundering facilitators whose role in the establishment of legal structures is specifically designed to facilitate criminality. Whether business finders (excluding the professional intermediaries referenced above) play a role in legitimate corporate activities is unknown; however, experience indicates that it is unlikely or questionable at best. Of the case studies analysed for this report, approximately 20% were assessed as having involved a professional money launderer who performed tasks similar to a professional intermediary (see Case Study 38 for one particular example).

149. This report has not sought to assess the vulnerabilities of these other intermediaries due to the lack of available information; however, it is assessed that these *non-professional* intermediaries pose a vulnerability to other professional intermediaries who may be engaged by them to perform services on behalf of a client. This vulnerability is heightened in national systems where such non-professional intermediaries have the ability to create legal persons and arrangements without the involvement of a professional intermediary.

OVERVIEW OF VULNERABILITIES

150. This section provides an overview of the vulnerabilities associated with the practices and services offered by professional intermediaries which are commonly exploited by criminals to conceal beneficial ownership. The vulnerabilities assessed in this section have been drawn from the case studies analysed for this report and from the experiences of FIUs, law enforcement agencies, and regulatory authorities. The key vulnerabilities that are assessed in this section are:

- establishing legal persons and arrangements
- establishing and selling shelf companies
- providing directorship, trustee, virtual office, and mailbox services
- facilitating transactions through trust accounts or client accounts
- facilitating the purchase or sale of real property
- client advocacy and brokerage services
- providing services to clients and intermediaries domiciled internationally
- providing advice on tax compliance and tax minimisation
- legal professional privilege and client confidentiality
- limited AML/CFT obligations or insufficient awareness and compliance.

151. The list of vulnerabilities assessed in this report is not intended to be exhaustive, and represents the more commonly exploited vulnerabilities exhibited by professional intermediaries.

Establishing legal persons and arrangements

152. It is common practice for professional intermediaries to advise clients on company formation, corporate structures, and asset management. The purpose of this advice will often centre on protecting wealth and assets from high-risk business activities, and minimising taxation obligations to the greatest extent lawfully possible. These services are particularly attractive to criminals, who are known to actively seek the advice of complicit and unwitting professionals to protect illicit assets and evade taxation obligations through the concealment of beneficial ownership.

153. Some countries require legal professionals (principally notaries) to incorporate and register companies. However, many jurisdictions do not have such a requirement, and companies can be established by engaging directly with the relevant public authority. In countries where legal representation is not necessary, professional intermediaries are often employed to:

- provide expert advice on the most appropriate company structure to meet the needs of the client

- explain and/or facilitate the process, which can be confusing for most small to medium business owners
- enhance respectability and perceptions of legitimacy and trustworthiness.

154. The case example (Case Study 100) below demonstrates how the services of a legal professional were exploited to enhance the apparent legitimacy of a corporate structure used to facilitate a loan-fraud pyramid scheme. In this case, the legal representative was likely to have been complicit.

155. As a result of their expertise and role in the establishment of companies and other legal persons, professional intermediaries are vulnerable to being involved, knowingly or unwittingly, in facilitating complex money laundering schemes. The majority of cases that involved companies and other legal persons were facilitated by a professional intermediary. Professional service providers who offer company establishment services in major global trade and finance hubs are vulnerable to exploitation from international clients or professionals seeking company establishment services in that country.

156. Professional service providers will often be involved in the establishment of trusts and other legal arrangements due to the legal nature of the contracts between settlor, trustee, and beneficiary. Of the cases that involved legal arrangements, almost all involved professional intermediaries. Noting the manner in which trusts can be established using legal persons as trustees in place of a natural person, it is possible for trust arrangements to be established in such a way that the professional service provider never engages directly with the ultimate beneficial owner of the assets held in trust. This, in conjunction with strict confidentiality laws that can be applied to trust arrangements[52], makes professional service providers who offer trust establishment services vulnerable to exploitation for the purpose of disguising the beneficial ownership information of laundered proceeds of crime.

Case Study 100 – United States
In this case, an individual organised a loan-fraud pyramid scheme to falsely inflate the sales and revenues of his company. His company served as a front to generate loans. The scheme involved his wife and son. The defendants created numerous legal entities, including trusts, corporations, and LLCs to open bank accounts to manage the illicit funds and conceal the ownership and involvement in the scheme. The defendants used the help of a legal professional (attorney) to create a number of legal entities, and diverted loans for the company for private benefit, including gems and jewellery. The attorney also set up trusts on behalf of the individual and their family, and helped to sell jewellery held in those trusts. The individual provided false documents purporting to show that the jewellery was a gift of deed into the trust. The trusts provided an air of legitimacy and a cover story to explain the

[52] Van der Does de Willebois, E. et al., 2011: p. 168.

fraud, and as a result, USD 2.8 million from the sale of the jewellery was wired into the trust's brokerage account. Subsequently, USD 200 000 was later moved from the trust checking account into an account opened for a different trust. This transfer was facilitated using the address of the attorney, who was by this time deceased.

Establishing and selling shelf companies

157. Professional intermediaries, such as corporate law practices and TCSPs, will occasionally establish and hold shelf companies in anticipation of a future need. In these instances, the professional intermediary or its employees are recorded as nominee directors or shareholders of the company. While the ease and speed with which companies can be incorporated has, to a large degree, limited the need for legal and accounting professionals to establish and hold shelf companies for future use, TCSPs continue to sell shelf companies. This is particularly true for online TCSPs and TCSPs in major international finance and business hubs. The simplicity associated with purchasing an established shelf company suits virtual transactions and small- to medium-sized business clients with less complex corporate and financial structures. However, shelf companies can be used for any purpose, and can form part of large and complex business structures.

158. In addition to offering readymade legal persons, many TCSPs will establish bank accounts registered to the shelf company, which are retained by the shelf company following its sale. This practice can complicate CDD activities performed by the financial institutions. Approximately one-third of professional intermediaries identified in the case studies were assessed as opening bank accounts on behalf of their clients, most of whom were located in a foreign jurisdiction.

159. The case study below demonstrates how criminals specifically targeted shelf companies to facilitate their fraudulent scheme. It is likely that the corporate history of the shelf companies was desired by the criminal to lend legitimacy to the fraud, which may have been diminished if newly created companies had been used. The case also demonstrates the manner in which the shelf companies were sold by nominee directors along with pre-established bank accounts.

Case Study 104 – United States

The defendants engineered a conspiracy to sell fraudulent renewable energy credits through the use of shell and shelf companies in the US in order to fraudulently receive renewable energy tax credits from the US government for renewable fuels never produced, and to launder those illicit proceeds for their own benefit. Among their ill-gotten gains from these proceeds were real estate, boats, cars, watches, and gold. During the course of their investigation, law enforcement determined that the defendant directed a network of his professional contacts to purchase shelf companies throughout the US, to serve as purported purchasers of renewable fuel and purported sellers of feedstock. The use of shelf companies was discovered by interviewing the

nominees who had opened bank accounts on behalf of those companies and through search warrants executed on a number of the businesses.

Directorship, trustee, virtual office, and mailbox services

160. In addition to establishing legal persons on behalf of clients, many professional service providers, particularly TCSPs, offer directorship, virtual office and mailbox services. These services allow the legal person to maintain a physical footprint in a country, and can distance the legal person from other assets and activities controlled by the beneficial owner. As a result, these services are vulnerable to exploitation for the purpose of disguising the true controllers and beneficial owners of a legal person, its assets, and its transactions. Nominee directors and virtual offices are common features in many complex legal structures that FIUs and other competent authorities have identified as being involved in money laundering, tax evasion, investment fraud, and other criminality. Analysis of the case studies used for this report identified that approximately half of the professional intermediaries provided directorship services to their clients. TCSPs represented the large majority of intermediaries involved in the provision of these services, and were often assessed as providing services to other professional intermediaries on behalf of third-party clients.

161. Nominee directors can be formal or informal, and criminals have been known to recruit people with no criminal history to perform these roles, or who agree for their details to be recorded in these positions. Instances of identity theft for the purposes of filling nominee director roles have also been identified; however, these activities pose a risk to criminal groups, and professional service providers that offer these services are an attractive and low-risk alternative.

162. By providing directorship and virtual office services, professional intermediaries may unwittingly facilitate money laundering services and deal in the proceeds and instruments of crime. Even in instances where the professional service provider does not take an active role in the company, which is often the case, the nominee director is at risk of prosecution or other penalty as a result of crimes performed by the legal entity. A majority of professional intermediaries who provided directorship services in the case studies were assessed as being unwittingly involved.

163. Some countries require legal persons to maintain an active presence in the country where they are registered. This is generally achieved through a requirement for a resident of the country to be appointed as a director of the company, or for the company to maintain a physical presence in the country, or both. Professionals operating within these jurisdictions, that offer directorship and virtual office services will be more vulnerable to exploitation from overseas clients than those operating in countries without these requirements. A large majority of professional intermediaries who provided directorship services in the assessed cases were providing services to clients based overseas. One case study (Case Study 78), included below, demonstrates how a foreign client of a TCSP appointed a domestic-based national as a nominee director to meet the country's requirements to have a

resident as director. The nominee director had little knowledge of the activities of the companies.

164. In addition to offering directorship and nominee services, some professional service providers offer **trustee services** to domestic and international clients for trusts established under domestic law. In some countries, professional rules prohibit legal professionals from acting as a trustee. In these countries, the role of the legal profession would be limited to providing professional advice on the contract that underpins the trust arrangement.

165. In most countries trustees are not required to register the existence of, or beneficiary of, a trust arrangement, while in other countries they are expressly prohibited from doing so under law. Trustees are also required to act on behalf of the interests of the beneficiaries. This means that, when dealing with matters relating to the trust, they must consider the interests of the beneficiary over their own.

166. Professional service providers who offer trustee services are at risk of becoming the effective legal owner of criminal assets[53], and of dealing with the proceeds of crime. Only strict due diligence measures, for the settlor, the beneficiary, and the asset in trust, can assist professionals in avoiding this form of exploitation.

Case Study 78 – New Zealand

A New Zealand law firm was linked to clients who had been implicated, arrested or convicted of a myriad of offences including embezzlement, bribery, corruption, tax evasion, and money laundering. This law firm set up its business basis in New Zealand, and worked for overseas clients using its in-depth knowledge of New Zealand tax, trust and company law.

The companies and partnerships were set up by this New Zealand law firm, who routinely used its employees as nominee directors and shareholders, with the beneficial owners (who were sometimes offenders and their associates) not publicly named. Furthermore, often a chain of companies was established, with one company the shareholder of another, which was the shareholder of another, which added complexity to the structure, and further removed the beneficial owner from the assets. Sometimes a New Zealand (shell) company was used as a trustee of the trust.

The companies involved were usually all shell companies with nominee directors, shareholders, and addresses. The companies, partnerships and trusts comprised the complex structures established by this New Zealand law firm, which can be used to hide and protect wealth. Furthermore, sometimes entities were set up

[53] In a trust, the title of assets stands in the name of the trustee (or in the name of a person acting on behalf of the trustee), although they constitute a separate fund and are not part of the trustee's own estate (see Article 2 of the Hague Convention).

internationally by this New Zealand law firm's business associates in other countries, which were added to the structures, further increasing the complexity and decreasing the ability and efficiency of detecting crime and hidden wealth. If suspicions did arise and a person with such a structure was investigated, there was a convoluted audit trail that would have been arduous to trace. There were strong indications that criminals have had structures set up by this New Zealand law firm with evidence that some of these structures have been used by criminals to hide assets.

A NZ-based employee was also named as a director to satisfy the legal requirement to have a New Zealand resident director and address; however, the beneficial owner of the company was not identified in every instance.

Facilitating transactions through trust accounts or client accounts

167. Professional service providers, particularly law firms and larger accounting firms, often maintain and operate a trust account to facilitate financial transactions on behalf of clients, hold funds in escrow, or receive payment for services rendered. In most countries, these trust accounts are highly regulated to prevent misappropriation of client funds; however, this oversight often falls short of AML/CFT considerations, and professional trust accounts continue to pose a money laundering vulnerability globally.

168. It is not uncommon for some professionals to facilitate transactions, including cash transactions, on behalf of their client. Analysis of the case studies identified where this had occurred. This service is attractive to criminals seeking to obscure the beneficiary of cash transactions, as it places the burden of integrating the cash into the regulated finance sector on the legal professional (via the law firm's trust or client account). This has the dual effect of:

- leveraging the credibility and reputation of the legal profession to reduce any potential suspicion associated with the cash deposit
- distancing the client and any associates or third parties from the AML/CFT controls of the financial sector.

169. Furthermore, the involvement of an intermediary in a financial transaction between two parties can disrupt a chain of transactions and obscure the relationship between the two parties. As a result, it can be difficult to ascertain the beneficial owner of funds that are transferred through trust or client accounts, especially if the transaction involves a clustering or structuring of transactions, or the transaction occurs over a protracted period of time. This vulnerability is increased when a lawyer allows funds to be placed in the firm's trust or client account when no legal services are performed or expected to be performed. The cases below demonstrate how the trust accounts of law firms and accounting practices were used to achieve this aim.

Case Study 102 – United States

Individual 1, a U.S. citizen and resident of Belize, incorporated more than 5 000 shell companies in Belize and the West Indies to facilitate numerous securities and tax fraud schemes. Individual 2, a dual U.S. and Canadian citizen, was the secret owner of an international broker-dealer and investment management company based in Panama City, Panama, and Belize City, Belize. There were 3 interrelated schemes: 1) fraudulent stock promotion and price manipulation; 2) circumventing capital gains taxes under the Foreign Account Tax Compliance Act (FATCA); 3) laundering more than USD 250 million in profits through unidentifiable debit cards and attorney escrow accounts.

Individual 2 used the services of a US-based lawyer to launder the more than USD 250 million generated through his stock manipulation of a number of U.S. companies – directing the fraud proceeds to five law firm accounts and transmitting them back to members of the scheme and its co-conspirators. These concealment schemes also enabled Individual 2 to evade reporting requirements to tax authorities.

Case Study 3 – Australia

Managers at a university and directors of construction companies were complicit in a fraudulent invoice scheme. The managers approved inflated invoices for maintenance work to be carried out by the construction companies, as well as invoices for work that was never undertaken. The profits from the fraud were used to purchase racehorses and property. The managers at the university were repaid with kickbacks or direct shares in racehorses. Accounting firms, which were undertaking international transfers on behalf of the suspects, sent money to many countries, including New Zealand, Canada, Hong Kong and the US. A large proportion of the funds were sent to companies linked to the horse racing industry. The accounting firms also received international transfers from various overseas entities that were similar in value to the amounts the firms had sent overseas initially. The majority of these transfers originated from Hong Kong. The authorities suspected that the accounting firms were laundering the funds on behalf of the suspects as part of a professional money laundering syndicate.

Facilitating the purchase or sale of real property

170. Real estate property is a highly attractive medium for laundering the proceeds of crime. Unlike other high-value assets, the real estate market in most countries has demonstrated a strong resilience to economic fluctuations, and has generally appreciated in value in most high-density cities. Real estate generally represents a relatively safe medium for storing illicit wealth, and the sale of the asset offers a legitimate rationale for the receipt of large volumes of wealth. Furthermore, the purchase of real estate property offers a convenient and legitimate excuse for acquiring mortgage loans, including from private lenders, and for the receipt of

regular and ongoing payments in the guise of rental income. Both of these are common money laundering methods (refer to Section 2 for further analysis on the use of false loans to obscure beneficial ownership). Approximately one-third of the case studies analysed for this report involved the acquisition of real estate, and most of these cases involved the use of a professional intermediary to execute the purchase.

171. In some jurisdictions, legal professionals are required to facilitate real estate transactions. In countries where legal representation is not required by law, it is common practice for professional service providers to be employed to assist in the conveyancing of the property as a precaution due to the high value of the asset. As a result, professionals will often be responsible for identifying and reporting the vendor and/or purchaser of the land and property titles to relevant government authorities. This makes the professional intermediary vulnerable to exploitation by individuals seeking to disguise the beneficial owner of the real estate asset. Cases analysed for this report demonstrated the following methods used to conceal the beneficial owner of real estate assets:

- purchase of assets through intermediaries, such as companies, trusts, family members, associates, or other complicit third parties who have no criminal record (Case Study 2)
- use of a false name or fraudulent identification information (Case Study 101).

172. In some instances, the beneficial owner of the real estate asset will not be involved in its purchase at all, and will instead direct a third party to make the purchase. This method is difficult to detect, and requires the professional intermediary to be vigilant and aware of their ML/TF risks in order for them to detect the activity. One Australian case study (Case Study 2) demonstrates how an individual suspect to an investigation purchased a property in the name of a family member and used the proceeds of crime to pay down a mortgage loan. The solicitor involved provided conveyancing services in relation to the property, and was thereby responsible for registering the purchase with the relevant government authorities. Furthermore, the solicitor acted as an intermediary for loan repayments, which further distanced the beneficial owner from the asset and associated loan.

Case Study 2 – Australia
An Australian drug syndicate used multiple money laundering methods to launder more than AUD1 million worth of proceeds of crime. One method involved a syndicate member purchasing a property worth more than AUD700 000 in a family member's name. The property purchase was financed using a mortgage. Over a two-month period the syndicate member paid more than AUD320 000 in 16 cash deposits to their solicitor (who provided conveyancing services and acted on behalf of the syndicate member in the transaction) to pay off the mortgage on the property. These cash payments were the proceeds of crime.

Client advocacy and brokerage services

173. In addition to providing business advice to clients and facilitating the formation of legal persons and arrangements, professionals will often offer client advocacy and brokerage services. This can include introducing clients to banks and other financial service providers, and opening accounts and seeking loans on their clients' behalf. As a result, the professional becomes an intermediary between the client and the regulated finance sector, and takes on the responsibility of providing banks with the requisite information to meet their CDD obligations. Analysis of the case studies used in this report identified that, in these particular examples, many professional intermediaries facilitated the establishment of banking relationships on behalf of their clients.

174. In countries where financial institutions are permitted to rely on third parties to perform CDD on the customer[54], professional intermediaries are vulnerable to exploitation for the purposes of disguising beneficial ownership and control. While the ultimate responsibility for conducting CDD should remain with a financial institution during a third-party reliance arrangement, criminals will still seek to use the reputation of professional intermediaries to convince the financial institution of the legitimacy of a false or misleading identity or ownership and control structure. One US case study (Case Study 101 below) demonstrates how a complicit professional used their role as a professional intermediary to frustrate and overcome the CDD activities of financial institutions to attain fraudulent loans.

175. Occasionally, professional service providers maintain some level of control over some or all of their clients' banking accounts. This allows them to manage the financial affairs of their clients in a timely manner, perform accurate bookkeeping, and facilitate transactions on their clients' behalf. To achieve this, professionals are listed as signatories to their clients' accounts, thereby allowing them to act in their clients' interests, but without their clients' direct involvement. This is standard practice for in-house accountants and lawyers (those who work solely for a company or public sector authority), but also occurs when professionals service a number of small to medium-sized businesses as an outsourced professional on an ongoing and regular basis. It is not common for professionals who offer only occasional services to a client to maintain control over the clients' accounts.

176. Managing a client's accounts places the professional at a heightened risk of facilitating money laundering or terrorism financing; however, the service presents a lower risk of obscuring beneficial ownership, provided the transaction is not conducted through an account opened in the name of the professional or their firm and appropriate CDD measures are conducted by the professional and subsequently by the financial institution.

177. In addition to introducing clients to financial institutions, professional service providers will, when necessary, introduce their client to other professional service providers, including other lawyers, accountants, TCSPs, real estate agents,

54 See Recommendation 17 of the FATF Standards.

mortgage brokers and financial advisers. Occasionally, the professional will act on their client's behalf and seek specialist advice or services for their client. This is especially true for those legal professionals who have professional relationships with professionals in other countries. This poses the same risks as those associated with being a client advocate or intermediary. Analysis of the case studies identified that a number of professional intermediaries performed services for another intermediary on behalf of a third-party client.

178. Professionals who receive facilitation requests from international professionals working on behalf of international clients are at a heightened risk of facilitating money laundering and obscuring beneficial ownership information due to the challenges associated with properly verifying the identity and motives of the client and beneficial owner. One Israeli case study (Case Study 39 below) demonstrates how law firms contacted foreign TCSPs to establish companies and bank accounts on behalf of local clients. In this case, the CDD activities of the foreign bank, and the TCSP, would have been inhibited by the numerous layers of professional intermediaries between the client and end service provider and increased the likelihood of incorrectly identifying the true beneficial owner.

179. Furthermore, an unwitting professional may not be in a position to judge the complicity of a corrupt international professional, and may naively trust the legitimacy of the request based on their own professional ethics and morality. This may place them at risk of unwittingly committing a domestic crime on behalf of an international criminal syndicate and may compromise their domestic reputation and professional standing.

Case Study 39 – Israel
This scheme was used to hide the proceeds of fraud conducted through foreign exchange and binary options trades. Local companies attracted foreign investors and presented themselves as legitimate foreign exchange and binary trading platforms. Private companies, Israeli representatives of foreign banks and law firms set up foreign companies abroad by contacting TCSPs located in international jurisdictions. The latter established shell companies in the international jurisdictions. The service provided by the foreign TCSPs also included opening bank accounts in favour of the shell companies in other countries. After the companies were established, the TCSPs were not involved in their management nor in any related activity. In some cases, the suspects used the companies as a vehicle to launder money and in other cases they sold the companies to third parties for a profit.

Case Study 101 – United States
The defendant operated a mortgage broker business and several other companies that owned and managed real estate. He used nominee accounts, shell corporations and other schemes to conceal his ownership. The scheme involved

the purchase of properties owned by entities that the defendant controlled through an employee. The purchases were financed through loans. In connection with the loan applications, the defendant and others submitted fraudulent information related to the financial position of the borrower/purchaser, fraudulent appraisals that overstated the value of the collateral, and other documents that contained other material misrepresentations. The subject would "sell" commercial property owned by an entity he controlled to another entity that he controlled at highly elevated prices. The purchases were financed through fraudulent loan applications and through the submission of fraudulent documents. Also, the defendant altered invoices directed to one of the entities by inflating the cost of the work listed on the original invoices to make it falsely appear as though improvements had been made to the properties serving as collateral for the loans.

Providing services to clients and intermediaries domiciled internationally

180. Professional service providers are vulnerable to exploitation from clients and intermediaries domiciled internationally. As most professionals specialise in establishing and managing legal persons and arrangements within their own country of operation, it is common for international clients and intermediaries to seek their services to facilitate activities in that country. Analysis of the case studies identified that the majority of professional intermediaries were providing services to clients based in another country. In some cases, the relationship between a professional service provider and an international client will be short-term and transactional in nature; however, some professionals, particularly TCSPs, will provide ongoing company and trust management services, particularly if domestic laws require resident directors or trustees. The majority of professional intermediaries who provided services to clients based overseas were also providing directorship, trustee, nominee, or virtual office services.

181. Due to the transnational nature of these customer relationships, professionals that service international clients are vulnerable to deception and fraud perpetrated by criminal clients, complicit foreign professionals, or unwitting intermediaries. This vulnerability is common to all service providers that interact with international clients, and professional intermediaries and financial institutions require sophisticated CDD capabilities to accurately identify beneficial ownership, particularly in the absence of face-to-face engagement with clients. Most professional intermediaries who provided services to clients based overseas were assessed as being unwittingly or negligently involved in the scheme. One Panamanian case study (Case Study 85 below) demonstrates how a smaller TCSP failed to conduct enhanced due diligence on their overseas client and relied on the due diligence performed by the financial institution that referred the customer to them. The trust, managed by the TCSP, was used to collect the proceeds of corruption and illicit enrichment.

182. Criminals will seek to use the services of professionals with domestic and international contacts and associates in order to facilitate international business activity, including the establishment of companies and bank accounts in other countries. Some professionals, particularly in countries that apply strict regulations

to DNFBP sectors, have developed international networks of trusted intermediaries on whom they rely for CDD activities. Although these measures are likely to mitigate some of the vulnerabilities associated with transnational client relationships, they rely on the trusted intermediary having the capabilities necessary to perform accurate CDD to discover the ultimate beneficial owner, and remaining honest throughout the transaction (i.e. not being complicit or wilfully negligent when dealing with suspicious clients). As the professional only has limited control or oversight of the activities of their trusted intermediaries, and retains the risk associated with their activities, the vulnerability to the professional remains.[55]

183. One Guernsey case study (Case Study 36 below) demonstrates how a Guernsey TCSP was exploited by a foreign client to administer a company used to facilitate market manipulation. Over the five-year period of their involvement, the TCSP was unaware of the fraudulent nature of the business' operations, and had not raised any suspicious matters with Guernsey authorities.

Case Study 36 – Guernsey
During a two-year investigation (2014-2016), the US Commodity Futures Trading Commission (CFTC) launched an investigation into UK national Mr. X Doe for market manipulation. It came to the attention of Guernsey Financial Services Commission that a TCSP provider (TCSP B) administered a corporate structure for the benefit of Mr. X Doe. Over a five-year-period Mr. X Doe made approximately GBP 32 million (British pounds). The purported legitimate business was futures dealing. Prior to Guernsey TCSP B's involvement, it was administered by a Cayman Island Company. The Guernsey TCSP, which was licensed for AML/CFT, identified that Mr. X Doe was under investigation and co-operated with the Guernsey AML/CFT authorities.

Case Study 85 – Panama
The purported legitimate purpose of the scheme was the development and construction of real estate, based on small investors who injected capital. The funds provided by the settlor or third-party adherents were derived from illegal activities (corruption of public servants and illicit enrichment). The scheme involved a BVI company with nominee directors, ultimately controlled by a PEP, who was a client of a bank that had a relationship with the TCSP. The TCSP set up a real estate trust to receive money and assets that come from the business of the settlor and "investors." The assets received were invested in a real estate project, with the same assets given as a warranty to the bank that was financing 60% of the real estate project. The ultimate beneficial owner of the real estate project was the son of the PEP.

[55] See also Recommendation 22 (FATF, 2012a)

The trustee did not conduct extensive due diligence and relied on the due diligence performed by the bank that referred the client, since both the client and the trustee maintained a business relationship with the bank.

Providing advice on tax compliance

184. A key role of many professional service providers, particularly accounting and legal professionals, is to provide advice to individuals and businesses on how to maximise profits and minimise costs. This often includes advising clients on lawful means of minimising their taxable liabilities.

185. This service and professional expertise in this area is vulnerable to exploitation from individuals and legal persons seeking to disguise beneficial ownership to avoid taxation obligations - otherwise referred to as revenue and taxation fraud or tax evasion. However, due to their knowledge of tax law, the risk of innocently or unwittingly providing advice on, or facilitating of tax evasion schemes is reduced.

186. The experiences of law enforcement agencies, FIUs, and other competent authorities have identified a high level of involvement from professionals in tax evasion schemes. These schemes have often involved complex transnational company structures, fraudulent trade and false invoicing, and *phoenixing activities* to disguise beneficial ownership of assets and income. Many case studies involved tax evasion as a predicate offence, most of which involved professional intermediaries – principally legal or accounting professionals – the majority of whom were assessed as being complicit in their involvement. Criminals actively target complicit professionals to assist with tax evasion, and are willing to pay lucrative fees as motivation for their complicity.

187. Furthermore, almost all complicit intermediaries involved in tax evasion cases were also assessed as being the designer and/or promoter of the scheme. In situations where the professional intermediary has designed and promoted an illegal tax minimisation scheme to prospective clients, it is possible that the beneficial owner will not be aware of the illegality of the scheme. This poses a significant vulnerability to unwitting beneficial owners as well as the broader reputation of professional services sectors. While no cases specifically identified the involvement of unwitting beneficial owners, a number of cases focused on the corrupt activities of professional service providers themselves, rather than their clients (the beneficial owners). The Australian case study below demonstrates how a complicit accountant exploited their knowledge of tax laws in multiple jurisdictions to facilitate tax evasion on behalf of their clients.

Case Study 5 – Australia

This "round robin" scheme aimed to make funds movements appear as payments to other parties while, in reality, the funds ultimately returned to the original beneficiary. The suspects transferred funds from their companies' accounts to the bank accounts of companies in New Zealand. The New Zealand companies

and bank accounts were controlled by a Vanuatu-based accountant, who was a signatory to the bank accounts. The payments were falsely described in the companies' records as "management and consultancy fees," with false invoices that matched amounts paid to the New Zealand bank accounts. No evidence was available to show that any consulting work had been carried out. The false expense payments were claimed as deductible expenses in the tax returns of companies X, Y and Z, thereby fraudulently reducing the companies' taxable income and taxes owed. The accountant then transferred the funds under the guise of international "loans" through a series of round-robin international transactions, through accounts held in the name of companies owned and operated by the accountant. The accountant transferred the funds into the personal bank accounts of the suspects in Australia. The funds were transferred via an overseas company controlled by the accountant, separate to the companies in New Zealand that received the funds originally. In order to disguise the funds being transferred back into Australia as loans, false documents were created purporting to be international loan agreements with a foreign lender, which are not assessed as income and have no tax liability.

Legal professional privilege and client confidentiality

188. Legal professionals are subject to a range of ethical obligations, which differ from country to country, but which generally adhere to a core set of professional rules. These include: independence from the State; acting with honesty, integrity and fairness; duty to act in the client's interest; and the maintenance of client confidentiality and legal professional privilege (LPP).[56] These ethical obligations are aimed at ensuring fair and equitable access to justice, and ensuring probity and integrity across the profession. Some law societies and regulatory bodies consider that these codes of conduct and professional rules prevent legal professionals from being knowingly involved in money laundering or terrorism financing; however, some of these obligations can be vulnerable to criminal exploitation. FIUs and other competent authorities have reported the use of LPP and client confidentiality to protect the disclosure of the identity of the beneficial owner of assets, which frustrates criminal investigations.

189. LPP generally does not extend to all communications between a lawyer and their client, and often stops short of commercial advice (although this can differ between countries). Communications that do not meet the relevant national definition of LPP (if available) are considered to be protected by legal confidentiality, which is not absolute and is limited in certain key areas.

190. LPP and client confidentiality play an important role in the legal system; however, the initial application of these protections often rests with the legal professional rather than an independent third party. Subsequently, there is no clear and consistent interpretation or application of these protections amongst legal professionals, despite case law and the release of guidance and interpretive notes by

[56] International Bar Association. (2011). IBA International Principles on Conduct for the Legal Profession.

regulatory bodies. Furthermore, LPP is considered to belong to the client, and can only be waived at the direction of the client or if the legal professional is being used to commit a criminal offence. It is an offence in many countries for a legal professional to breach LPP, often punishable by professional sanctions or a criminal charge. Due to varying interpretations, the protections afforded to LPP, and the significant personal and professional consequences for breaching LPP, legal professionals can take a conservative approach to the application of LPP.

191. LPP and client confidentiality can be exploited by complicit legal professionals who are seeking to delay an investigation. However, the general caution with which legal professionals deal with LPP means that any legal professional can unwittingly conceal criminality using it. The case study below involves a Dutch investigation into the activities of a TCSP and civil-law notary involved in establishing structures designed by an international law firm known to be involved in the establishment of structures designed to obscure beneficial ownership. Multiple legal professionals from numerous countries were involved in the establishment of these structures, and have asserted privilege in order to delay or frustrate the investigation. Dutch authorities were required to verify the rights of these legal professionals via mutual legal assistance requests, which can be a time-consuming process.

192. Law enforcement agencies and FIUs have reported that LPP is regularly exploited by complicit legal professionals to frustrate and hinder investigations. Due to the nature of LPP, claims of privilege need to be reviewed prior to being overturned, even if the grounds for LPP are questionable from the beginning. Regardless of the rules associated with LPP in most countries, the subjective nature of LPP will continue to pose a challenge. Other challenges associated with LPP and gathering evidence in relation to legal professionals have previously been reported by the FATF[57]. These challenges may explain a lower proportion of case studies involving legal professionals submitted for this report, and the lack of evidence of complicity cited in those case studies.

193. During the consultation phase with key private sector stakeholders, some private sector representatives highlighted that LPP training offered to legal professionals can often be inadequate unless the legal professional specialises in litigation where LPP is frequently considered. It is likely that legal professionals involved in tax, private client, corporate, or estate planning matters may rarely be required to consider or employ LPP. It has been suggested that the low level of training, coupled with a lack of practical application by some lawyers, leads to the development of broad and conservative approaches to LPP. Enhanced training and guidance in this area may assist to reduce this vulnerability over time.

[57] Obtaining records held by DNFBPs, the uncertainty of the scope of privilege, difficult and time-consuming processes for seizing legal documents, and a lack of access to client account information can present challenges in the evidence-gathering process. Law enforcement agencies are required by law to have strong evidence from the outset to demonstrate that LPP/secrecy should be removed. Claims of LPP could impede and delay the investigation (FATF, 2013: pp. 30–33).

194. While client confidentiality is a common principle among accounting professionals, it generally does not prohibit the disclosure of information that is permitted to be, or required to be, disclosed under law. As a result, it is less vulnerable to exploitation. However, in some countries, accounting professionals afford their clients LPP, or a form of privilege that closely resembles LPP. Additionally, some accounting professionals also hold legal qualifications, and operate as solicitors in law firms to provide expert advice on taxation and company law. Accounting professionals working at the behest of lawyers may also be subject to LPP. Accounting professionals who are subject to LPP obligations face similar vulnerabilities as their counterparts in the legal sector.

Case Study 71 – Netherlands
A criminal investigation into a Dutch TCSP was instigated on account of the systematic failure to notify unusual transactions and money laundering. This was presumed to involve the facilitation of fake transactions on behalf of foreign clients to ensure, for example, the assets or property of those clients were scarcely taxed, or funds parked were transferred by means of fake transactions to another jurisdiction. This was carried out by means of complicated well-considered structures with companies and trusts in various countries for which instructions were given by a financial service provider and were also discussed in this way by the suspect with the Dutch civil-law notary. Dutch entities were part of these complicated structures. The same applied for the Dutch foundations registered at an international address. The structure sometimes consisted of eight different entities, in various countries. The suspect reportedly did not know in several cases the identity of the actual beneficiaries of the companies that he incorporated.

Limited AML/CFT obligations or insufficient awareness and compliance

195. Internationally, there has generally been an increase in the effective application of risk-based measures by financial institutions to prevent ML and TF[58]. As a result, the risk of detection for those seeking to exploit financial institutions for ML and TF purposes has increased. In contrast, the implementation of AML/CFT obligations to DNFBPs has been slower, with many jurisdictions yet to fully implement Recommendations 22 and 23[59].

196. FIUs, law enforcement agencies, and other competent authorities report that the primary environmental vulnerability that continues to effect the concealment of beneficial ownership is the lack of regulatory obligations to collect, disclose, and make available information regarding beneficial ownership across the globe.

[58] See the outcomes of the latest round of Mutual Evaluation Reports conducted by the FATF available at www.fatf-gafi.org.

[59] *Ibid.*

197. One of the most significant findings of the FATF's Horizontal Study is that 17% of jurisdictions that responded do not impose any AML obligations or AML supervision on professional intermediaries whatsoever, despite this being a requirement of FATF Recommendations 22, 23 and 28. In some cases, this is partly the result of resistance to regulation from the relevant sectors or professions (e.g. these groups work to prevent the enactment of laws or regulations which would impose such obligations or to mount constitutional challenges to such laws once passed). In other cases, it may represent an "unfinished" aspect of the AML/CFT system which has not yet been implemented. See Section 4 for further analysis of jurisdictional vulnerabilities associated with the lack of AML/CFT obligations for DNFBPs.

198. Combatting ML and TF requires an awareness of established and emerging ML/TF risks and typologies. Professionals who are not subject to AML/CFT obligations are more vulnerable to ML/TF exploitation than their regulated counterparts in other countries due to the lower level of awareness and understanding of ML/TF threats.[60] Analysis of the case studies identified that less than 10% of intermediaries involved in these schemes identified and reported a suspicious matter to a supervisory body. All of these cases were from countries that regulate DNFBPs, suggesting that the effectiveness of supervision of DNFBPs in the countries where they are regulated needs improvement.

199. In many countries, the authority to submit a suspicious transaction report is limited to businesses and professional service providers who are expressly regulated under that country's AML/CFT legislation. In these instances, the inability for unregulated professionals to voluntarily report a suspicious matter to the FIU or self-regulating body (SRB)[61] is an additional vulnerability, as it may limit how an unregulated professional can respond to a suspicious request.

200. The vulnerability posed by reduced AML/CFT obligations is greater for small professional firms and firms that do not operate in international markets. Larger multinational firms are more likely to be attuned to money laundering vulnerabilities and may have robust AML/CFT measures in place, particularly if they are subject to AML/CFT regulation in one or more of their countries of operation.

201. In countries where AML/CFT legislation has been applied to DNFBPs, FIUs and supervisory bodies have expressed concern regarding the standard of compliance exhibited by the sector, and the level of reporting, which sometimes appears low in comparison to the size and activities of the sector. One Dutch case

60 ACC, 2015: p. 83.

61 A self-regulatory body is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals, or accountants), and which is made up of members from the profession. It also plays a role in regulating the persons that are qualified to enter and who practice in the profession, and performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practicing in the profession. See, in particular, Question 5 of the Horizontal Study at Annex B.

study (Case Study 71 above) provides an example of systematic non-compliance by a Dutch TCSP, which was exploited by foreign clients to facilitate tax evasion. Whether the level of compliance exhibited by legal professionals in some countries is indicative of an unwillingness to comply, or a limited understanding of their AML/CFT risks, has not been assessed. However, compliance and awareness of AML/CFT risks within some professions is considered by FIUs and other competent authorities to be a vulnerability[62]. Another Dutch case study (Case Study 66 below) demonstrate how a lack of awareness of ML and TF risks amongst professional service providers facilitated money laundering and other criminality. In both cases, professionals involved in managing companies and promoting investment schemes on behalf of their clients failed to identify indicators of criminality or conduct sufficient due diligence on their customers. These failures were not due to a lack of regulatory obligations, but rather insufficient awareness within the TCSPs of their risks and/or inadequate measures to detect high-risk activities. The effectiveness of supervision of DNFBPs and the extent to which DNFBPs are applying their obligations (where they exist) has been a consistent challenge for countries throughout the current round of FATF Mutual Evaluations[63].

Case Study 66 – Netherlands
The case involves funds derived from extortion. The suspect created legal constructs made up of parent companies registered in a low tax jurisdiction with few or no or scarcely any obligations to keep administrative and accounting records. The suspect used a coded bank account in Switzerland to further conceal the money laundering activity. TCSPs managed the companies. According to the public prosecutor: "*the refinement also included the use of persons and trust companies who/which from the nature of their profession should have noticed what was going on and should have had alarm bells going off in their heads. However, no one saw reason to flag any concerns*."

62 HM Treasury, 2015.

63 See www.fatf-gafi.org.

SECTION 4 — ENVIRONMENTAL VULNERABILITIES

202. Aside from the main characteristics leading to the misuse of legal persons and legal arrangements, and the inherent vulnerabilities associated with the professional intermediaries involved in their establishment, a number of environmental vulnerabilities can affect the overall risks posed by these legal structures and the service providers that support their creation and operation. These environmental vulnerabilities include jurisdiction-specific vulnerabilities, such as AML/CFT regulations and trade and commercia trends, and vulnerable business practices, including online client interactions. These vulnerabilities are outlined in greater detail below.

Jurisdictional vulnerabilities

203. The availability of beneficial ownership information varies significantly between different countries. Despite a renewed focus on the importance of timely and accurate beneficial ownership information by key bodies such as the FATF, Egmont Group, and OECD Global Forum, as well as the G20 and UK Anti-Corruption Summit, many countries have not taken sufficient steps to enhance the transparency of beneficial ownership through the effective implementation of the FATF Standards. This is reflected in the aggregated results for the fourth-round of mutual evaluations completed to date, which demonstrate that most countries assessed at the time of the drafting of this report had demonstrated low or moderate levels of effectiveness and technical compliance against key recommendations relevant to beneficial ownership.[64] This increases the difficulties and costs associated with conducting due diligence, particularly for small businesses (such as the majority of professional intermediaries), and makes it harder for professionals and financial institutions to identify patterns and indicators of criminality.

204. In parallel, the FATF has undertaken a Horizontal Study of enforcement and supervision of beneficial ownership obligations of FATF and FSRB members. The Horizontal Study demonstrated that, even where professional intermediaries are subject to AML/CFT requirements, supervisory mechanisms remain weak due to capacity issues and the lack of a consistent approach for different types of professions. Enforcement actions are also rare[65]. The results of the Horizontal Study are located at Annex B of this report.

205. Aside from considerations of the effectiveness of regulatory, enforcement, and supervisory measures in a given country, consideration should also be given to whether the country in which the legal person or arrangement is established, or the country in which the legal person or arrangement has an active bank accounts, is a common international trade or financial centre and/or a low-tax jurisdiction. These geographic vulnerabilities are outlined in greater detail below.

64 FATF (2018).

65 See, in particular, Questions 5 and 6 of the Horizontal Study.

Trade and Financial Centres

206. As this report has demonstrated, there are a number of reasons why criminals seek to exploit legal persons and arrangements to disguise beneficial ownership. One of the primary benefits offered by legal persons is the opportunity to disguise transactions as legitimate business and trade activities. In particular, legal persons can facilitate trade-based money laundering (TBML) typologies, including those that do not result in the actual movement of goods, or which purport to involve the provision and/or acquisition of services to or from other international businesses. The Israeli case study below (Case Study 40) demonstrates how companies in international jurisdictions (including one in a major South-East Asian trading hub) were used to facilitate TBML through false invoicing.

207. In order to leverage domestic and international trade and finance trends, criminals will often establish legal persons and bank accounts in cities that are considered to be major regional and global trade and financial centres. These trade and financial centres can be loosely defined as any city which:

- can be considered an epicentre of regional or international trade
- is known to accommodate regional headquarters of major international businesses, consultancy firms, and/or financial institutions
- is home to a cluster of national and internationally significant financial services providers, such as banks, investment managers, or stock exchanges.

208. Establishing legal persons in these trade and financial centres serves to:

- legitimise the legal person as a seemingly high-functioning and active business
- legitimise the transactions between two or more legal persons as lawful trade
- conceal the unlawful transactions made by, or to, the legal persons behind the vast number and value of genuine transactions occurring across the same trade and finance channel.

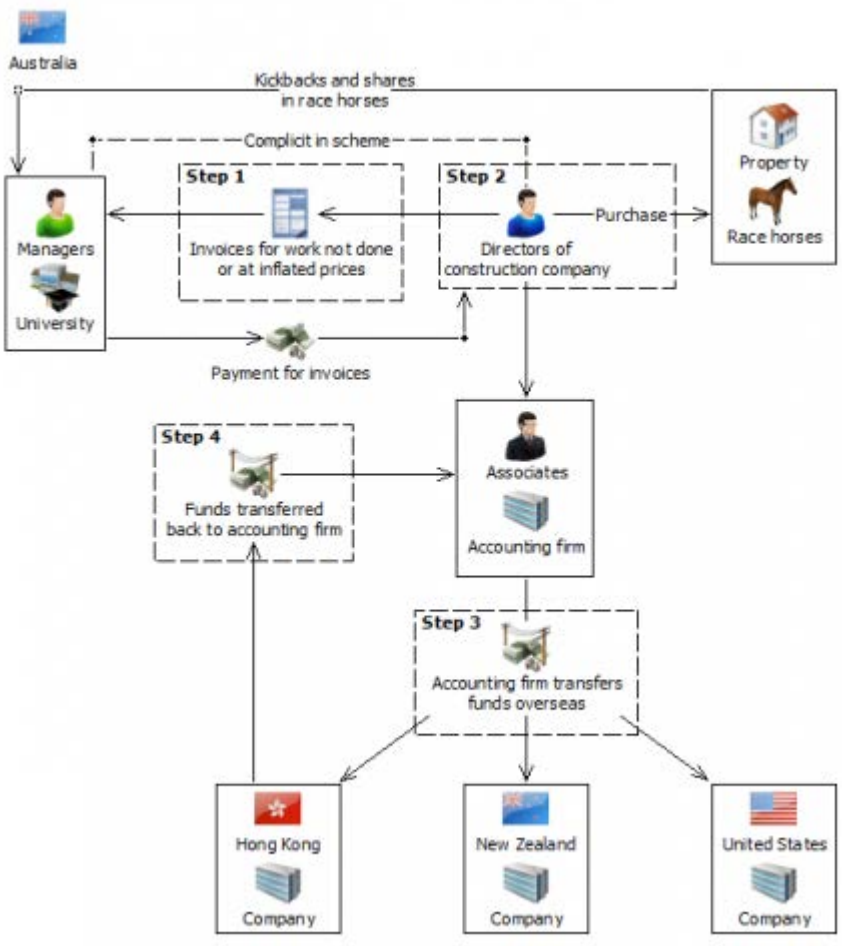
209. As a result of the value and popularity of legal persons incorporated in global and regional trade and financial centres to facilitate criminality and the concealment of beneficial ownership, these entities are likely to represent a greater vulnerability compared to legal persons established in other countries or cities. This jurisdictional vulnerability is unique for each country, and is based on the trade and finance corridors that most affect the economy and society of that country. In the Australian case below (Case Study 3), the accounting firm that facilitated the fraud on behalf of the two university managers utilised companies in Hong Kong, the US, and Canada to launder the proceeds under the guise of legitimate business transactions. These countries represent major trading and finance hubs in the Australian context.

210. Due to the unique nature of this jurisdictional vulnerability, this report has not sought to list highly-vulnerable cities or countries. FIUs, other competent authorities, and financial institutions are best placed to identify high-risk money laundering corridors specific to their economy, and should use this information to assess the vulnerability posed by legal persons operating or transacting along these corridors. Furthermore, countries and cities that are themselves major trade and

finance centres should be aware of their vulnerabilities as possible jurisdictions of choice for international criminals.

Case Study 3 – Australia

Managers at a university and directors of construction companies were complicit in a fraudulent invoice scheme. The managers approved inflated invoices for maintenance work to be carried out by the construction companies, as well as invoices for work that was never undertaken. The profits from the fraud were used to purchase racehorses and property. The managers at the university were repaid with kickbacks or direct shares in racehorses. Accounting firms, which were undertaking international transfers on behalf of the suspects, sent money to many countries including New Zealand, Canada, Hong Kong, and the USA. A large proportion of the funds were sent to companies linked to the horse racing industry. The accounting firms also received international transfers from various overseas entities that were similar in value to the amounts the firms had sent overseas initially. The majority of these transfers originated from Hong Kong. The authorities suspected that the accounting firms were laundering the funds on behalf of the suspects as part of a professional money laundering syndicate.



Case Study 40 – Israel

This case involved a fraudulent tax scheme designed to evade paying tax generated from international trade and a ML infrastructure that was used to hide the illegally gained funds. The suspects used a TCSP to register and operate two international shell companies (Company A and Company B) to create the false appearance that the revenues from their international trading did not belong to the local Israeli company which they controlled, to avoid tax. The two companies traded with each other exclusively and did not have any other source of income. Company A (foreign shell company) transferred significant funds to company C (local company) using the cover of a "consulted fee"/ "service commission". Only this commission, which was less than half of the real income, was reported to the tax authority in Israel. Thus, ultimately, the suspects paid taxes only on a small part of their income.

Low-Tax Jurisdictions

211. A number of jurisdictions across the globe have implemented favourable tax conditions, including very low or even nil corporate or income tax rates, or other tax incentives designed to appeal to foreign investors.[66] These are characteristics associated with many offshore financial centres (OFCs)[67]. International research has demonstrated that the decision by a jurisdiction to offer favourable tax concessions, even marginal concessions, can stimulate investment and result in overall benefits to the jurisdiction (despite the obvious reduction in direct corporate taxes).[68] These low-tax jurisdictions attract foreign investment, not only because income earned locally is taxed at favourable rates, but also because it makes it possible to facilitate the avoidance of taxes that might otherwise have to be paid to other countries.[69]

212. FIUs, law enforcement, and other competent authorities regularly identify criminals using legal persons and bank accounts established in low-tax jurisdictions. Many of the case studies included in this report demonstrated this trend, and over half of the cases analysed involved a transfer of funds via companies or accounts held in low-tax jurisdictions. Many case studies, however, were not specific when referring to international jurisdictions (many simply referred to "offshore jurisdictions" to refer to jurisdictions outside of the reporting country's national boundaries). This prevalence may also be a result of selection bias, whereby

66 Dharmapala, D. & Hines, J., 2009: p. 1058.

67 Defined as countries or jurisdictions with financial centres that contain financial institutions that deal primarily with non-residents, in foreign currency on a scale out of proportion to the size of the host economy, jurisdictions where non-resident owned or controlled institutions play a significant role within the centre and where the institutions in the centre may gain from tax benefits not available to those outside the centre. See the OECD Glossary on Statistics (www.stats.oecd.org).

68 Dharmapala, D. & Hines, J., 2009: pp. 1058-1068.

69 *Ibid:* p. 1060.

participating countries chose cases for submission based on the involvement of certain jurisdictions. Regardless, it is likely that criminals will continue to target low-tax jurisdictions due to the favourable return on investment made possible by tax concessions and the ease with which companies and bank accounts can be established in some of these jurisdictions by foreign nationals.

213. It is important to note that many OFCs are actively involved in global efforts to combat money laundering and tax evasion, including via the FATF, Egmont Group, and the OECD Global Forum. Many of the jurisdictions that are members of the OECD Global Forum are signatories to the two internationally agreed standards on the exchange of information for tax purposes: the *Exchange of Information on Request* (EOIR) and *Automatic Exchange of Information for Tax Purposes* (AEOI). Some OFCs commenced the automatic exchange of information in 2017, while others are expected to commence the exchange of information by September 2018.

214. Due to the degree to which OFCs are exploited by criminals to conceal wealth and beneficial ownership, legal persons established in these jurisdictions, particularly those indicative of being shell companies, can pose a vulnerability to other jurisdictions. Whilst OFCs are vulnerable, they should not be viewed as a collective, but on an individual basis.

Case Study 43 – Italy

This case related to an investigation into a transnational criminal organisation active in money-laundering and that perpetrated crimes in Italy. It was triggered by STRs concerning financial flows from a company in the British Virgin Islands channelled through a Swiss bank and sent to an Italian legal person to be used for a refurbishment of a real estate unit which had a value of EUR 9 million. The investigation resulted in the charging of a chartered account for money laundering. The search of the individual's office resulted in the seizure of documents pertaining to a high number of off-shore vehicles which were established on behalf of wealthy national clients. The subsequent investigations led to the discovery that around EUR 800 million had been moved between Italy and international accounts.

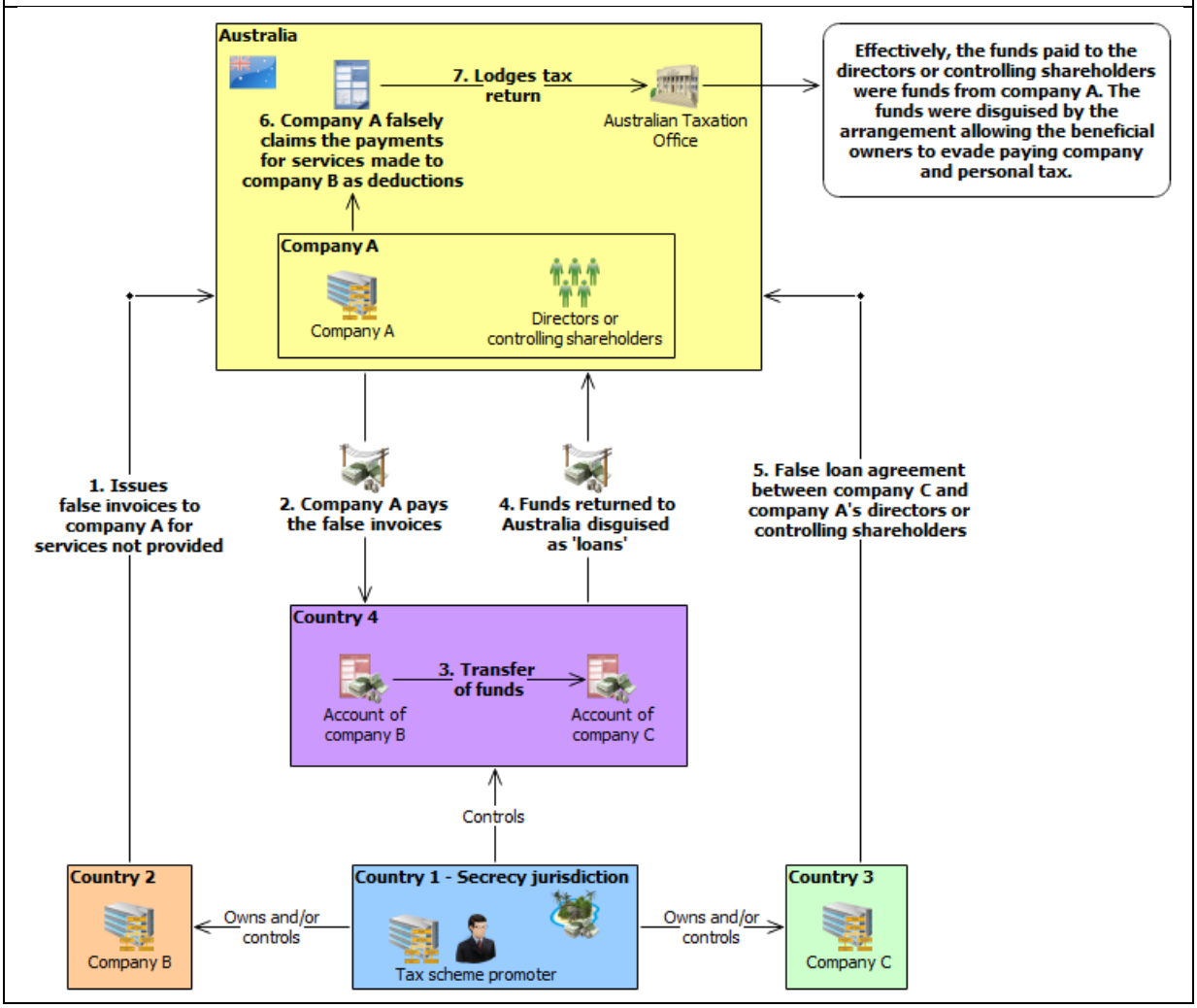
Case Study 68 – Netherlands

This case was an investigation into Dutch suspects for filing incorrect tax returns, money laundering and forgery. During the investigation, it was identified that funds had been transferred through a numbered account in Switzerland in the name of a financial service provider in Panama. Shortly thereafter, very similar amounts were debited from the account, under a false description, to the credit of the Dutch suspects.

A financial service provider facilitated this by providing the Dutch suspects with the opportunity to conceal these cash flows from third parties. The invoices for the services provided were paid to the financial service provider via the account in Switzerland.

Case Study 8 – Australia

Project Wickenby identified the use of false invoices and loans in illegal international arrangements. The scheme involved an Australian company (company A) which entered into an agreement with a tax scheme promoter based in a tax secrecy jurisdiction (country 1). The promoter benefited from the confidentiality and privacy offered in the tax secrecy jurisdiction. The tax scheme promoter owned and/or controlled two international companies (company B and C). Control may have involved the use of a trust or the use of third parties; for example, a relative or associate may act as the director of the international companies. Company B provided consultancy and/or management services and is incorporated in country 2. Company C provided a financial service (as a lender of money, for example) and was incorporated in country 3. Companies B and C held bank accounts in country 4. The promoter controls and operates these accounts.



Vulnerable business practices

215. In analysing the role of professional intermediaries in the concealment of beneficial ownership, this report has focused on a range of business practices that make these professional intermediaries more vulnerable to exploitation. These vulnerable business practices are most commonly performed by professional intermediaries, and contribute to the risks posed to, and by, those professions. Of these vulnerable business practices, the provision of online and virtual services is one exhibited by many businesses across a wide range of industry sectors, including the professional intermediary and finance and banking sectors. Due to its ubiquitous nature, it has been addressed separately as an environmental vulnerability below.

Online and Virtual Services

216. The ability to disguise beneficial ownership is exacerbated by the provision of online and virtual services to clients and banking customers. Many professional service providers and financial institutions have implemented business practices and client tools designed to simplify client interactions by reducing or removing the need for face-to-face interactions. These services leverage the pervasive nature of the online marketplace and meet the expectations of modern consumers, who largely expect that everything can be purchased, sold, or otherwise transacted online. Online services are therefore likely to become more prevalent over the course of the digital age.

217. The ability to establish companies, business banking relationships and move money virtually in the absence of direct face-to-face contact with a professional service provider or financial institution can increase the risk of these entities facilitating illicit activity; whether identity fraud or common money laundering typologies such as smurfing[70] and cuckoo smurfing[71]. Similarly, the ability to establish companies and move funds in this way can help facilitate the concealment of beneficial ownership information. Many financial institutions have implemented measures to verify the identity of clients in the absence of face-to-face engagement, and governments are establishing or exploring tools and resources to support these efforts, including document verification services and formal virtual identities. However, despite these measures, reliance on documentation provided by a customer in the absence of face-to-face engagement can enable the use of fraudulent documentation or help enable informal nominees to act as representatives without the knowledge of professionals or financial institutions. As a result, online and virtual services are vulnerable to exploitation by criminals, and financial institutions

70 The term “Smurfing” is given to the practice of using multiple individuals or accounts to perform transactions so as to avoid suspicion or currency reporting requirements.

71 The term “cuckoo smurfing” originated in Europe because of similarities between this typology and the activities of the cuckoo bird. Cuckoo birds lay their eggs in the nests of other species of birds which then unwittingly take care of the eggs believing them to be their own. In a similar manner, the perpetrators of this money laundering typology seek to transfer wealth through the bank accounts of innocent third parties. (AUSTRAC Website: www.austrac.gov.au/typologies-2008-methodologies, cited 25 January 2018).

and professional service providers need to be conscious of individuals and intermediaries that may be manipulating these facilities.

218. In addition to the challenges of conducting CDD in a virtual environment, the use of internet banking services to facilitate transactions further exacerbates these issues by allowing unknown individuals to control bank accounts anonymously. FIUs and other competent authorities have reported that criminals will often coerce "straw men" to establish bank accounts for use by the criminal at a later time. Once accounts are established, and following the CDD activities conducted by the financial institution, these "straw men" will hand over the account details, including internet banking login details and passwords to the criminal. This effectively disguises the beneficial owner of the account and allows the controller to circumvent CDD obligations altogether.

219. The Israeli case study below demonstrates how the provision of online services allowed a suspect to establish companies and open bank accounts abroad using identification information provided by third-party straw men. It also demonstrates how the availability of foreign online banking platforms allows unknown third parties (in this case, the suspect) to circumvent the due diligence measures of financial institutions located abroad and actively control foreign accounts opened by unrelated individuals. The case study also shows that authentic identification documents, such as a lawful passport, can be easily used in foreign jurisdictions by third parties in the absence of face-to-face interaction, as document verification controls are only designed to verify the authenticity of the document, and not whether the document belongs to the person opening the account.

220. Some financial institutions and RegTech firms have implemented, or are developing, CDD measures that harness modern technologies to enhance customer identification in a virtual environment. These measures include:

- capturing metadata from client interactions, such as internet protocol (IP) addresses and geolocation data
- using in-built cameras from mobile phones, tablets, laptops, and automatic teller machines (ATMs) to capture the customer's image (with the customer's knowledge and consent) for verification against other identity documents, and
- utilising biometric identifiers, including facial recognition and fingerprint scanning technologies.

221. These developments have the potential to significantly reduce the vulnerabilities associated with the provision of online and virtual services. However, the expense and sophistication of these CDD systems is likely to limit their implementation in the short term, and the vast majority of professional service providers and smaller financial institutions will continue to be vulnerable to exploitation and the challenges associated with identifying beneficial ownership in a virtual environment.

Case Study 38 – Israel

This scheme was used to hide funds from social engineering fraud and other criminal offenses. The cover story for the criminal offences was international trade – funds from merchants in Europe and the US sending payments to suppliers in East Asia. The suspect, an owner of a registered MSB, operated a second, unregistered MSB. The suspect used several natural persons as his contact points in East Asia which in turn contacted local company service providers for the purpose of setting up international companies and opening bank accounts. Local straw men were registered as the shareholders of the new international companies established for the scheme. Shareholders were registered based on passports provided by the suspect's contact persons mentioned above. The registered addresses of the companies were in East Asia. Bank accounts were opened in the same East-Asian countries where the offices were located.

Immediately after opening the bank accounts, the suspect received the sole means to control them, i.e. an electronic token with the passwords for online activities. In order to establish creditability and credit history, some accounts were activated as low-volume activity accounts, while others were used for high-volume transactions. In case the bank had questions about the nature of the transactions, the questions were sent to the suspect by the straw men and were returned to the bank by them.

Use of Third-Party CDD and Identity Verification

222. There are a range of third-party service providers who specialise in providing support to identity verification and customer due diligence services to corporate clients, such as sanctions lists and other adverse information, and information on company ownership. These services can be an important part of a robust and effective CDD program, and can improve the ability of a financial institution or DNFBP to assess customer risk and verify a customer's identity (although it should be noted that responsibility for CDD measures remains with the financial institution or DNFBP in context of outsourcing or agency relationships, in accordance with FATF Recommendation 17).

223. Despite the value of these services, some major financial institutions have reported, via the Wolfsberg Group, that the information provided by third-party service providers can be out-of-date or incomplete. This has the potential to frustrate CDD activities, including the verification of beneficial ownership and related ML/TF risk assessments due to the provision of inaccurate information. These major financial institutions have only been able to identify the deficiencies in the information provided by third-party service providers due to their own CDD and financial intelligence capabilities. However, if smaller financial institutions who do not have well established CDD mechanisms rely on third-party service providers to support their CDD efforts, they may not be aware of the inaccuracy of the

information being provided, resulting in a vulnerability in cases when the information is inaccurate.

224. Due to the expense of establishing and maintaining a robust and effective in-house CDD and financial intelligence capabilities, most financial institutions and professional service providers will continue to rely heavily on the services provided by third parties. The reason why the information stored by third-party service providers is sometimes deficient is not understood, and may be symptomatic of the enormous challenges associated with collecting relevant and contemporary information on a global scale. While the advent of virtual identities may improve this situation in the future, there may be opportunities for this information resource to be improved.

Reliance on introduced business

225. Financial institutions and DNFBPs can also rely on other regulated financial institutions and DNFBPs to carry out the CDD process in certain circumstances, which are set out in Recommendation 17. In many cases, this will involve a financial institution relying on a lawyer or TCSP, which is providing company formation services and also seeking to open bank accounts on behalf of the newly created company. If the requirements for reliance set out in Recommendation 17 are not properly applied, then a financial institution's CDD can be compromised by a negligent or complicit DNFBP which it relies on, undermining their ability to accurately identify beneficial ownership or suspicious activities indicative of efforts to disguise ownership and control.

SECTION 5 — CONCLUSIONS AND ISSUES FOR CONSIDERATION

226. Schemes designed to obscure beneficial ownership often employ a "hide in-plain-sight" strategy, leveraging global trade and commercial infrastructures to appear legitimate. However, visibility does not equate to transparency, and many of the tools that were designed to encourage business growth and development, such as limited liability corporations and nominee directorship services, are now also being exploited to facilitate money laundering. The globalisation of trade and communications has only increased this threat, and countries now face the challenge of enforcing national laws in a borderless commercial environment.

227. This report has analysed open-source research, public intelligence reports, classified intelligence holdings, and public and private sector experience and expertise to compile a comprehensive overview of the main characteristics and vulnerabilities that lead to the misuse of legal persons and arrangements, and the exploitation of professional intermediaries, to conceal beneficial ownership. Much of what this report has identified confirms key principles and concepts reported in the canon of literature available on the subject of beneficial ownership. This suggests that the vulnerabilities associated with the concealment of beneficial ownership are enduring, or increasing, despite ongoing efforts to combat money laundering and terrorism financing. These key findings are outlined in detail in the Executive Summary.

228. The FATF Recommendations require competent authorities to have access to adequate, accurate and timely information on the beneficial ownership and control of legal persons (Recommendation 24). In addition, countries must take measures to prevent the misuse of legal arrangements for money laundering and terrorist financing - in particular ensuring that there is adequate, accurate and timely information on express trusts (Recommendation 25). Implementation of the FATF recommendations on beneficial ownership has proven challenging for countries. As a result, the FATF developed the *FATF Guidance on Transparency and Beneficial Ownership* to assist countries in their implementation of Recommendations 24 and 25, as well as Recommendation 1 as it relates to understanding the ML/TF risks of legal persons and legal arrangements.

229. This section includes a series of issues for consideration that may, alongside the conclusions of the study, support the effective implementation of these two FATF Recommendations including by outlining areas of further potential work to reduce the barriers faced by law enforcement and increase the accuracy and/or availability of beneficial ownership information.

230. This report shows that limited liability companies (and similar companies in various jurisdictions) are more vulnerable to misuse for the concealment of beneficial ownership than other types of legal persons. This is due to the ease with which they can be established, and the manner in which they are often used to generate complex legal ownership structures. Moreover, the availability and use of nominee directors and shareholders (both formal and informal) appear to exacerbate the risks despite the FATF Standards requiring measures to prevent their misuse. Nominees have been identified as a central enabler of indirect ownership chains. Given the vulnerabilities associated with the use of nominees,

further study into the role that professional nominees play is merited to better understand the costs and benefits associated with allowing the practice, and to identify the best means to tackle their misuse. Any further study in this area may benefit from also having the expertise of other international organisations that have a wider view of global economics than the FATF, which is focused on combatting money laundering and terrorist financing.

Issue for Consideration 1
Given the vulnerabilities associated with use of nominees, individual countries and the FATF, working with the broader global community may wish to consider measures to limit their misuse.

231. The use of specialists and professional intermediaries is a key feature of schemes designed to conceal beneficial ownership. The majority of case studies analysed for this report involved professional intermediaries. While it was not always explicitly stated in the case studies, approximately half of all cases were assessed as involving a complicit professional intermediary (gatekeepers were determined to be complicit if, on the basis of the case summary provided, they appeared to have had a role in designing the scheme, knew of the scheme's illegal nature, or were charged with a crime). This demonstrates that although complicity may be a factor, it is not strictly necessary when facilitating a scheme designed to obscure beneficial ownership, and that some professionals are unwitting or negligent in their involvement. This also serves to highlight the importance of effective regulation and education of DNFBPs, and the need for increased AML/CFT awareness amongst professional services sectors. The FATF's *Horizontal Study of Supervision and Enforcement of Beneficial Ownership Obligations* identified that a number of countries do not impose any AML/CFT obligations or supervision on any DNFBPs, despite this being a requirement of the FATF Standards. Professional intermediaries operating outside of an AML/CFT regulatory regime represent a "back-door" through which illicit wealth can enter the regulated banking and finance sector. This places the AML/CFT programs of financial institutions at risk and detracts from the overall effectiveness of national and international AML/CFT regimes, and should be addressed as a matter of priority through the effective implementation of relevant FATF standards.

232. A key part of ensuring effective implementation is the need for ongoing dialogue between competent authorities and DNFBPs. Government authorities should work closely with private sector bodies to educate professionals of their vulnerabilities to ML/TF activity, and the underlying threats that may seek to exploit these vulnerabilities, and allow professionals to share emerging risks drawing on their experience. Gateways have been established in many countries to enable the sharing of information between law enforcement and regulated entities, and countries could consider how these avenues of information exchange could be used to enhance risk awareness amongst professional intermediary sectors.

Issue for Consideration 2
The regulation of professional intermediaries under AML/CFT law[72], and efforts to educate professionals of their money laundering and terrorism financing threats and vulnerabilities[73], will help mitigate the vulnerabilities associated with the concealment of beneficial ownership.

233. The Horizontal Study identified a lack of consistency in the approach to supervision when different types of professional intermediaries are supervised by different bodies (self-regulating bodies), even if the intermediaries are performing essentially similar functions (such as company formation). While many jurisdictions have established various forums to facilitate co-operation and risk awareness among SRBs and other competent authorities, the results of the Horizontal Study suggests that this does not necessarily lead to a coherent approach in supervision.

234. TCSPs play an important role in facilitating the establishment and management of legal persons, particularly in circumstances where the beneficial owner resides in a foreign jurisdiction. From a regulatory standpoint, the TCSP sector is less clearly defined or understood in many countries when compared to the legal and accounting sectors. As a result, authorities in many countries face challenges in regulating and educating TCSPs on their ML/TF risks. Conversely, some countries, particularly low-tax jurisdictions, have well-established and regulated TCSP sectors, and have implemented a range of measures to enhance the AML/CFT regulation of TCSPs, including integrity, competence, and financial soundness tests. These measures are a good means of professionalising the TCSP sector, and countries with TCSP sectors that are not as well-defined should consider implementing similar measures domestically.

235. Law enforcement and FIUs have reported that LPP can be exploited by complicit legal professionals to frustrate and hinder investigations. This issue has also been reported in previous FATF reports, including the 2013 report on *Money Laundering and Terrorism Financing Vulnerabilities of Legal Professionals*[74], and the 2014 guidance on *Transparency and Beneficial Ownership*[75]. Due to the nature of LPP, claims of privilege need to be reviewed prior to being overturned, even if the grounds for LPP are questionable from the beginning. Regardless of the rules associated with LPP in most countries, the subjective nature of LPP will continue to pose a challenge due to the potential for its inconsistent application, and the difficulties that it can cause competent authorities undertaking financial investigations. Private sector representatives have highlighted that LPP training offered to legal professionals can often be inadequate unless the legal professional specialises in litigation where it is frequently considered. It has been suggested that the low level of training, coupled with a lack of practical application by some legal

72 In accordance with Recommendations 22, 23, and 28 of the FATF Standards

73 In accordance with Recommendation 34 of the FATF Standards

74 FATF, 2013: p. 23.

75 FATF, 2014: p. 38.

professionals leads to the development of broad and conservative approaches to LPP. Enhanced training and guidance in this area may assist to reduce this vulnerability over time; however, countries are encouraged to work with the legal profession to determine the best means of addressing this problem, and to provide greater clarity on the scope and parameters of LPP so as to limit the extent to which it is inadvertently misused resulting in the impediment of financial investigations. Further consideration of possible solutions is merited.

Issue for Consideration 3
Further work to identify possible solutions or measures to prevent the misuse of LPP to conceal beneficial ownership information, including through the provision of enhanced training and guidance material for legal professionals, could be considered.

236. When investigating cases involving a concealed beneficial owner, FIUs and other competent authorities confirmed that traditional financial institutions, namely banks, were the primary source of information required to identify and confirm beneficial ownership and control. The wealth of information held by the private sector is substantial, and crucial to the identification of money laundering and broader criminality. In comparison, the information held by many FIUs is limited to suspicious transaction reports, and many FIUs are not capable of independently analysing other sources of information such as cross-border financial flows, without requesting further information from financial institutions. Those FIUs that receive a broader set of reports, including cross-border wire transfer and threshold cash transaction reports, have reported the importance of those reports and their value in tracing money flows and identifying beneficial ownership information. Consideration should be given to possible measures to increase the breadth and depth of information available to FIUs.

Issue for Consideration 4
FIUs should have access to the widest possible range of financial information. Consideration of possible measures to increase the breadth and depth of information available to FIUs is merited.

237. Further to the need for FIUs to have greater independent access to account and transaction information, the direct sharing of information and intelligence, in real time, between competent authorities and private sector partners, cannot be understated. This includes the sharing of transaction records, as well as information collected through customer due diligence. The significant body of work conducted by the FATF, the Egmont Group, and other international bodies on information sharing already attests to the value of effective information sharing. Information sharing between public and private sectors is an essential means of enhancing the transparency of beneficial ownership. Additionally, the information that is exchanged through established mechanisms, such as the Automatic Exchange of Information (AEOI) and the Exchange of Information on Request (EOIR) for Tax

Purposes, has the potential to significantly enhance the law enforcement visibility of asset ownership in other jurisdictions. However, privacy protections may limit the extent to which this information can be used for law enforcement and financial intelligence purposes.

Issue for Consideration 5
Increased sharing of relevant information and transaction records would benefit global efforts to improve the transparency of beneficial ownership. Further consideration of possible ways to enhance this information sharing is merited.

238. As a result of the transnational nature of most schemes designed to disguise beneficial ownership, it is often not possible for FIUs and other competent authorities to have direct and independent access to the information necessary to discover and prove beneficial ownership. In addition to a range of information sharing mechanisms available to competent authorities, mutual legal assistance has been identified as a key tool in most major investigations that involve a transnational corporate structure or international financial flows. However, many law enforcement and intelligence practitioners have also reported that delays in mutual legal assistance requests are one of the issues that most significantly inhibits an investigation. While it is acknowledged that the ability of a country to respond to a mutual legal assistance request is dependent on the resources available in that country and the operational demands of its law enforcement agencies, it is evident that more can be done to improve the quality and timeliness of mutual legal assistance responses. FATF Recommendations 36-40 require countries to implement formal and informal mechanisms for sharing information on ML/TF and predicate offences. Further study to understand what can be done to improve international co-operation, including MLA, is merited.

Issue for Consideration 6
Further research should be undertaken to understand what can be done to improve the quality and timeliness of the cross-border sharing of information, including through mutual legal assistance.

239. In recent years, increased media attention given to the role of opaque ownership structures in tax evasion, money laundering, and corruption schemes[76] has prompted a range of responses from governments across the globe, including the consideration and development of centralised registers of beneficial ownership. Other registries, such as corporate registries (centralised or not) which hold information on beneficial ownership, are also being implemented or enhanced. These registries are among several mechanisms for countries to consider under the

[76] Principally as a result of the leak of confidential documents from two large law firms involved in the creation of complex international corporate structures: Panama-based law firm Mossack Fonseca (2015), and Bermuda-based law firm, Appleby (2017).

FATF standards to support the identification and verification of beneficial ownership. Multiple sources of information can be used simultaneously by competent authorities for intelligence and investigative activities, and the FATF Standards state that it is very likely that countries will need to utilise a combination of mechanisms to ensure law enforcement authorities have access to adequate, accurate and timely information on the beneficial owner of legal persons. It is also possible that, if correctly monitored and supervised, registers of beneficial ownership could support CDD efforts by financial institutions and professional intermediaries. However, in designing and implementing such repositories of beneficial ownership information, governments should be conscious of the need to ensure that beneficial ownership information is accurate, up-to-date and readily available to competent authorities and the private sector. A register of information, whether it contains beneficial ownership or any other type of company information, is only as valuable as the quality and accuracy of the information held. This report has outlined the myriad measures used by criminals to conceal beneficial ownership, including the use of formal and informal nominees, and it is expected that many of these techniques could be adapted to circumvent beneficial ownership registers or attempt to diminish their utility.

Issue for Consideration 7
Countries that make use of registers of beneficial ownership information should consider the resourcing and expertise requirements associated with their maintenance to ensure that the information recorded in the register is adequate, accurate, and up-to-date, and can be accessed in a timely manner. This is also true for the maintenance and supervision of company registries.

240. The ability to establish companies, open bank accounts, and move money virtually in the absence of direct face-to-face contact with a professional service provider or financial institution is a growing vulnerability. The Horizontal Study confirms that direct on-line incorporation of companies using various forms of digital identity is permitted by a number of jurisdictions[77]. Many financial institutions have implemented measures to verify the identity of clients in the absence of face-to-face engagement, and governments are establishing or exploring tools and resources to support these efforts; however, the provision of services in the absence of face-to-face engagement is a vulnerability commonly exploited by criminals. Technological innovations, particularly in the fields of digital identification and information sharing, will likely be an important element in future solutions to this challenge. The private sector has identified some emerging measures that may be highly valuable in conducting CDD, and countries may wish to consider how these initiatives might be harnessed to improve the transparency of business transactions. The FATF and Egmont Group are both increasingly engaged with the private sector and these engagements may lead to the identification of additional measures to improve transparency in the future.

77 See, in particular, Question 1 of the Horizontal Study at Annex B.

241. To meet the challenges posed by opaque beneficial ownership arrangements, governments, financial institutions, and professional intermediaries need to clearly understand the vulnerabilities, threats, and overall risks associated with legal persons and arrangements. It is therefore essential for governments to maintain a robust, contemporary, and publicly accessible assessment of ML and TF risks affecting their jurisdiction. The FATF Standards require countries to understand the risks that they face, including having mechanisms to assess the money laundering and terrorist financing risks associated with different types of legal person created in their country. These national risk assessments should not be limited to the risks identified within a jurisdiction's borders, but should also carefully analyse transnational threats and vulnerabilities. By maintaining an ongoing and publicly accessible risk assessment, governments will nurture and inform risk assessments conducted by financial institutions and professional service providers operating in their jurisdiction. This report, and others like it, may be useful in informing these assessments.

Issue for Consideration 8
The FATF Recommendations require jurisdictions to assess the money laundering and terrorist financing risks associated with different types of legal persons created in their country. It would be beneficial for these assessments to carefully consider and articulate the vulnerabilities and threats relating to domestic and foreign legal persons and arrangements, the domestic and foreign intermediaries involved in their establishment, and the means by which criminals may exploit them to facilitate money laundering and other criminality.

242. The concealment of beneficial ownership is a significant vulnerability for money laundering activity in every country around the world. For this reason, it will continue to pose a major challenge to the FATF and Egmont communities. Continued globalisation, the digitisation of commerce, trade, and financial and professional services, and increased access to opaque legal vehicles, are all enduring challenges that will affect the availability of information on the beneficial owner. There is no one solution or panacea for this problem; rather, the global endeavour to enhance transparency will require numerous iterative and interrelated solutions, and the continued will of governments, private organisations and the public to implement them.

ANNEX A. REFERENCES

ACC (2015), *Organised Crime in Australia*, ACC, Canberra.

ACIC (2017), *Organised Crime in Australia 2017*, ACIC, Canberra.

AUSTRAC (2011), *Money Laundering in Australia 2011*, AUSTRAC, Sydney.

Dharmapala, D. & Hines, J. (2009), "Which Countries Become Tax Havens?" in *Journal of Public Economics*, Volume 93, pp. 1058-1068.

FATF (2006), *Misuse of Corporate Vehicles, Including Trust and Company Service Providers*, FATF, Paris.

FATF (2007), *Money Laundering and Terrorist Financing through the Real Estate Sector*, FATF, Paris.

FATF (2008a), *Risk Based Approach Guidance for the Legal Sector*, FATF, Paris.

FATF (2008b), *Risk Based Approach Guidance for Accountants*, FATF, Paris.

FATF (2008c), *Risk Based Approach Guidance for Trust and Company Service Providers (TCSPs)*, FATF, Paris.

FATF (2008d), *Risk Based Approach Guidance for Real Estate Agents*, FATF, Paris.

FATF (2010), *Money Laundering Using Trust and Company Service Providers*, FATF, Paris.

FATF (2011), *Laundering the Proceeds of Corruption*, FATF, Paris.

FATF (2012a), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations*, FATF, Paris.

FATF (2012b), *Specific Risk Factors in Laundering the Proceeds of Crime: Assistance to Reporting Institutions*, FATF, Paris.

FATF (2013), *Money Laundering and Terrorism Financing Vulnerabilities of Legal Professionals*, FATF, Paris.

FATF (2014), *FATF Guidance: Transparency and Beneficial Ownership*, FATF, Paris.

FATF (2018), *Consolidated Assessment Ratings*. FATF, Paris, www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html (updated: 6 April 2018) (accessed cited: 12 April 2018)

Hayton D.J., Kortmann, S.C.J.J.K, Verhagen, H.L.E. (1999), *Principles of European Trust Law*, Kluwer law international, The Hague, the Netherlands. 215 p.

HM Treasury (2015), *UK National Risk Assessment of Money Laundering and Terrorist Financing*, HM Treasury, London.

IBA (2011), *IBA International Principles on Conduct for the Legal Profession*.

ICIJ (2017), *The Panama Papers*, https://panamapapers.icij.org/, last accessed July 2018.

IMF (2014), *Offshore Financial Centres (OFCs): IMF Staff Assessments*, www.imf.org/external/np/ofca/ofca.aspx, last accessed July 2018.

Jersey Financial Crime Strategy Group (2015), *Money Laundering Typologies and Trends: Jersey*, Government of Jersey, Jersey.

Knobel, A. (2017), *Technology and Online Beneficial Ownership Registries: Easier to create companies and better at preventing financial crimes,* Tax Justice Network, https://www.taxjustice.net/wp-content/uploads/2017/06/Technology-and-online-beneficial-ownership-registries-June-1-1.pdf, last accessed July 2018.

OECD (2001), *Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes*, OECD, Paris.

OECD (2012), *Automatic Exchange of Information: What it is, how it works, benefits, what remains to be done*, OECD, Paris.

OECD (2017a), *OECD Global Forum on transparency and Exchange of Information for Tax Purposes*, www.oecd.org/tax/transparency/exchange-of-information-on-request/peer-review/.

OECD (2017b), *Signatories of the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information and Intended First Information Exchange Date*, www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/MCAA-Signatories.pdf, last accessed July 2018.

Sharman, J. C. (2010), "Shopping for Anonymous Shell Companies: An Audit Study of Anonymity and Crime in the International Financial System", *Journal of Economic Perspectives*, Volume 24, Number 4, pp. 127-140.

US Department of State (2013), *Major Money Laundering Countries*, US Department of State, Washington D.C., https://www.state.gov/j/inl/rls/nrcrpt/2013/vol2/204062.htm, last accessed July 2018.

US Treasury (2015), *National Money Laundering Risk Assessment*, US Treasury, Washington D.C.

Van der Does de Willebois, E. et al. (2011), *The Puppet Masters: How the corrupt use legal structures to hide stolen assets and what to do about it*, The World Bank, Washington D.C., p. 240.

WEF (2012), *Organised Crime Enablers*, World Economic Forum, Geneva.

ANNEX B. HORIZONTAL STUDY: ENFORCEMENT AND SUPERVISION OF BENEFICIAL OWNERSHIP OBLIGATIONS

1. Two sets of questions were circulated to FATF delegations and delegations from the FATF-style regional bodies in seeking information on the creation and maintenance of legal persons and arrangements and the supervision and enforcement of maintenance and beneficial ownership requirements.

Question 1: What businesses or professions in your jurisdiction are engaged in the formation and/or maintenance of legal persons or legal arrangements?

2. This question was meant to elicit information on the composition, size and importance of the gatekeeper sectors in each jurisdiction, as well as the roles gatekeepers play in formation of legal persons and arrangements. The information provided demonstrates that, generally speaking, many of the same types of gatekeepers can be involved in the formation of both legal persons and legal arrangements (to the extent legal arrangements are available).

3. Despite the involvement of the same types of intermediaries, the processes for forming legal persons and arrangements are, in most cases, quite different. Accordingly, this paper will address them separately. The following information will address company formation, while formation of legal arrangements will be addressed under Question 2.

4. The information provided by members describes a range of processes for company formation and the role of gatekeepers in those processes. Although there are unique elements to each jurisdiction's system, the descriptions could be divided into four general categories:

- systems where gatekeepers are not necessarily required
- systems in which gatekeepers (other than notaries) are required
- notarial systems
- systems in which the Registrar tests the accuracy of filings or takes on the customer due diligence (CDD) obligations of a gatekeeper.

5. Hybrids of these systems are also possible. Each main type of system is described below.

Gatekeepers Optional

6. In almost half (29 of 64) of the responses received to this question, jurisdictions indicate that gatekeepers are available, but not required for company formation. This includes a variety of systems: some jurisdictions clearly indicated that any member of the public may form a company, but that it is often facilitated by gatekeepers. The UK indicates that, while anyone may register a company, in practice, approximately 75% of companies are formed by gatekeepers. In some jurisdictions, gatekeepers are optional in most circumstances, but required for others, as noted in the next category. Six jurisdictions indicated that the services of a

gatekeeper were available, but did not indicate whether such services were required or how frequently they are used in practice.

Gatekeepers Required

7. In sixteen jurisdictions, intervention by a gatekeeper (other than a notary or government employee) is required to form a legal person in most, if not all, cases. This category includes some jurisdictions with unique characteristics. For example, four jurisdictions only require intervention by a gatekeeper to form "offshore" companies or corporate vehicles (companies or trusts) that were perceived as posing higher risk. The entities in question were designed specifically for the purposes of international activities targeting non-resident customers, in the first place, and as such were probably deemed by the legislators as requiring strengthened measures, such as mandatory involvement of a professional intermediary. In some instances, there is no oversight to make sure that the companies that are restricted to certain activities upon creation (e.g. international holding companies) do not subsequently conduct other activities. However, the main incentive to register them in the correct manner would be preferential tax treatment. Two jurisdictions require involvement of a gatekeeper only to form limited liability companies.

8. The concept of risk-based approach to company formation mechanisms could be subject to closer consideration in future, but the following is one such example.

Box 1. Singapore's Registered Filing Agents and Registered Qualified Individuals

Since 2015, Singapore has had measures in place to ensure that an individual who wishes to form a legal entity on behalf of another person in the course of business must be registered with Accounting and Corporate Regulatory Authority (ACRA) as a Registered Qualified Individual (RQI). Firms or companies that provide such services must register as Registered Filing Agents (RFA) and act through at least one RQI. In this way, members of the public acting on their own behalf (generally considered to be lower risk) retain free access to company registration while gatekeepers are required to register and made subject to anti-money laundering / countering the financing of terrorism (AML/CFT) obligations - regardless of any professional status or registration which they may already hold. Since creation of legal persons is performed online via ACRA's electronic transaction system, this system only allows RQIs of RFAs and individuals to create legal persons and file documents. An individual must use his SingPass, which is a personal access code issued to Singaporeans and permanent residents permitting entry to online government services, to access ACRA's electronic transaction system. Foreigners who do not hold a SingPass have to engage the services of RFAs to create and register legal persons with ACRA. This approach prevents the creation of legal persons by people unauthorised to do so.

The approach taken by Singapore in imposing this requirement to register is in addition to the usual approach of applying AML/CFT obligations to specific

classes of designated non-financial businesses and professions (DNFBPs) (e.g. lawyers, accountants, etc.). For instance, lawyers and accountants who perform FATF defined activities remain to be supervised by the respective regulators/specialised regulatory bodies. At the same time, a firm, whether it is a corporate service provider (CSP) firm, law firm or accountancy firm, will need to be registered with ACRA. RFAs need to provide information on its entity name, registered office address, nature of business and the personal details of the professional Registered Qualified Individuals (RQI) they wish to appoint to assist it. RQIs, in turn, need to provide his or her personal details qualifications. A CSP firm will not be permitted to be registered as a RFA if any of its beneficial owners, directors, partners or managers has been convicted of criminal offences or if they are undischarged bankrupts. An individual will not be permitted to be registered as a RQI, if he has been convicted of a criminal offence (especially those related to fraud and dishonesty) or if he is an undischarged bankrupt. In addition to that, ACRA will also check background information on the legal owners, beneficial owners, directors, partners and managers of RFAs, and RQIs looking at their previous conduct and compliance history.

Notarial Systems

9. Thirteen of the responding jurisdictions report use of a notarial system for company formation. Notarial systems generally entail an attestation of registry filings by a notary who is vested with public office and responsible directly to a government ministry. Such systems are found almost exclusively in civil law jurisdictions and entail a high degree of formality in the company formation process. Understandably, such an approach may not be appropriate for every jurisdiction; however, FATF members have assessed these systems as some of the most effective systems for implementation of beneficial ownership (BO) obligations.

Box 2. Spain's and Italy's notarial system

In their 4th Round mutual evaluations, Spain and Italy were both assessed as having systems that are substantially effective. In both jurisdictions, notaries are public officials, and are subject to AML/CFT obligations under each jurisdiction's AML/CFT legal framework. Duly executed notarial acts are presumed to be valid, self-authenticating, self-executing, and are considered probative. The involvement of a notary is required at the company formation stage, as well as subsequently to validate and ensure accuracy of information reflected in the business register and authenticate changes in ownership.

The effectiveness of Spain's notarial system is enhanced by the implementation of a Beneficial Ownership Database. The Beneficial Ownership Database became operational in March 2014, and was made available to competent authorities in April of the same year. It builds upon the information available in the Single Computerised Index by aggregating the information on beneficial ownership and on transfers of shares. For each company, the database offers two levels of information: (i) the beneficial ownership information obtained by the individual

notary in the conduct of the normal CDD requirements (i.e. the declaration of beneficial ownership which, if at least one risk indicator is met, includes a copy of the beneficial owner's ID document); and (ii) For private limited liability companies (*Sociedades de Responsabilidad Limitada*, which represent some 92% of all legal persons and 96% of new incorporations in Spain) the beneficial ownership information is obtained through aggregating the information on the successive transfers of shares. Since notaries are required to be involved in these transfers, this information is always verified and updated twice monthly.

Registry with Oversight Functions

10. Findings from other FATF research suggest that systems combining one or more approaches to ensuring availability and accuracy of basic and beneficial ownership information are often more effective than systems that rely on a single approach. In 21 jurisdictions, one of the systems referred to above is complemented by a Registry with some level of oversight function, including verification of completeness or accuracy of filings, conducting CDD in certain cases, or cross-checking information against other government databases. Two of these jurisdictions have notarial systems, including Spain, as discussed above. In six jurisdictions, gatekeepers (other than notaries) are required. Thirteen of the jurisdictions fall into the category where gatekeepers are optional.

Box 3. Guernsey's and Jersey's Registrars

Guernsey and Jersey are both jurisdictions in which intervention by a fully regulated and supervised gatekeeper in company formation is mandatory for most company formations (although optional for local residents). However, in both jurisdictions, the Registrar performs the CDD functions of gatekeepers when there is no gatekeeper involved in company formation or administration.

Box 4. UK's Companies House

In the UK, Companies House is part of the Government Agencies Intelligence Network. Although Companies House does not conduct CDD or verify information, it does conduct data analysis to identify suspicious activity and patterns of behaviour, which it then shares with relevant law enforcement agencies. Suspicious activity and patterns of behaviour are identified through a variety of mechanisms. These include:

1. following receipt of a complaint from a third party informing the Registrar that their details (either name, date of birth and/or home address) has been used without consent,
2. contact from Law enforcement/Government agencies regarding suspicions over a single company, and

3. other intelligence that suggests suspicious activity. This could include a single credit card or email address being used to incorporate many companies, which on the surface are unconnected.

Internal investigations utilising non-public data (such as email address, IP address where available and credit/debit card details) can result in the linking of a single suspicious company to tens or hundreds of companies. It should be noted, that there is no automatic feed for this information which leads the Registrar to take action.

Online registry systems

11. Some jurisdictions permit their residents to use different forms of digital identity to incorporate companies directly online, without any intermediaries. Modalities of those digital identities vary: they can be based on tokens, passwords, SMS, or biometric authentication. The basic idea is that an in-person identification takes place only once, either through a government authority or an authorised agent, such as a bank or a post office, on the basis of valid ID papers and/or biometrical data. Once the digital identity is created, it is centrally stored and can be used to access services provided by various public and private sector entities. This information in some cases may not be updated after the initial issuance and the person may be held responsible for keeping the details of access to their digital identity confidential and bears responsibility for how it is used, e.g. use of another person's identify can be a criminal offence in and of itself. On one hand this system has advantages such as simplifying formalities and providing more security (it is almost impossible to falsify a digital ID).However, on the other hand it raises concerns relating to the higher risks of identity theft and misuse by straw men, particularly where insufficient safeguards are in place.

Question 2: Describe the legal requirements for the formation of legal arrangements (whether under domestic or foreign law).

12. In February 2017, the FATF decided that the scope of this project should be expanded to include trusts. Accordingly, this question sought information specific to the formation of trusts and other similar arrangements, whether those trusts or arrangements were created under domestic law or under foreign law. 60% of responses were from jurisdictions whose domestic law provides for the creation of trusts or other similar legal arrangements. A further 21% of responses were from jurisdictions which are not the source-of-law for legal arrangements, but which give some recognition to foreign legal arrangements and permit foreign legal arrangements to be created or administered by gatekeepers or others within their jurisdiction (e.g. under the Hague Trust Convention). Finally, 19% of responses indicate they do not recognise (e.g. in courts or in their tax system) any legal arrangements, whether based on domestic or foreign law.

13. Among the 52 jurisdictions that allow for creation of trusts or similar legal arrangements under domestic or foreign law, almost 54% did not provide any information as to whether registration is required. In the same group, 46% did not provide information regarding implementation of beneficial ownership obligations. Although the information received may be sufficient to recognize some general

patters, a sample this small may not be sufficient to draw any conclusions as to best practices.

14. Among those 24 jurisdictions that provided information on registration of legal arrangements, 29% require registration of trusts. Another 29% do not require registration. The largest percentage, 42% require registration of trusts only when certain criteria are met. Those criteria include generation of taxable income or making taxable distributions, real property included as a trust asset, or when the trust is a foreign trust. It should be noted that trusts might be registered as some other type of business entity if the jurisdiction does not allow for the creation of trusts under its legislation.

15. Regarding implementation of beneficial ownership requirements, 27 jurisdictions provided information. Of those, 52% impose beneficial ownership obligations by applicable statute. Another 26% rely on a combination of common law and statutory requirements, while 22% rely solely on common law trustee obligations for availability of beneficiary information.

Box 5. Jersey's requirements for professional trustees

An interesting example of imposing beneficial ownership obligations by statute was provided in information from Jersey. In Jersey, any person who, by way of business (regardless of underlying profession), acts as or fulfils or arranges for another to act as or fulfil the function of trustee of an express trust conducts a regulated activity and is subject to AML obligations. Similar to the formation of legal persons in Singapore, this system uses an activity-based approach which avoids reference to any particular profession and the unintended imposition of AML obligations on members of those professions whose day to day activities are not at risk for abuse for illicit purposes.

Box 6. New Zealand' regime for foreign trusts

Another example was provided by New Zealand. Since February 2017 it has been implementing a new regime whereby foreign trusts (defined as a trust to which a settlor has never been resident in New Zealand) with a New Zealand resident trustee must register with Inland Revenue Department. Trustees are required to update any changed details within 30 days of becoming aware of the change. Furthermore, the regim**e requires annual returns to be filed, updating details, attaching financial sta**tements and providing details of new settlors and beneficiaries who receive a distribution from the trust. Where a New Zealand resident trustee fails to comply with their obligations they may cease to receive the tax exemption for foreign sourced income and may be subject to prosecution. The reason for this new regime was responding to the publications by international bodies and media reports which identified foreign trusts as being misused in criminal schemes. In order to address the risks, authorities took measures to enhance oversight of those entities.

16. Almost 20% of jurisdictions responding indicated that trusts of any kind are not allowed in the jurisdiction. Of those 12 jurisdictions, five are identified by either an OECD Global Forum Peer Review Report or other open source information as having a legal framework in place that specifically allows for legal arrangements. This raises several further questions, including the need to clarify what is meant when jurisdictions say that trusts are "not allowed" and exploring the potential reasons why tax authorities and AML/CFT authorities from the same jurisdiction might have a different understanding of the answer to that question.

17. As noted, very little information was provided regarding specific legal requirements to form trusts. This issue could be reviewed in more depth to consider whether any conclusions may be drawn as to best practices. In the information that was provided, some of the approaches to trust formation may potentially help to address common challenges in implementing effective measures to prevent the misuse of legal arrangements. These approaches could be reviewed in more depth, as a basis for more detailed description and analysis in the final Horizontal Study. These include in particular registration of trusts when certain criteria are met; Jersey's approach to imposing beneficial ownership obligations on trustees; and the need to clarify what is meant when jurisdictions say that trusts are "not allowed" and issues related thereto.

Question 3: What are the legal requirements for maintenance of legal persons and arrangements and how is compliance with those requirements monitored?

18. Maintenance of legal persons and arrangements, i.e. requirements for annual returns, accounts, reporting changes in control or ownership, etc., is important to ensuring that basic and beneficial ownership information remains accurate and up-to-date. Information on monitoring compliance was originally sought as part of first questionnaire (question 2(e)). However, little information specific to this issue was received. In February 2017, the FATF expanded the scope of this project to seek information on the legal requirements for maintenance of legal persons and arrangements, as well as the systems in place for monitoring compliance.

19. Unfortunately, a gap in the information on these issues still exists. In 53% of responses received, no information was provided regarding requirements for maintenance of legal persons. For maintenance of legal arrangements, no information was provided in 46% of responses. Likewise, the majority of responses received (64%) did not provide any information on monitoring compliance with maintenance requirements. Nevertheless, a third round of information gathering would delay this study excessively, so we have sought to reach conclusions based on the incomplete responses received. This does mean the conclusions on this issue are less well-evidenced than on other questions. In the paragraphs that follow, statistics reflect only the responses that provided relevant information. Also, some jurisdictions may impose more than one of the following measures; the categories are not mutually exclusive.

Legal Persons

20. The most common requirement of maintenance of legal persons is filing of annual returns (other than tax returns), certification or accounts. This requirement

applies in 53%of responses received (17 of 32). Notification of changes is the next most common at 37.5% (12 of 32). In 1% of responses (3 of 32), jurisdictions indicated that there are no requirements for maintenance of legal persons other than those imposed by any applicable AML/CDD obligations.

Legal Arrangements

21. In the case of legal arrangements, other than those to which common law obligations apply, there seem to be either no requirements or minimal requirements for maintenance. Only 9 of 23 responding jurisdictions impose any maintenance requirement for legal arrangements. Three of those require notification of changes in beneficial ownership or control. It is more often the case (in 14 of 23 jurisdictions) that there is no maintenance requirement at all. Based on these figures, availability of accurate and up-to-date information on legal arrangements depends almost entirely on the gatekeepers and non-professional trustees (or equivalent), with little or no role for public-sector registries. To the extent that gatekeepers are involved in the formation of legal arrangements, this finding underscores the importance of effective supervision to ensure compliance with CDD obligations.

Ongoing Monitoring of Compliance with Maintenance Requirements

22. Twenty-five jurisdictions provided information regarding mechanisms to monitor compliance with requirements to maintain legal persons or arrangements. Among these jurisdictions, the most common mechanism for ongoing monitoring of compliance with those requirements is oversight by the registry. Some registries have automated systems to monitor deadlines for filing annual returns or certifications. In other cases, registries cross-check their information with data held by other authorities (e.g. with tax authorities) to ensure veracity. Finally, some registries conduct sample testing or targeted audits to verify the accuracy of information on selected legal persons (or arrangements). Such mechanisms are reported by 40% of jurisdictions responding to this question (10 of 25). Only slightly fewer, 9 of 25, report monitoring by the AML supervisor or prudential regulator as an element of compliance inspections. However, 24% of jurisdictions responding to this question report they do not monitor for compliance at all.

Box 7. Belgium's beneficial ownership registry

To address these and other issues, Belgium is implementing a beneficial ownership registry, which is expected to be operational by 2018. When this registry is in place, there will be two types of automated controls: one will cross check "obligated entities" against the entities that actually provide beneficial ownership information; the other will cross check the beneficial ownership database against other government databases (primarily within the Ministry of Finance) to verify data quality. These cross checking systems will be monitored by a dedicated data miner and compliance will be enforced by a special unit of the Treasury.

23. According to information gathered for this Study, ten of the responding jurisdictions (15.6%) either have, or will have by the end of 2018, a beneficial ownership registry system.

24. Although the information is incomplete, the responses provided indicate serious weaknesses in measures designed to ensure that basic and beneficial ownership information remains accurate and up-to-date.

Question 4: Describe how agencies responsible for AML/CFT supervision of gatekeepers (whether government agency or SRB) assess compliance with beneficial ownership obligations.

25. There is insufficient information - either from the questionnaire responses or from mutual evaluation reports - to set out a general picture of how authorities or SRBs are assessing compliance with these specific obligations. It is possible, nevertheless, to describe certain common elements that might not, however, be present in every case. In most cases, the supervision combines both desk-based reviews and on-site inspections. Desk-based reviews involve analysis of annual independent audit reports and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identify the gatekeeper responsible for the filing. On-site inspections involve reviewing internal policies, controls and procedures, gatekeeper's own risk assessments, spot checking CDD documents and supporting evidence, sample testing of reporting obligations. Some national supervisors, as well as SRBs, mandate independent auditors to perform on-site inspections on their behalf.

26. Delegations could consider whether this is an issue on which more information is needed (e.g. in the course of any further projects following the Horizontal Study, or as part of a risk-based approach(RBA) guidance for gatekeeper professions).

Question 5: How are the businesses or professions engaged in the formation and/or maintenance of legal persons or legal arrangements regulated and supervised?

27. Pursuant to Recommendation (R.)28, the categories of DNFBPs who act as gatekeepers should be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In other words, they should be subject to effective supervision. This question was meant to elicit information on the types of supervisory regimes in place for gatekeepers and the roles played by those supervisors. The most startling finding is that 17% of jurisdictions that responded do not impose upon their gatekeepers any AML obligations or AML supervision whatsoever, despite this being a requirement of R.22, R.23 and R.28. In some cases, such as the US and Canada, this is the result of resistance to regulation from the relevant sectors or professions (e.g. to prevent the enactment of laws or regulations which would impose such obligations, or to mount constitutional

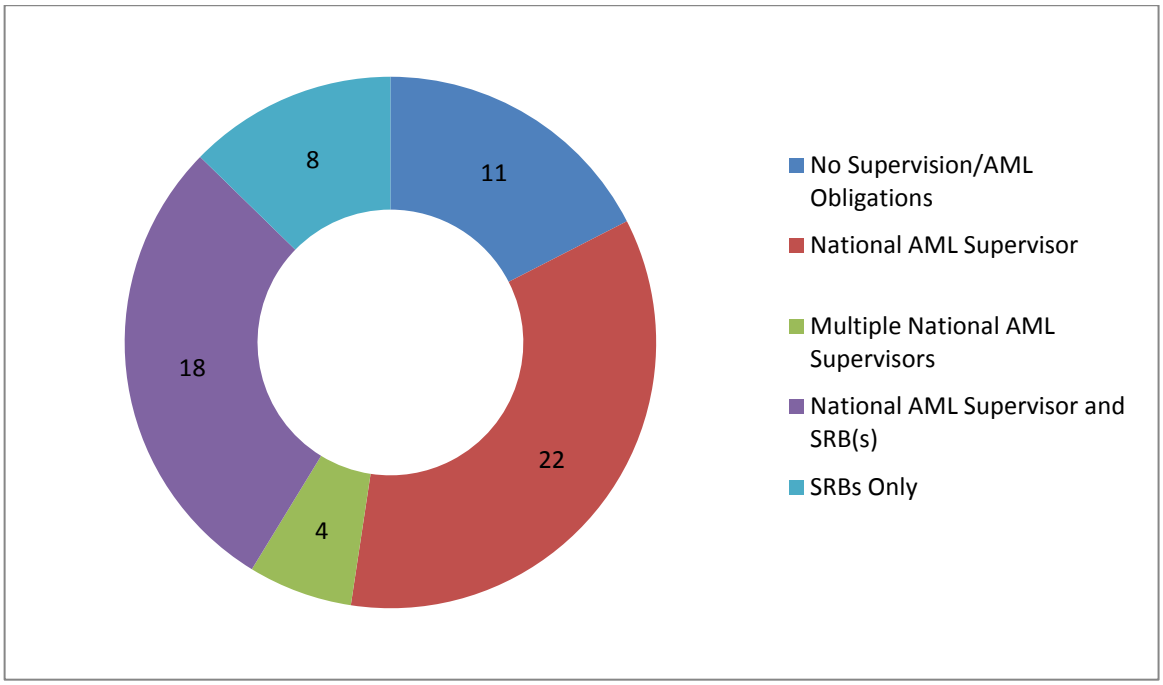
17% of jurisdictions that responded do not impose upon their gatekeepers any AML obligations or AML supervision whatsoever, despite this being a requirement of R.22, R.23 and R.28

challenges to such laws). In other cases, it may represent an "unfinished" aspect of the AML/CFT system which has not yet been implemented.

28. The information provided by members who do impose supervision describes a variety of arrangements for supervision of gatekeepers. Although there are variations in each category and unique elements to each jurisdiction's system, the descriptions could be divided into the following four general categories:

- national AML supervisor
- multiple national AML supervisors
- a national supervisor for one or more gatekeeping sector and one or more Self-regulating bodies (SRBs) for others
- SRBs only for all gatekeepers.

Figure 1. Gatekeeper Supervision Models
Breakdown of responses by jurisdictions participating in the survey



National AML Supervisor

29. In 42% of the jurisdictions that responded (22 of 64), there is a single authority for supervision of AML/CFT obligations. These authorities are often a Central Bank or Monetary Authority, Financial intelligence unit (FIU), or Financial Services Commission. The majority of jurisdictions that report such a regime, (12 of 22) are considered by the IMF to be "offshore financial centres".

30. Interestingly, 77% of jurisdictions using this supervisory model (17 of 22) reported cases of supervision or enforcement - the highest level of any other supervisory model. This fact, combined with the high number of offshore financial centres represented in this category is consistent with the findings of the Trust and

Company Service Provider Project conducted in connection with the book The Puppet Masters. This project entailed two audit studies involving the solicitation of offers for shell companies from a range of trusts and company service providers (TCSPs). The data were supplemented with in-depth interviews conducted with TCSPs. This approach was designed to test regulatory compliance in various jurisdictions. The project revealed that 94% of responses provided by gatekeepers in international financial centres, or tax havens, were compliant with the relevant AML/CFT framework, including collection of CDD information and refusal of suspicious business. Only 25.5% of gatekeepers in OECD countries provided compliant responses.

Multiple National Supervisors

31. In these jurisdictions, supervision of gatekeeper sectors is divided among government agencies such as FIUs, Central Banks, and Financial Services Authorities. The relatively small group (at 6% of respondents) makes it hard to conclude whether the fact that only two of the four jurisdictions report any enforcement action is a substantial concern. Nevertheless, the question of domestic co-operation where there are multiple government agencies tasked with AML supervision and presents an issue could be reviewed in more depth.

National supervisor and one or more SRBs

32. In 29% of participating jurisdictions (18 of 64), AML supervision of gatekeeper professions is divided between a government agency one or more self-regulating bodies (SRBs). In this supervisory model, 61% of jurisdictions (11 of 18) do not report any supervisory or enforcement action.

SRBs only for all gatekeepers

33. In this supervisory model, there is no national authority for AML oversight of gatekeepers – all the gatekeeper sectors are supervised by SRBs. Jurisdictions reporting this supervisory model comprise 13% of the sample. Five of the eight jurisdictions in this category (63%) do not report any supervision or enforcement action.

Supervision by SRBs

34. In the 26 jurisdictions where SRBs are tasked with supervision of AML/CFT obligations, lawyers are supervised only by SRBs in every jurisdiction but one. In 16 of those 26 jurisdictions (64%), no enforcement actions were reported. Seven jurisdictions reported active supervision of lawyers by an SRB.

35. For those jurisdictions, where gatekeepers are supervised by SRBs, no discernible patterns could be identified with regard to how this supervision is performed, due to a wide variety of approaches. It is even more difficult to draw conclusions which approach turns out to be more effective without a proper assessment. It is possible, however, to provide some general observations:

- There is a lack of consistent approach to supervision when different types of professional intermediaries are supervised by different bodies even if these intermediaries are performing essentially similar functions (e.g. company

formation). In other words, supervisory approach is often based on what type of profession intermediaries belong to, rather on what type of operations they perform in practice. Although many jurisdictions established various forums which facilitate co-operation and risk awareness among SRBs and competent authorities (especially FIUs), this does not seem to lead to coherent approach in supervision.

- Most of the SRBs especially those that cover lawyers and notaries are independent and do not seem to be subject to supervision/monitoring by a competent authority (as noted in the definition of "Supervisors" in the FATF Glossary), however in some cases competent authorities have a role, e.g. in appointing employees. There are two jurisdictions where SRBs are under direct supervision of competent authorities, and one jurisdiction where SRB is legally a governmental body. Another jurisdiction is in the process of creating of an umbrella organisation to oversee and facilitate activities of SRBs.

Box 8. Switzerland's national oversight of SRBs

An example where SRBs are supervised by a single national AML/CFT supervisor was provided by Switzerland. The legislator has mandated responsibility to the SRBs for AML/CFT supervision and FINMA (national supervisor) is tasked with supervising implementation. SRBs are structures which must be recognised by FINMA. This requires that they issue regulations (approved by FINMA) specifying the due diligence obligations with which their affiliates must comply, that they oversee compliance with these rules and that they ensure that the persons and bodies they instruct to carry out controls are independent and professionally qualified. If an SRB fails to meet with these conditions, FINMA can issue a warning and then withdraw its recognition.

36. Resources available to SRBs for inspections are limited. There are different models to deal with that: eight SRBs indicated that they hire independent experts with appropriate professional background who work solely for the SRB, two SRB rely on the staff of the peer members to supervise each other, three SRBs outsource their inspection functions to established auditing companies, and there might be combinations of the above;

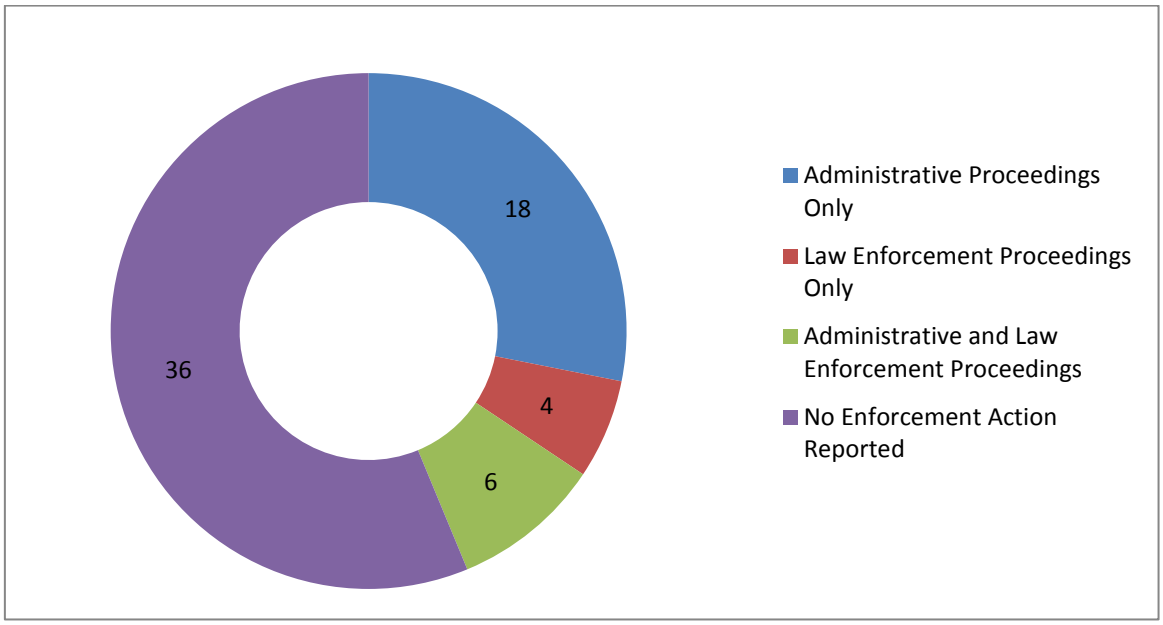
- Seven SRBs take proactive approach with regard to identifying breaches of compliance (i.e. during the on-site, and not after a complaint or a law enforcement investigation), however, that seems to be related to overall obligations, rather than those related to AML/CFT, or BO in particular.
- Application of RBA with regard to professional intermediaries is not widespread, and even in that case it is not always based on ML/TF risk factors. One jurisdiction indicated that all lawyers and notaries undergo an inspection on an annual basis, and auditors at least on a 6-years basis.

- Supervisory actions are very rare (as highlighted below), although most SRBs have the appropriate tools at their disposal (warnings, monetary penalties, disqualifications).

Question 6: Cases of supervisory and enforcement actions.

Figure 2. Enforcement Models

Breakdown of responses by jurisdictions participating in the survey



37. This question was meant to elicit information regarding the approach to oversight taken in each jurisdiction – whether beneficial ownership obligations are enforced by administrative supervisory action, or by law enforcement authorities. It was hoped that, upon review of this information, some conclusions might be drawn as to best practices, but the information provided is not sufficient for that purpose. Nonetheless, some emerging issues may be considered for further targeted information gathering.

38. No supervisory or enforcement actions were reported in 56% of responding jurisdictions. In three jurisdictions, this is attributed to newly enacted legislation that had not yet been implemented. Some jurisdictions specified that AML enforcement action had been taken, but none specific to beneficial ownership obligations. As noted previously, 17% of respondents do not impose upon their gatekeepers any AML obligations or AML supervision. As such, there could be no enforcement action to report. Other jurisdictions may have found it difficult to provide meaningful information in the questionnaire format.

39. Among the responses that did provide information on enforcement mechanisms, the most commonly reported is administrative enforcement taken by AML supervisors. Eighteen of the 28 jurisdictions reporting enforcement action (64%) rely on supervisors to enforce beneficial ownership requirements. In many cases, information provided includes sanitized case studies.

Box 9. BVI's list of sanctions imposed

In the case of the British Virgin Islands (BVI), a table was provided which listing examples of AML/CFT breaches related to beneficial ownership and the sanctions imposed – administrative penalties ranging from USD 440 000 to USD 5 000. The BVI also included a link to the supervisor's website, where a comprehensive listing of enforcement actions and sanctions applied could be accessed by any member of the public.

Box 10. Jersey's FSC and Registry

Another interesting sample of enforcement actions was provided by Jersey, where both the AML supervisor and the Registry perform complementary functions. The Jersey Financial Services Commission (JFSC) reports using enforcement tools such as formal remediation plans with regular monitoring and reporting by the TCSP; issuing directions to safeguard assets, prevent the take on of new business or transfer of existing business, appointing independent co-signatories to review and approve certain business activities and transactions. Jersey also reports using its supervisory powers to issue public statements and ban individuals from working in the financial services industry. The Companies Registry will not incorporate or register an entity if it does not have sufficient information. Applications are placed on hold until such time as information is provided. Failure to provide information is noted and this information is shared by the Companies Registry with the supervision and enforcement units of the JFSC.

40. In ten of the 28 jurisdictions that reported enforcement action, law enforcement proceedings may be used to enforce beneficial ownership requirements. In four of the ten jurisdictions, law enforcement proceedings are the only available remedy; in the other six jurisdictions, authorities may take administrative or law enforcement proceedings.

Box 11. Liechtenstein and Croatia

In Liechtenstein and Croatia, the AML supervisor initiates legal proceedings when weaknesses are identified during compliance inspections. In Liechtenstein, the AML supervisor identified weaknesses in establishing and corroborating the source of wealth of the beneficial owner and the source of funds held by the legal person or arrangement in question and brought the matter to the attention of the courts. In some instances, monetary fines were imposed by the court upon the responsible senior management member. In Croatia, the AML supervisor filed misdemeanour proceedings for violation of beneficial ownership, CDD, and risk assessment obligations.

Box 12. Latvia

Latvia reports that, in the period from 2013 to 2015, five criminal cases were initiated on grounds of non-provision of information and provision of false information regarding ownership of resources and the true beneficiary. Of these five cases, two have been submitted for prosecution and one case is under review by the court. No information was provided regarding the outcome of these cases.

Box 13. Spain and the US

Information provided by Spain and the US describes cases where police followed illicit financial flows to gatekeepers who were complicit in setting up networks of shell companies to launder proceeds of drug trafficking, political corruption, fraud, and tax evasion.

41. Although the sample is quite small, there seems to be a pattern in the way law enforcement proceedings are taken. Some jurisdictions have AML supervisors who initiate court proceedings to penalize weaknesses found during compliance inspections. Other jurisdictions, like Spain and the US, do not use criminal proceedings to enforce preventative measures like beneficial ownership obligations. Rather, legal proceedings are limited to cases of complicit actors actively engaged in money laundering.

42. Some of the approaches to enforcement of beneficial ownership obligations noted above are interesting and may potentially help to address common challenges in implementing effective measures to prevent the misuse of legal persons. These could be reviewed in more depth, as a basis for more detailed description and analysis in the final Horizontal Study. These include in particular the exercise of administrative supervisory powers and its impact on compliance; Jersey's approach of using both the AML Supervisor and Companies Registry to enforce beneficial ownership obligations; and the role of law enforcement in enforcing preventative measures. The lack of reported information on enforcement gives rise to questions that should also be considered for further information gathering.

ANNEX C. CASE SUMMARIES

Case Study 1 - Argentina	
A complex corporate structure, with Company G 95% owned by Mr. A and 5% by Mr. B. Company G purchased a power generator from Company K, owned by Company R in the Cayman Islands. Company R was linked to Panamanian Foundation P, which had Mr. A and his spouse as beneficiaries. Company G leased the generator to Company E, receiving amounts cleared by Company L. The funds were drawn against Company K's bank account, and Company G made payments to K to settle a debt. The funds were credited to the accounts of Companies S, T and R. The simulation of commercial operations introduced funds of dubious origin to the financial system, hiding the true beneficiary.	
Indicators	• Declared income which is inconsistent with their assets, transactions or lifestyle • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement regularly sends money to low-tax jurisdictions or international trade or finance centres • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Financial activities and transactions inconsistent with the corporate profile • False invoices created for services not carried out • Falsified paper trail • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Loans are received from private third parties without any supporting loan agreements, collateral or regular interest repayments • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 2 - Australia	
An Australian drug syndicate used multiple money laundering methods to launder more than AUD1 million worth of proceeds of crime. Trust accounts, a "front" company, high-value goods and real estate were used to launder the profits from cannabis sales. The syndicate also misused the services of two "professional facilitators" (an accountant and solicitor) to facilitate its criminal activity. The syndicate made significant profits by purchasing bulk amounts of cannabis in one state and then selling the drugs in another state. As a cover for its illicit activities, the syndicate established what appeared to be a transport company. The syndicate purchased a truck and rented a warehouse in the name of the company and used these to traffic the cannabis interstate.	
Indicators	• No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or a withdrawal, which is anomalous, or inconsistent with the company's profile • Transaction involves a professional intermediary without due cause or apparent justification • Transaction involves the use of multiple large cash payments to pay down a loan or mortgage

Case Study 3 – Australia	
Managers at a university and directors of construction companies were complicit in a fraudulent invoice scheme. The managers approved inflated invoices for maintenance work to be carried out by the construction companies, as well as invoices for work that was never undertaken. The fraud profits were used to purchase racehorses and property. The managers at the university were repaid with kickbacks or direct shares in racehorses. Accounting firms, which were undertaking international transfers on behalf of the suspects, sent money to many countries, including New Zealand, Canada, Hong Kong and the US. A large proportion of the funds were sent to companies linked to the horse racing industry. The accounting firms also received international transfers from various overseas entities that were similar in value to the amounts the firms had sent overseas initially. The majority of these transfers originated from Hong Kong. Authorities suspected that the accounting firms were laundering the funds on behalf of the suspects as part of a professional money laundering syndicate.	
Indicators	• Financial activities and transactions inconsistent with their customer profile • Declared income which is inconsistent with their assets, transactions or lifestyle

	• Transaction appears cyclical • Transaction involves a professional intermediary without due cause or apparent justification

Case Study 4 – Australia	
Suspect declared minimal income to the tax office while living a luxurious lifestyle, and was identified as having disguised income derived from securities trading. The criminal investigation revealed that the suspect created several international companies which, on paper, were owned by a stichting (a foundation in which the identity of the beneficial owner is not yet publicly available) in the Netherlands. The suspect sold securities below market value to the international companies to reduce Australian tax liability. The suspect later arranged for the shares to be sold via his international companies at market value. The proceeds of the sales were returned to the suspect in Australia disguised as loans from international companies. Over two years, the suspect arranged 15 international funds transfer to send funds from international companies under his control based in Switzerland to his Australia-based company.	
Indicators	• Financial activities and transactions inconsistent with their customer profile • Declared income which is inconsistent with their assets, transactions or lifestyle • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Loans are received from private third parties without any supporting loan agreements, collateral or regular interest repayments • Funds are unusual in the context of the client or customer's profile • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 5 – Australia
The "Round Robin" scheme aimed to make funds movements appear as payments to other parties while, in reality, the funds ultimately returned to the original beneficiary. The suspects transferred funds from their companies' accounts to the bank accounts of companies in New Zealand. The New Zealand companies and bank accounts were controlled by a Vanuatu-based accountant, who was a signatory to the bank accounts. The payments were falsely described in the companies' records as "management and consultancy fees," with false invoices that matched amounts paid to the New Zealand bank accounts. No evidence was available to show that any consulting work had been carried out. The false expense payments were claimed as deductible expenses in the tax returns of

companies X, Y and Z, thereby fraudulently reducing the companies' taxable income and taxes owed. The accountant then transferred the funds under the guise of international "loans" through a series of round robin international transactions, through accounts held in the name of companies owned and operated by the accountant. The accountant transferred the funds into the personal bank accounts of the suspects in Australia. The funds were transferred via an overseas company controlled by the accountant, separate to the companies in New Zealand that received the funds originally. In order to disguise the funds being transferred back into Australia as loans, false documents were created purporting to be international loan agreements with a foreign lender, which are not assessed as income and have no tax liability.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • False invoices created for services not carried out • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Legal Person pays no taxes, superannuation, retirement fund contributions or social benefits • Loans are received from private third parties without any supporting loan agreements, collateral or regular interest repayments • Transaction appears cyclical • Transaction involves a professional intermediary without due cause or apparent justification • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 6 – Australia

Investigating authorities identified that suspect A operated an import business in Australia and was a participant in a tax evasion scheme operated by an accountant. Suspect A and his wife were directors and shareholders of an Australian company (company 1). Suspect A was also a director and shareholder of another Australian company (company 2). An associate of suspect A was the co-director of company 2. Authorities identified that the accountant controlled company 3, which was registered in Hong Kong and operated a bank account in Australia.

This company was used to issue false invoices to companies 1 and 2. Over a five-and-a-half-year period company 3 issued false invoices to companies 1 and 2 for supposed "brokering services." Suspect A paid the false invoices, which totalled more than AUD2 million, by directing companies 1 and 2 to pay company 3. The

	funds paid to company 3, less the accountant's 10% fee, were returned to suspect A and individuals associated with him.
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • False invoices created for services not carried out • Falsified paper trail • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Simple banking relationships are established using professional intermediaries • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Client is both the ordering and beneficiary customer for multiple international funds transfers • Loans are received from private third parties without any supporting loan agreements, collateral or regular interest repayments • Transaction appears cyclical • Transaction involves the two-way transfer of funds between a client and a professional intermediary for similar sums of money • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners • Transaction involves a professional intermediary without due cause or apparent justification • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 7 – Australia
Individuals A and B were family members who owned and controlled a group of Australia-based companies that undertook motor vehicle repairs and sold automotive products. Individuals A and B received advice from an accountant about the purported benefits of international superannuation funds, and as a result Individual A established a superannuation fund in Samoa with a Samoa-based company acting as fund trustee. Company 1, controlled by Individuals A and B, contributed AUD 200 000 to the fund, which was then returned back to Company 1 disguised as a loan. The superannuation contribution was claimed as a tax deduction. Individuals A and B also entered into a secondary loan agreement on behalf of company 1 with the Samoa-based private bank. This second loan arrangement remained in place for more than 10 years and was later transferred

to other companies in the group. Companies controlled by Individuals A and B made "interest payments" by way of international funds transfer, which were then returned back to the companies as further loans. To further complicate the loan arrangement, another Australian organisation was introduced to the transaction activity. This organisation was unrelated to the main group of companies and was described as a charitable organisation. The organisation facilitated the transfer of funds between the bank's New Zealand subsidiary and the Australian group of companies.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement regularly sends money to low-tax jurisdictions or international trade or finance centres • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Focused on aggressive tax minimisation strategies • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Client is both the ordering and beneficiary customer for multiple international funds transfers • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Loans are received from private third parties without any supporting loan agreements, collateral or regular interest repayments • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Transaction appears cyclical • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 8 – Australia
Illegal international arrangements are an established way of evading tax, laundering funds and concealing beneficial ownership. Project Wickenby identified the use of false invoices and loans in illegal international arrangements. The scheme involved an Australian company (company A) which enters into an agreement with a tax scheme promoter based in a tax secrecy jurisdiction (country 1). The promoter benefits from the confidentiality and privacy offered in the tax secrecy jurisdiction. The tax scheme promoter owns and/or controls two international companies (company B and C). Control may involve the use of a trust

or the use of third parties; for example, a relative or associate may act as the director of the international companies. Company B provides consultancy and/or management services and is incorporated in country 2. Company C provides a financial service (as a lender of money, for example) and is incorporated in country. Companies B and C hold bank accounts in country 4. The promoter controls and operates these accounts.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement regularly sends money to low-tax jurisdictions or international trade or finance centres • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • False invoices created for services not carried out • Falsified paper trail • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Loans are received from private third parties without any supporting loan agreements, collateral or regular interest repayments • Transaction appears cyclical • Transaction involves a professional intermediary without due cause or apparent justification • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 9 – Belgium	
International transfer from the account of a foreign foundation to an account in Belgium of one of the ultimate beneficial owners of the foundation, followed by attempt to repatriate a significant amount. Limited tax adjustment declaration and remaining uncertainty about the origin of the assets gave rise to a suspicion of fiscal fraud, evasion of inheritance tax and attempted money laundering.	
Indicators	• Client is reluctant or unable to explain their source of wealth/funds • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Focused on aggressive tax minimisation strategies • Correct documents not filed with the tax authority

	• Falsified paper trail • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 10 – Belgium	
Natural persons repatriated to Belgium funds originating from accounts in a foreign jurisdiction in the name of two Stiftung and an AG corporation with address in that jurisdiction and a Ltd. corporation with its address in another jurisdiction, as well as in the name of trustees of a trust in that jurisdiction. The repatriated funds were used for various payments and purchases. Inadequate justification of the source of funds led to a suspicion of serious fiscal fraud.	
Indicators	• Client is reluctant or unable to explain their source of wealth/funds • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Focused on aggressive tax minimisation strategies • Correct documents not filed with the tax authority • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 11 – Bolivia	
Multiple money orders originated from the same geographic area in Spain, sent by individuals and corporations to straw men nominees (often related) in the same geographic area in Bolivia. The purpose of the transfers was declared as the construction and purchase of properties through a local company. Funds were also sent to USD accounts in two financial institutions held by a money exchange house. The MSB's bank accounts also received international money orders from two companies with the same UK address. The straw men nominees and the MSB's bank accounts transferred money to a separate group of individuals, which included a partner in the MSB business. These individuals deposited the funds in case into local currency bank accounts before sending the funds on as electronic transfers to individuals residing in the Brazil-Bolivia border area.	
Indicators	• Registered at an address that is also listed against numerous other companies or legal arrangements • Legal person or arrangement conducts a large number of transactions with a small number of recipients • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • No real business activities undertaken • Legal Person pays no taxes, superannuation, retirement fund contributions or

	social benefits • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile • Funds are unusual in the context of the client or customer's profile • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 12 - Canada	
A publicly-listed company's common stock was part of a fraud affecting the market price of their security that involved numerous stock promoters in Canada and elsewhere who manipulated the stock price by making misleading representations and/or omissions. It is alleged that the proceeds, of up to USD 20 million, were then laundered through offshore banks. The US SEC provided information that established the flow of shares from Serbian nominees, through intermediary international business companies. These shares were effectively in bearer form having been signed over by the seed shareholders at the time of issue. An opinion letter was written by a US based securities lawyer that allowed these shares to trade and a subsequent reverse merger was completed immediately after the free-trading shares were anonymised and immediately before a prolific series of paid promotions were carried out. Canadian investigators were unable to prove and confirm identities behind real owners of the international business companies, which held control of the free trading shares. Additional investigative challenges included the inability to access information from offshore jurisdictions with regards to pertinent documentation used to obscure beneficial ownership of intermediary international business companies. Canadian investigators encountered refusal from Serbian nominees to co-operate and provide witness statements on several occasions.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Nominee owners and directors • Transaction involves the transfer of bearer shares in an off-market sale

Case Study 13 – Cayman Islands
Mr. A established a Cayman Islands revocable trust, with himself as settlor and a local TCSP acting as trustee. Mr. A also arranged for the incorporation of a Cayman Islands company known as 'Company B', with the local TCSP also acting as the

	registered office. The TCSP became aware of allegations relating to Mr. A and his involvement in an oil and gas contract scam which also involved members of a foreign government. Over a two-year period, the TCSP reported that the trust and underlying company had received numerous transfers of funds and property from what was now deemed to be questionable sources, which in turn heightened its suspicions and prompted an STR. An analysis of the trust accounts revealed outgoing funds to individuals named in numerous media reports who allegedly took part in the kickback scandal. In response a request, the foreign jurisdiction's confirmed that Mr. A was being investigated for money laundering and corruption of government officials.
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Under investigation or have known connections with criminals • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Funds are unusual in the context of the client or customer's profile

Case Study 14 – Cayman Islands	
	The managing director of an overseas company issued a prospectus which contained misleading and false information within the company's annual report. He overstated the company's group revenue by 275%. This information was provided to that country's securities commission as part of the company's proposal for listing on their stock exchange. The managing director established a revocable trust and underlying company in the Cayman Islands. He then opened an overseas bank account in the name of the Cayman Islands company for which he held the Power of Attorney, allowing him to trade in the account. This structure was devised to hide the managing director's trading in the overseas company and to hide assets derived from his illegal activities. The Cayman Islands company held over USD 1 million in this bank account. The Financial Reporting Authority (FRA) made an onward disclosure to the FIU of the foreign national's home country. The foreign national has been charged in his home country with three counts of providing misleading and false information.
Indicators	• Falsified paper trail • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Bank accounts in multiple international jurisdictions without good reason • Repeat transaction, and the executing customer is a signatory to the account, but is not listed as having a controlling interest in the company or assets

Case Study 15 – China	
The suspect used the identity of his close relatives and company employees to establish eight shell companies while maintaining actual control over these companies. He fabricated false documents and sales contracts to fraudulently obtain financing from six banks. Additionally, the suspect defrauded 3 state-owned enterprises through financing and false trading by utilizing illegal financial institutions such as underground banks. The suspect transferred the money into his private accounts for personal use and the repayment of personal debt.	
Indicators	• False invoices created for services not carried out • Falsified paper trail • Family members with no role or involvement in running the business are listed as beneficial owners of legal persons or arrangements • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Transaction is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners

Case Study 16 – China	
Suspect A used his influence as the manager of an enterprise to help Company X to win a tender bid and receive dividends in proportion to capital stock held. Company X was owned by Suspect A, B, and C. After Company X won the tender bid, Suspect B took over control of the company. Suspect A asked Suspect B to open an offshore account for him in Hong Kong, and transfer funds under the guise of a housing purchase. The offshore companies and accounts were opened in the name of Suspect B's wife and sisters, respectively. After depositing a portion of the funds, the accounts were transferred to Suspect A's control. Suspect A then fled and Suspect B asked the vice president of Company X to transfer funds to the Hong Kong accounts held in his family members' names. The money was then transferred back to China through underground banks and distributed to five new domestic bank accounts in the name of an employee of Company X.	
Indicators	• Director or controlling shareholder(s) cannot be located or contacted • Legal person or arrangement regularly sends money to low-tax jurisdictions

	or international trade or finance centres or international trade or finance centres • Multiple bank accounts without good reason • Family members with no role or involvement in running the business are listed as beneficial owners of legal persons or arrangements • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Transaction is a business transaction that involves family members of one or more of the parties without a legitimate business rationale • Transaction appears cyclical • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre or international trade or finance centre

Case Study 17 – China	
A low-ranking official A, who worked for a local government department, took advantage of his position to obtain privileges and contracts for CC Company, and received bribery payments from the manager of CC Company in return. A also arranged for his cousin to work for CC Company and for his sister and wife to keep the company books. A positioned himself as a dormant shareholder, claiming money from the principal as profit sharing. A also installed his daughter as a shareholder of CC Company without equity.	
Indicators	• Director or controlling shareholder(s) does not appear to have an activity role in the company • Family members with no role or involvement in running the business are listed as beneficial owners of legal persons or arrangements • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction is a business transaction that involves family members of one or more of the parties without a legitimate business rationale • Transaction involves the transfer of shares in an off-market sale

Case Study 18 – Croatia
Croatian Company A received funds from Company B (incorporated in a financial centre), which were used to invest in real estate on Croatian coast. The founder of

Company A was another Croatian company, the founders of which were citizens of Country D. The funds of foreign Citizen K (citizen of Country D) were suspected to originate from bribery in Country D, and were sent to the account of Company B, which then transferred funds as loan to the account of Company A. The ownership structure of Company A involved another Croatian company and 4 other citizens of Country D, but based on intelligence there is reason to suspect that beneficial owner of Company A is Citizen K.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification

Case Study 19 – Ecuador	
Public officials along with relatives and individuals connected to law firms created a series of companies in several countries for the purpose of receiving bribe payments. The bribe payments were effected through individuals with links to companies that provide goods and services to a public institution in the oil sector. To send the payments, and to hide the real beneficiaries of the transfers, the suppliers created companies in Panama, Hong Kong, British Virgin Islands, Bahamas, Uruguay, and the US.	
Indicators	• Client is reluctant or unable to explain their source of wealth/funds • Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement regularly sends money to low-tax jurisdictions or international trade or finance centres • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation • There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. • False invoices created for services not carried out • Employees of professional intermediary firms acting as nominee directors or shareholders • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense

	• Nominee owners and directors • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 20 – Egypt	
The scheme involved making investments in different fields through legal persons without clear economic purpose to launder funds obtained from the appropriation of public funds. It lasted 18 years and laundered EGP 300 million. It involved an Egyptian shareholding company and another company located abroad with unclear legal structure. The legal entity was managed by the primary suspect's sons, and the directors, shareholders and board of directors were nominees.	
Indicators	• There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors

Case Study 21 – Egypt	
The scheme involved real estate investment, the management of securities and portfolios investment and real estate marketing. Over the course of 5 years, the suspects received EGP 50 million for the purposes of real estate investment but stole the funds. Money was transferred and cash deposits made across eight legal persons with nominee shareholders and boards of directors, and one sole proprietorship.	
Indicators	• There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. • Nominee owners and directors • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile

Case Study 22 – Egypt
14 companies and 8 Egyptian persons working in the tourism sector laundered EGP 42 million over the course of 3 years. The suspect used his official position to embezzle funds and invested the proceeds to top-up the capital of his companies before transferring the money abroad. The suspect's family members acted as

front people.	
Indicators	• Client is reluctant or unable to explain their source of wealth/funds • Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise

Case Study 23 – Egypt	
The scheme involved the reclamation of agriculture lands, trading, marketing and acting as agents for other brands, and trading in medical tools. It operated over the course of 15 years and involved four legal persons and 18 natural persons. EGP 17 million of funds originating from a foreign predicate offense were laundered by co-mingling in Egyptian joint-stock companies with the suspect's relatives used as front people. The shareholders and board members were nominees, and a lawyer was involved in the scheme.	
Indicators	• Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Nominee owners and directors • funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client.

Case Study 24 – Egypt	
A financial consultancy firm misappropriated investment funds. The funds were transferred using three companies to bank and securities accounts in overseas jurisdictions. Over the course of four years, the suspects laundered EGP 21 million, USD 4 million & EUR 68 thousand. The funds were collected by the firm for a declared purpose of investing them, yet they were actually misappropriated.	
Indicators	• There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. • funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client.

Case Study 25 – Egypt	
The scheme involved the misappropriation of a company's funds by one of its employees. The predicate offense took place in a foreign jurisdiction. The company operated in construction, real estate development and import-export activities in Egypt. The funds were laundered by co-mingling the proceeds of crime with the capital of 8 legal persons (partnerships and Egyptian joint-stock companies). The shareholders and some of the partners were nominees.	
Indicators	• Nominee owners and directors • funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client.

Case Study 26 – Egypt	
The accused created six British Virgin Island shell companies and used the bank accounts of these shell companies to launder the proceeds of crime of a total amount of more than EGP 1 billion. The predicate offence was "illegal earning". The six shell companies all had a nominee shareholder.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre • Nominee owners and directors.

Case Study 27 – Egypt	
The scheme laundered the proceeds of illegal forex exchange through two exchange houses over the course of 10 years. The Chairmen and boards of directors of both legal persons were professional nominees. EGP 70 million originated from the predicted offence were laundered through establishing companies.	
Indicators	• Nominee owners and directors including formal nominees

Case Study 28 – Europol
Complicit facilitators set up shell companies and bank accounts. Banks in two EU countries facilitated the formation of shell companies (in EU, Belize, BVI and Panama) and registered bank employees as fake directors. Those bank accounts were controlled via Internet banking by criminals. Independent agents acting as

company service providers registered and administered those companies. A variety of OCGs used this network, on some ad-hoc basis for specific periods of time.	
Indicators	• Under investigation or have known connections with criminals • Registered at an address that is also listed against numerous other companies or legal arrangements • Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Bank accounts in multiple international jurisdictions without good reason • Employees of professional intermediary firms acting as nominee directors or shareholders • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise

Case Study 29 – Europol	
An organised crime group linked to the "Camorra" was involved in the transport of large amounts of drugs to Italy. Individuals from the crime group performed transactions on behalf of others, moving funds through company and foundation bank accounts. Those middlemen operated multiple bank accounts, exploiting products such as loans and stock market trading. Trade-based money laundering was also used to conceal the criminal funds by buying/selling companies, vehicles and jewellery.	
Indicators	• Under investigation or have known connections with criminals • Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense

Case Study 30 – Europol
A non-EU organised crime group used offshore shell companies, controlled by various professional straw men, offering substantial loans with high interest rates and deferred payment loans and mortgages for property investments. Companies investing in Spain belonged to the same crime group.

Indicators	• Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason • Nominee owners and directors including formal nominees • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Loans are received from private third parties without any supporting loan agreements, collateral, or regular interest repayments

Case Study 31 - Fiji	
Mr. X used two shell companies to launder the money he had fraudulently obtained from his business partner Mr. Z. Mr. X set up a fake real estate company to facilitate the purchase and transferred the funds to another shell company and to his wife. The funds were then used to acquire property under their names.	
Indicators	• Legal person or arrangement receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification • False invoices created for services not carried out • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Transaction is a business transaction that involves family members of one or more of the parties without a legitimate business rationale

Case Study 32 – Fiji	
This case involved fraudulent activities conducted by Mr. X, an accountant at a Fijian resort. Mr. X altered the resort's cheques written to the resorts' creditors. A shell company was established to conceal the fraudulently converted funds. Some of the cheques that were fraudulently converted were altered and deposited into the bank account of the shell company. The remaining cheques were issued to other family members and associates of Mr. X. The laundered proceeds were used to purchase six motor vehicles, a private property and cash. The vehicles were registered under Mr. X's and others' names, whereas the property was registered under Mr. X's mother's name, and later transferred to one of his associates.	
Indicators	• Financial activities and transactions inconsistent with the corporate profile • Multiple bank accounts without good reason • Nominee owners and directors including informal nominees, such as children,

	spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Transaction is a business transaction that involves family members of one or more of the parties without a legitimate business rationale • Transaction is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile

Case Study 33 – Ghana	
A charity (Charity A) undertaking humanitarian work for orphans, war victims and disasters began operation in Ghana in 2016, but had been working with other partners 15 years. Charity A received three remittances totalling over USD 1 million from Charity B. The economic purpose of the funds was not indicated. Enhanced due diligence by the financial institution identified that Charity B was a wing of an UN-designated terrorist group.	
Indicators	• There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. • Designated persons or groups

Case Study 34 – Gibraltar	
Company X listed as a subsidiary of company Y which received funds from an energy company deal. Company Z (managed by a licensed TCSP) owned company X. The scheme involved two regulated TCSPs acting as nominee shareholders. The directors had also been provided by the TCSP, but resigned less than four years after incorporation. The underlying client had also been a director. The company secretary (also a licensed TCSP) incorporated and administered the company, and provided the registered office. The supervisor obtained information being sought by the LEA using formal powers and disclosed this under a statutory gateway as being necessary for the prevention and detection of crime.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Resignation and replacement of directors or key shareholders shortly after incorporation • Nominee owners and directors including formal nominees

Case Study 35 – Gibraltar	
Two companies used to present what was suspected to be misleading picture of the firm's true financial position. The scheme used nominee shareholders (licensed TCSPs). Corporate director used for one director, company secretary for both, as well as provision of registered office facilities.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Falsified records or counterfeited documentation • Nominee owners and directors including formal nominees

Case Study 36 – Guernsey	
During a two-year investigation (2014-2016), the US Commodity Futures Trading Commission (CFTC) launched an investigation into UK national Mr. X Doe for market manipulation. It came to the attention of Guernsey Financial Services Commission that a TCSP provider (TCSP B) administered a corporate structure for the benefit of Mr. X Doe. Over a five-year period Mr. X Doe made approximately GBP 32 million. The purported legitimate business was futures dealing. Prior to Guernsey TCSP B's involvement, it was administered by a Cayman Island Company. The Guernsey TCSP, which was licensed for AML/CFT, identified that Mr. X Doe was under investigation and co-operated with the Guernsey AML/CFT authorities.	
Indicators	• Under investigation or have known connections with criminals • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre

Case Study 37 – Guernsey	
Persons A and B were married residents of Guernsey, and purported to be TCSPs but were unregistered. Person A was the subject of an investigation by the IRS, while the TCSP's Client C was under investigation by the FBI. It was identified that Client C was operating a "boiler room" fraud. Investigations suggested that Person A was providing nominee directors for the shell companies used by Client C in execution of his fraud. The FBI identified that significant funds of Client C had moved through an account that Person A's company, Company D, held in Hong Kong. Company D was incorporated in Niue with Person A the sole registered Director and Person B the Secretary. Persons A and B were connected to organised crime groups via the "business facilities" they provided, including acting as nominee directors.	
Indicators	• Under investigation or have known connections with criminals • Prohibited from holding a directorship role in a company or operating a TCSP

	• Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Falsified paper trail • Nominee owners and directors including formal nominees • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 38 – Israel	
This scheme was used to hide funds from social engineering fraud and other criminal offenses. The cover story for the criminal offenses was international trade – funds from merchants in Europe and the US that were sending payments to suppliers in East Asia. The suspect, the owner of a registered MSB, operated a second, unregistered MSB. The suspect used several natural persons as his contact points in East Asia, who in turn contacted local TCSPs for the purpose of setting up international companies and opening bank accounts. Local straw-men were registered as the shareholders of the new international companies established for the scheme. In addition, shareholders were registered based on passports provided by the suspect's contact persons mentioned above. The registered addresses of the companies were in East Asia. Bank accounts were opened in the same East Asia countries where the offices were located. Some of the funds were transferred to Israel to an account opened by the suspect. More than 60 beneficiaries were declared to the bank as beneficiaries, in such a way that the bank had difficulty in establishing which transaction was made on behalf of which beneficiary. The funds were sent from the companies set up by the suspect but the receiving bank did not know that these companies were actually under the suspects' control.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement conducts a small number of high-value transactions with a small number of recipients • Legal person or arrangement receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification • Simple banking relationships are established using professional intermediaries • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Only a post-box address • Legal person does not have a physical presence

Case Study 39 – Israel	
This scheme was used to hide the proceeds of fraud conducted through foreign exchange and binary options trades. Local companies attracted foreign investors and presented themselves as legitimate foreign exchange and binary trading platforms. Private companies, Israeli representatives of foreign banks and law firms set up foreign companies abroad by contacting TCSPs located in international jurisdictions. The latter established shell companies in the international jurisdictions. The service provided by the foreign TCSPs also included opening bank accounts in favour of the shell companies in other countries. After the companies were established, the TCSPs were not involved in their management nor in any related activity. In some cases, the suspects used the companies as a vehicle to launder money and in other cases they sold the companies to third parties for a profit.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason • Simple banking relationships are established using professional intermediaries • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise

Case Study 40 – Israel	
This case involved a fraudulent tax scheme designed to evade paying tax generated from international trade and a ML infrastructure that was used to hide the illegally gained funds. The suspects used a TCSP to register and operate two international shell companies (Company A and Company B) to create the false appearance that the revenues from their international trading did not belong to the local Israeli company which they controlled, to avoid tax. The two companies traded with each other exclusively and did not have any other source of income. Company A (foreign shell company) transferred significant funds to company C (local company) using the cover of a "consulted fee"/ "service commission". Only this commission, which was less than half of the real income, was reported to the tax authority in Israel. Thus, ultimately, the suspects paid taxes only on a small part of their income.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Bank accounts in multiple international jurisdictions without good reason • Correct documents not filed with the tax authority • False invoices created for services not carried out

	• Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Corporation has no personnel • Transaction is a repeat transaction between parties over a contracted period of time • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners

Case Study 41 – Israel	
The scheme involved underground banking - the suspects provided money services such as check clearing, currency exchange, international transfers and loans. These activities of the "bank" and its customers were unregistered and concealed. The investigation showed that the "customers" of the "underground bank" provided illegally gained cash, then, depending on the type of service, the transfers were registered and declared as diamond export/import or the selling and buying of diamonds locally. The funds were laundered by the underground bank's "managers" through the guise of diamond trade using false declarations and fictitious export/import diamond documentation. The "customers" of the "underground bank" used the diamond dealers' accounts to transfer money without reporting it to the authorities. The total sums laundered amount to hundreds of millions of USD.	
Indicators	• Discrepancy between purchase and sales invoices • Falsified paper trail

Case Study 42 – Italy	
The *Nucleo Polizia* of Milan conducted a preventive seizure of funds traceable to a single family, which were held in the Channel Islands, for a total value of EUR 1.3 billion. The assets were concealed through a complex network of trusts. Multiple trust accounts were hiding the beneficiaries of assets consisting in public debt securities and cash. The investigation established that between 1996 and 2006 the subjects placed their assets in Dutch and Luxembourgian companies through complex corporate operations and by transferring them to different trusts in the Channel Islands. Subsequently, the funds were legally repatriated through a tax amnesty in December 2009. The investigation identified chartered accountants who had over time facilitated the concealing of funds through trusts with the aim of facilitating laundering and reinvestment.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction

	or international trade or financial centre • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense

Case Study 43 – Italy	
This case related to an investigation into a transnational criminal organisation active in money-laundering and that perpetrated crimes in Italy. It was triggered by STRs concerning financial flows from a company in the British Virgin Islands channelled through a Swiss bank and sent to an Italian legal person to be used for a refurbishment of a real estate unit which had a value of EUR 9 million. The investigation resulted in the charging of a chartered account for money laundering. The search of the individual's office resulted in the seizure of documents pertaining to a high number of off-shore vehicles which were established on behalf of wealthy national clients. The subsequent investigations led to the discovery that around EUR 800 million had been moved between Italy and international accounts.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre

Case Study 44 – Italy	
The Nucleo Polizia Tributaria of Milan conducted a money laundering inspection at a professional office providing "chartered accountants services", aimed at verifying compliance with money laundering regulations. The investigation was conducted mainly through a series of databases/registries and enabled to establish how a joint stock company active in the real estate sector, owned by two companies based in Cyprus and Austria, had made a considerable investment in Milan (approx. EUR 8 million). Two years after the buyer had not proceeded to complete the works as planned. A money laundering inspection was carried out against the professional office and it was found to be the custodian of the books of accounts as well as the domicile of the joint stock company previously targeted. A senior partner was found to be borrowing considerable funds via credit institutions from a company based in a high-risk jurisdiction.	
Indicators	• Legal person or arrangement incorporated/formed in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason

Case Study 45 – Italy	
An anti-money laundering inspection for compliance into a TCSP led to the investigation. The case involved the acquisition of a well-known Italian transport company. It involved a trustee mandated in the name of a foreign company with no specified ownership. Documents obtained showed that several files on trustee registrations indicated offenses committed by the legal representative. The TCSP served to screen the transfer of funds to Italy that were illegally generated and concealed abroad. The investigation into beneficial ownership of the foreign company helped to link investigated persons to considerable financial assets that were fraudulently transferred abroad and used to purchase the transport company.	
Indicators	• Client is reluctant or unable to explain the identity of the beneficial owner • Multiple bank accounts without good reason • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense

Case Study 46 – Italy	
A trust structure was setup for the son of Mr. X, a client of a UK law firm. The trust structure was set up to hold funds illegally diverted from an Italian company run by Mr. X. The scheme consisted of a BVI company owned by an Irish company. The BVI company, in turn, owned 100% of a Luxembourg company. The Luxembourg company would receive money from the Italian company from fictitious sales. The director of the Irish company was a partner of the same UK law firm. The director of the BVI company was another partner of the same UK Law Firm. A close associate of Mr. X had a power of attorney in the BVI company. The shares of the Irish company were held in trust for Mr. X's son (beneficial owner of the trust) by a TCSP in Jersey connected to the same UK law firm. Using such scheme there was no apparent link between the funds diverted from the Italian company and the beneficial owner of such funds. The only link was the trust.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Employees of professional intermediary firms acting as nominee directors or shareholders • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense. • Nominee owners and directors

Case Study 47 – Italy	
Mr. D and Mr. S were involved in the top management of two Italian hospital corporations: the SR Foundation and the SM Foundation. These foundations were carrying out commercial operations outside their normal course of business to facilitate the illegal transfer of money from the Foundations to Mr. D and Mr. S to pay bribes to Mr. F, a PEP. The illegal commercial operations were carried out through various foreign corporate vehicles, which were managed by a Swiss trust fiduciary. The suspects were charged with conspiracy, money laundering, corruption and embezzlement.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation • Financial activities and transactions inconsistent with the corporate profile • False invoices created for services not carried out • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense or which do not make commercial sense • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Transaction is a repeat transaction between parties over a contracted period of time • Transaction is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre or international trade or finance centre

Case Study 48 – Italy
A designated person was found to be in possession of assets and economic resources located in Italy. Bank records indicated the individual owned 100% of a Cyprus-based company and the tax register verified the date, place of birth and current tax residency in Italy. The Italian Official Register revealed the listed

individual owned 50% of a limited liability company based in Rome (whose corporate purpose is the purchase and construction of buildings and building complexes owned by the same company) through the aforementioned Cypriot company. The tax register revealed a 2012 tax return of the designated individual showing income from real estate, which exactly matched that of the Cypriot company, and a tax return for the Rome-based company showing a turnover of EUR 502 731 and taxable income totalling EUR 3 405. The designated individual owned shares or stakes in several companies based in Russia and Cyprus, including two banks and the mentioned Cypriot company. The designated individual, the Cypriot company and the Roman company were also found to own several properties located in various Italian provinces. As such, the designated individual was the holder of assets and economic resources in his own name or otherwise available through corporate vehicles that had been under freezing orders since 2014.	
Indicators	• Foreign nationals with no significant dealings in the country in which they are procuring professional or financial services • Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or finance centre • Focused on aggressive tax minimisation strategies • Designated persons or groups • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense or which do not make commercial sense • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client

Case Study 49 – Jersey	
The main fraudulent activity centred on a software business based in the suspect's home country. The business sold its intellectual property rights to an Irish company which in turn transferred them to a BVI company. The business then entered into license and distribution agreements with the BVI company, which enabled it to sell and distribute the software and accordingly it continued its business activities as before. The resulting license and distribution fees paid to the BVI company resulted in a significant reduction in its taxable income. All 3 entities were owned and controlled by same person ("X"). It is alleged that X operated a scheme whereby the company made fraudulent claims and omissions by claiming deductions resulting from "sham" license and distribution arrangements. X established a trust structure with underlying companies using a Jersey based financial service provider. It is alleged these entities were involved in the scheme as conduits for funds transfers or for holding assets derived from the scheme.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre

	• Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense. • Transaction involves licensing contracts between corporations owned by the same individual

Case Study 50 – Latvia	
Foreign national Mrs V opened an account in a Latvian bank B, and received USD 3 827 000 and EUR 208 000 shortly thereafter from foreign Company M. Company M had received the funds from foreign Companies R and W. Public information revealed that Companies M and W had the same shareholder – an offshore legal entity, whereas the beneficiaries of Companies M and W presented at the bank were two other individuals, which raised concerns of a scheme to obscure beneficial ownership. Mrs V transferred USD 2 980 000 USD to Individuals E, O and A to accounts at foreign Bank F, stating the purpose of transaction as a gift to grandchildren. At the same time Mrs V transferred USD 840 000 to her own account at foreign Bank F. All beneficiaries had the same address, which suggested that Mrs V was residing in a country different from that on bank CDD records. The sum of USD 220 000 was further received in Mrs V's account from Individual L, and further transfers of USD 300 000 were initiated to Individuals A and E. Bank B made an EDD request, and according to documents received on behalf of Mrs V electronically, Mrs V had sold two paintings to Individual B for USD 220 000 using Individual L as an intermediary, but the signatures on the agreement appeared digitally embedded. Individual A presented himself at Bank B claiming to be a grandchild of Mrs V, who he claimed to be deceased but could not provide a death certificate. The FIU confirmed with Mrs V's country of residence that she was deceased and that transactions since the date of death had been performed by third parties. The FIU issued an order to freeze USD 350 000 in Mrs V's accounts.	
Indicators	• Client is reluctant or unable to explain why they are conducting their activities in a certain manner • Foreign nationals with no significant dealings in the country in which they are procuring professional or financial services • Transactions which appear strange given an individual's age • Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Falsified paper trail • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client

Case Study 51 –Mexico	
A network of 42 shell companies with different lines of business was dismantled, with companies located in Mexico and others abroad. The network was created to offer money laundering services to criminal organizations through a group of independent agents who contact customers to offer the said services, charging a fee from between 1 and 5% the amount of the funds operated.	
Indicators	• Previous conviction for fraud, tax evasion, or serious crimes • Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Financial activities and transactions inconsistent with the corporate profile • Fabricated corporate ownership records • False invoices created for services not carried out • Falsified paper trail • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 52 – Mexico	
Four shell companies requested from the Mexican Tax Administration Service (SAT) the refund of the Value Added Tax, from non-existent operations carried out in 2008 and 2009. In total, 26 companies participated in the simulation of transactions, and 48 individuals were part of the scheme as partners, administrators, and legal representatives. Part of the illegally obtained resources were sent to bank accounts in the U.S., and later used to make transfers to accounts in Las Vegas, Nevada. These accounts were held by Casinos and by individuals who carried out gambling activities.	
Indicators	• Financial activities and transactions inconsistent with the corporate profile • Bank accounts in multiple international jurisdictions without good reason • False invoices created for services not carried out • Falsified paper trail • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate

	wealth or income • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 53 – Namibia	
Namibian national A (as sole owner) registered two close corporations using false national identity documents. Subsequently, A opened bank accounts at two local banks for each of these corporations. The bank accounts at one bank were active, while those at the other bank remained dormant resulting in their closure. A authorised foreigners B and C to manage the said accounts. B and C used online banking channels to make huge inward and outward transfers on the two corporate accounts. Funds had been transferred from foreign jurisdiction SA to Namibia and then immediately re-routed to other foreign jurisdictions, including back to SA from where the funds had emanated. The transfers started with relatively small amounts quickly grew larger. The funds were generally withdrawn in less than 48 hours after deposit.	
Indicators	• Signatory to company accounts without sufficient explanation • Declared income which is inconsistent with their assets, transactions or lifestyle • Registered at an address that does not match the profile of the company • Legal person or arrangement conducts a large number of transactions with a small number of recipients • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Financial activities and transactions inconsistent with the corporate profile • Multiple bank accounts without good reason • Falsified records or counterfeited documentation • Fabricated corporate ownership records • Falsified paper trail • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Transaction is a repeat transaction between parties over contracted period of time • Transaction appears cyclical • Transaction involves complicated transaction routings without sufficient explanation or trade records

Case Study 54 – Namibia	
The case involved two Namibians and three Chinese subjects. The subjects registered two Proprietary Limited companies as well as a Namibian close corporation. Subsequently they opened nine bank accounts at five local banks, with one Chinese and two Namibians directors/shareholders as signatories on the accounts. The entities and individuals received significant deposits and transfers derived from Namibian accounts and transferred to a foreign jurisdiction.	
Indicators	• Legal person or arrangement conducts a small number of high-value transactions with a small number of recipients • Legal person or arrangement receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification • Financial activities and transactions inconsistent with the corporate profile • Multiple bank accounts without good reason • Correct documents not filed with the tax authority • Legal Person pays no taxes, superannuation, retirement fund contributions or social benefits • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 55 – Namibia	
Mr. X declared that he is involved in taxi business. Analysis confirmed that X made regular large cash deposits into two accounts, followed immediately by large cheque withdrawals to other businesses and accounts of his close corporations and relative. The corporate entity's activities, as registered with the registrar of close corporations, include retail, mining, construction and fishing. Withdrawals from this account were exclusively electronic transfers. The account also received monthly funds from various individuals, as well as large-value of electronic transfers from a company in South Africa in the account of a Namibian Registered Trust. Analysis established that X owns several high value properties in Namibia and South Africa, which were purchased in cash. Some of these properties were registered under legal entities. Mr. X was found guilty of drug dealing.	
Indicators	• Transactions which appear strange given an individual's age • Previous conviction for fraud, tax evasion, or serious crimes • Signatory to company accounts without sufficient explanation • Financial activities and transactions inconsistent with their customer profile • Legal person or arrangement conducts a large number of transactions with a small number of recipients

	• Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Multiple bank accounts without good reason • Transaction is a business transaction that involves family members of one or more of the parties without a legitimate business rationale • Transaction is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 56 – Namibia	
An STR was filed on Y on suspicion that he might be involved in illegal diamond dealing and using a business bank account to co-mingle proceeds of crime with legitimate income. Analysis revealed that Y is the sole member close corporation with its principle business "manufacturing, recycling and cleaning". Substantial sums were deposited into the business account, with most deposits from electronic funds transfers originating from several individuals in America and in Asia. Y withdrew the funds in cash. Analysis revealed that Y presented himself as an authorized diamond dealer in Namibia to foreign buyers online.	
Indicators	• Long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Financial activities and transactions inconsistent with the corporate profile • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile • Funds are unusual in the context of the client or customer's profile

Case Study 57 – Namibia
This case involves subjects and entities using the electronic banking system to channel proceeds of crime to foreign jurisdictions. Funds deposited into close corporations and subject's personal account and then structurally withdrawn in the foreign jurisdiction under the pretext that it is business related funds. Subject 1, a Chinese national, opened a personal bank account and registered a

close corporation (Entity 1) that also opened accounts with three different financial institutions. Subject 1 further "assisted" a Namibian woman 1 to open personal accounts at the same three financial institutions. He also "assisted" her to register four close corporations in her name (Entities 2-5) and opened accounts with one of the financial institutions. Subject 1 assisted other Namibian women 2 and 3 to open bank accounts with two of the financial institutions. Subject 1 controlled the ATM cards of Entities 1-5 and accounts in name of Namibian women 1 and 2, to the extent that he was transacting on them. Namibian woman 3 did not pick up her ATM cards and when requested by the bank to explain why she opened accounts, she disappeared and could not be traced. The funds deposited or transferred into the accounts of Namibian women 1-3 and entities 2-5 were from Subject 1, whilst the funds into Subject 1's accounts were from Chinese owned entities.	
Indicators	• Client is reluctant to provide personal information. • Client is reluctant or unable to explain their business activities and corporate history • Actively avoiding personal contact without sufficient justification • Refuse to co-operate or provide information, data, and documents usually required to facilitate a transaction • Transactions which appear strange given an individual's age • Registered at an address that does not match the profile of the company • Director or controlling shareholder(s) does not appear to have an active role in the company • Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Multiple bank accounts without good reason • Disinterested in the structure of a company they are establishing • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile

Case Study 58 – Netherlands
Mr. B, a Dutch taxpayer, had put money in a Jersey trust and had not declared this to the tax authorities. Mr. B did not state in his income tax returns that he was involved in a trust and intentionally answered a tax questionnaire incorrectly or incompletely concerning his involvement in the trust. The court found that Mr. B

intentionally provided incorrect information to a public servant of the Netherlands Tax and Customs Administration, resulting in too little tax being levied.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Focused on aggressive tax minimisation strategies • Correct documents not filed with the tax authority • Falsified records or counterfeited documentation

Case Study 59 – Netherlands	
The Suspect, a doctor, received payments from the pharmaceutical industry with which he did business. The amount of this payment varied per contract. These payments, which can be considered income, were not paid into one of the suspect's Dutch bank accounts, but into Luxembourg numbered accounts in the name of a foundation. The suspect never declared the balances of these Luxembourg bank accounts in his income tax returns.	
Indicators	• Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason • Focused on aggressive tax minimisation strategies • Correct documents not filed with the tax authority • Transaction involves a numbered account • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 60 – Netherlands	
This tax evasion scheme consisted of sending false invoices from a company incorporated by the suspect in the BVI to the Dutch company, to create the illusion that services have been provided to the Dutch company. The Dutch company pays this invoice to the company in the BVI which results in a reduction in the turnover and profit because more costs have been incurred. From the BVI the amounts received were paid into the private bank accounts of the suspect and co-suspect in Cyprus who were able to access those accounts in the Netherlands by means of a debit/credit card. Funds were used by the suspect to finance real estate.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • False invoices created for services not carried out. • No real business activities undertaken • Client is both the ordering and beneficiary customer for multiple

	international funds transfers • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 61 – Netherlands	
The FIU received a notification from a financial institution in respect of an international transfer to a foreign company in Italy. The beneficial owner of this company appeared to be the ex-wife of the client. This client regularly transferred money from his private account but also from his business account to the account of his ex-wife and her businesses. By means of the "loan agreements" the money was deposited again into the bank account of the client. On the basis of this information the notification was declared suspicious and forwarded to the investigation teams.	
Indicators	• Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Transaction is a business transaction that involves family members of one or more of the parties without a legitimate business rationale

Case Study 62 – Netherlands	
A civil-law notary filed an STR that indicates a house purchase was financed with a loan from an Andorran company. The Netherlands FIU subsequently requested further information on this company from Andorra. The UBO of this company appeared to be the same person as the purchaser of the house. On the basis of this information, the notification was declared suspicious and forwarded to the investigation teams.	
Indicators	• Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification

Case Study 63 – Netherlands	
A Dutch target company received loans from a Swiss TCSP with a bank account in Montenegro, under the description of "repayment loan". This Swiss TCSP is also the sole shareholder of the Dutch target company. The received money was subsequently re-loaned again via a subsidiary of the Swiss TCSP in Moldavia to the UBO in The Netherlands. The Dutch target company was also used by other clients of the Swiss TCSP. The Dutch target company received loans from the Swiss TCSP and subsequently re-loaned these funds to operational companies in Italy and England, which were managed by the UBOs. The account in Montenegro of the Swiss TCSP was topped up by a Swiss bank account in the name of the UBO of the Dutch target company. The FIU suspects that this manner of re-loaning one's own money via this Swiss TCSP is also used by other persons.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Client is both the ordering and beneficiary customer for multiple international funds transfers • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification

Case Study 64 – Netherlands	
This case concerns a criminal investigation into money laundering and the purchase and financing of premises and apartment rights in the Netherlands by two Liechtenstein trusts. The ultimate beneficial owners and the source of funds for the purchase and financing of the real estate are shielded by the use of these trusts and by a number of facilitators. The purchase involves a total of almost EUR 2 million in purchase (costs) and financing of the real estate which is presumably derived from drug trafficking. The two trusts have their registered office in Liechtenstein and the persons who represent the trusts are family members of the suspects.	
Indicators	• Under investigation or have known connections with criminals • Registered at an address that is also listed against numerous other companies or legal arrangements • Financial activities and transactions inconsistent with the corporate profile • Correct documents not filed with the tax authority • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Client is both the ordering and beneficiary customer for multiple international funds transfers

	• Transaction is a business transaction that involves family members of one or more of the parties without a legitimate business rationale • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners • Transaction involves a professional intermediary without due cause or apparent justification

Case Study 65 – Netherlands	
A Dutch investment fund invested money deposited by investors in foreign life insurance policies. The investors participated in a trust that had become owner of the life insurance policies. After the death of the insured (third parties), the insurance would pay out to the fund that in turn would pay out to the investors. The risk that the original holder of the life insurance policy would live longer than the agreed maturity (the longevity risk) was re-insured. The re-insurers took over the policy from the trust fund and the investors received from the re-insurer an amount that was equivalent to the death benefit value of the policy. All deposits, EUR 175 million, went through the foreign accounts of the trust companies. It appears that only a limited part was invested in the promised second-hand life insurance policies. A large part was immediately channelled to the bank accounts of the suspect and the trustee.	
Indicators	• Unusually large number of beneficiaries and other controlling interests • Bank accounts in multiple international jurisdictions without good reason • Funds are unusual in the context of the client or customer's profile

Case Study 66 – Netherlands	
The case involves funds derived from extortion. The suspect created legal constructs made up of parent companies registered in a low tax jurisdiction with few or no or scarcely any obligations to keep administrative and accounting records. The suspect used coded bank account in Switzerland to further conceal the money laundering activity. TCSPs managed the companies.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Bank accounts in multiple international jurisdictions without good reason • Transaction involves a numbered account

Case Study 67 – Netherlands
A medium-sized Dutch company sent double invoices - one invoice from the Dutch company to which payments were made in the Dutch account and are also properly declared to the Netherlands Tax and Customs Administration. The

second email/false invoice was to be paid into a numbered account in Switzerland that is in the name of a fictitious company. When Dutch and Swiss relations improved, the Swiss bank advised the client to incorporate a Panamanian company and deposit the funds into numbered accounts in Cyprus in the name of two Panamanian S.A.s over which the directors of the Dutch company exercise control.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason • Falsified records or counterfeited documentation • Double invoicing between jurisdictions • False invoices created for services not carried out. • Transaction involves a numbered account

Case Study 68 – Netherlands	
This case was an investigation into Dutch suspects for filing incorrect tax returns, money laundering and forgery. During the investigation, it was identified that funds had been transferred through a numbered account in Switzerland in the name of a financial service provider in Panama. Shortly thereafter, very similar amounts were debited from the account, under a false description, to the credit of the Dutch suspects. A financial service provider facilitated this by providing the Dutch suspects with the opportunity to conceal these cash flows from third parties. The invoices for the services provided were paid to the financial service provider via the account in Switzerland.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Transaction involves the two-way transfer of funds between a client and a professional intermediary for similar sums of money • Transaction involves a numbered account • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 69 – Netherlands
A Panamanian Private Foundation was founded by a Panamanian company which is affiliated to Mossack Fonseca. The Foundation Council is another corporation, and the beneficiary is Mr. E, the director and sales advisor of a Netherlands TCSP.

The registered agent is X Legal Services. The Panamanian Private Foundation has opened a bank account in Cyprus. This is a very large criminal investigation, which also includes an investigation into the persons who made use of the structure offered by the TCSP.	
Indicators	• Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Focused on aggressive tax minimisation strategies • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including formal nominees

Case Study 70 – Netherlands	
Mr. and Mrs. X acted as directors of a Dutch holding company and a Dutch operating company, as well as the founders of a Unit Foundation and the beneficial owners in an Offshore Investment Holding Company. It appears that agreements for the provision of directorship and/or nominee shareholder services have been drawn up. The invoices of the Offshore Investment Holding Company list several services performed for the corporation including the opening of a bank account. No amount is charged for management services. An employee of the Dutch TCSP has signing powers for the Offshore Investment Holding Company's bank account. Mr. and Mrs. X determine whether funds are paid from the underlying companies to the Offshore Investment Holding Company and on to the Unit Foundation. As a result, it can be argued that the employee in Cyprus only carried out the wishes of Mr. and Mrs. X and that they are the de facto managers of the Offshore Investment Holding Company.	
Indicators	• Requests the formation of complex company structure without sufficient business rationale • Agreements for nominee directors and shareholders • Employees of professional intermediary firms acting as nominee directors or shareholders • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including formal nominees • No real business activities undertaken • Transaction involves a professional intermediary without due cause or apparent justification

Case Study 71 – Netherlands	
A criminal investigation into a Dutch TCSP was instigated on account of the systematic failure to notify unusual transactions and money laundering. This was presumed to involve the facilitation of fake transactions on behalf of foreign clients to ensure, for example, the assets or property of those clients were scarcely taxed, or funds parked were transferred by means of fake transactions to another jurisdiction. This was carried out by means of complicated well-considered structures with companies and trusts in various countries for which instructions were given by a financial service provider and were also discussed in this way by the suspect with the Dutch civil-law notary. Dutch entities were part of these complicated structures. The same applied for the Dutch foundations registered at an international address. The structure sometimes consisted of eight different entities, in various countries. The suspect reportedly did not know in several cases the identity of the actual beneficiaries of the companies that he incorporated.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation • Focused on aggressive tax minimisation strategies • Requests the formation of complex company structure without sufficient business rationale • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Transaction involves a professional intermediary without due cause or apparent justification

Case Study 72 – Netherlands	
The owner of a TCSP posed as a "Business Lawyer" but was not registered as a lawyer. The clients reportedly paid remuneration for the trust services, which were (partially) paid into the suspect's account in three different international jurisdictions. A TCSP in an international jurisdiction was also reportedly used. The suspect evaded tax on these amounts for a number of years. The suspect also committed immigration fraud by putting clients on the payroll of one of his companies to draw up false employment contracts and/or salary slips. Ownership of the shares of the Dutch companies was often veiled by means of foundations and foreign company structures via a low tax jurisdiction. Dutch companies appear to have been mainly used as a means of channelling money. In addition, the suspect reportedly laundered money in the purchase of real estate intended for himself, his family or for clients of the TCSP.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre

	• Legal person or arrangement regularly sends money to low-tax jurisdictions or international trade or finance centres • Frequent payments to foreign professional intermediaries. • Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason • Focused on aggressive tax minimisation strategies • Interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without sufficient commercial explanation • Correct documents not filed with the tax authority • False invoices created for services not carried out • Falsified paper trail

Case Study 73 – Netherlands	
A Dutch company has business transactions with two Ukrainian companies. On account of the strict rules in Ukraine, international legal constructs are created to continue doing business. The Dutch company delivers goods to the Ukrainian companies. However, the cash flow goes through a Panamanian entity with a bank account in Latvia. It subsequently appears that there is a discrepancy between the purchase and sales invoices and that this "surplus" remaining in the Latvian bank account.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Discrepancy between purchase and sales invoices • Transaction involves complicated routings without sufficient explanation or trade records

Case Study 74 – Netherlands	
A company registered in the BVI with an account in Switzerland transfers money via a Dutch bank account to a company registered in Cyprus with a Latvian bank account. The UBOs of both companies are Russian. STRs are submitted because of the use of (false) invoices which were not based on any fair consideration. This regularly occurs in what is referred to as the VAT carrousel fraud.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • False invoices created for services not carried out

Case Study 75 – Netherlands	
This South American investigation focused on persons whose tax profile did not correspond to the amounts paid into their accounts in foreign countries or their spending. Corruption funds were allegedly paid to the suspects via the Dutch company, which company was managed by a Legal Consultancy Agency registered in a low tax jurisdiction. The Dutch company was also reportedly registered in an international jurisdiction. The funds paid ended up in Luxembourg accounts in the name of the suspects which were later converted to numbered accounts.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Financial activities and transactions inconsistent with their customer profile • Bank accounts in multiple international jurisdictions without good reason • Transaction involves a numbered account

Case Study 76 – Netherlands	
International company A with its headquartered in The Netherlands paid corruption funds to a government employee via letter box companies. An international company was registered in an international jurisdiction, with a government employee registered as the beneficial owner but with nominee shareholders and directors. Payments were made via a Dutch bank account of a subsidiary of the international company to an account of the foreign company in Estonia and via an enterprise registered in Hong Kong, after which these funds were paid into bank accounts in an international jurisdiction and from there to a Luxembourg bank account of the international company. Bribes were also paid to charities that were directly associated with government employees. In order to account for the bribes, false invoices were entered in the accounting records.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Bank accounts in multiple international jurisdictions without good reason • False invoices created for services not carried out • Nominee owners and directors including formal nominees • Transaction involves complicated routings without sufficient explanation or trade records

Case Study 77 – New Zealand	
A New Zealand shell company was set up by a New Zealand TCSP based in Vanuatu. The shell company was registered on behalf of an unknown overseas client and nominees were used to hide the identity of the beneficial owners. The actual business of the shell company was not apparent and was not indicated by the company name. The address listed on the companies' register was the same virtual office in Auckland as the TCSP. The nominee director resided in Seychelles, and the nominee shareholder was a nominee shareholding company owned by the TCSP. The nominee shareholding company was itself substantially a shell company and had been used as the nominee shareholder for hundreds of other shell companies registered by the TCSP. News reports indicated that a power of attorney document transferred the directorship to a Russian national who had sold his passport details, with a bank account opened in Latvia. When journalists from the Organised Crime and Corruption Reporting Project (OCCRP) made contact with the Russian national, the man revealed he was unaware of the New Zealand company or its bank accounts. His identity, which he had sold, had been used without his knowledge. Furthermore, a former officer of the Russian tax police told journalists that hundreds of law firms specialise in establishing ready-made shell companies for their clients, who want to remain anonymous. Usually, these law firms rely on disadvantaged individuals who sell them passport details for approximately USD100-300. Trade transactions were conducted with several Ukrainian companies including a state-owned weapons trader. The contracts were then cancelled after the funds had been transferred and refunds were made to different third-party international companies. Transactions were also made with three other New Zealand shell companies registered by the same TCSP, using the same nominee director, nominee shareholder and virtual office address as the shell company. News reports indicated that all four shell companies had been involved in laundering USD40 million for the Sinaloa drug cartel based in Mexico.	
Indicators	• Foreign nationals with no significant dealings in the country in which they are procuring professional or financial services • Registered under a name that does not indicate the activity of the company • Registered at an address that does not match the profile of the company • Registered at an address that is also listed against numerous other companies or legal arrangements • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. • Discrepancy between purchase and sales invoices • Fabricated corporate ownership records • False invoices created for services not carried out • Falsified paper trail

	• Agreements for nominee directors and shareholders • Employees of professional intermediary firms acting as nominee directors or shareholders • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including formal nominees • Address of mass registration • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Corporation has no personnel • Legal person does not have a physical presence • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 78 – New Zealand

A New Zealand law firm was linked to clients who had been implicated, arrested or convicted of a myriad of offences including embezzlement, bribery, corruption, tax evasion, and money laundering. This law firm sets up its business basis in New Zealand, and worked for overseas clients using its in-depth knowledge of New Zealand tax, trust and company law.

The companies and partnerships were set up by this New Zealand law firm, who routinely used its employees as nominee directors and shareholders, with the beneficial owners (who were sometimes offenders and their associates) not publicly named. Furthermore, often a chain of companies was established, with one company is the shareholder of another, which was the shareholder of another, which added complexity to the structure, and further removed the beneficial owner from the assets. Sometimes a New Zealand (shell) company was used as a trustee of the trust.

The companies involved were usually all shell companies with nominee directors, shareholders, and addresses. The companies, partnerships and trusts comprised the complex structures established by this New Zealand law firm, which can be used to hide and protect wealth. Furthermore, sometimes entities were set up internationally by this New Zealand law firm's business associates in other countries, which were added to the structures, further increasing the complexity and decreasing the ability and efficiency of detecting crime and hidden wealth. If

	suspicions did arise and a person with such a structure was investigated, there was a convoluted audit trail that could be arduous to trace. There were strong indications that criminals have structures set up by this New Zealand law firm with evidence that some of these structures have been used by criminals to hide assets. A NZ-based employee was also named as a director to satisfy the legal requirement to have a New Zealand resident director and address; however, the beneficial owner of the company was not identified in every instance.
Indicators	• Previous conviction for fraud, tax evasion, or serious crimes • Under investigation or have known connections with criminals • Registered at an address that is also listed against numerous other companies or legal arrangements • Director or controlling shareholder(s) does not appear to have an activity role in the company • Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including formal nominees • Address of mass registration • No real business activities undertaken • Exclusively facilitates transit transactions and does not appear to generate wealth or income • Legal person has no personnel • Legal person does not have a physical presence

Case Study 79 – New Zealand
Assets believed to be acquired using proceeds of crime allegedly linked with the settlor of these trusts. Some of these structures were set up via a NZ TCSP. None of assets are held directly by the trustees of the trusts – but via various US domestic and foreign entities. It appears all activities were US based with orders against US entities indirectly owned via overseas companies. The scheme involved two trusts, four companies, with nominee directors and shareholders employed by a law firm. This complex structure prevented law enforcement from obtaining beneficial ownership information by establishing a complex web of shell companies and trusts.

Indicators	• Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Agreements for nominee directors and shareholders • Employees of professional intermediary firms acting as nominee directors or shareholders • Nominee owners and directors including formal nominees • Address of mass registration

Case Study 80 – New Zealand	
Shell companies based in Panama, Belize, and the UK with nominee shareholders and directors have been used to open Latvian bank accounts to conduct hundreds of millions of dollars' worth of international payments. The majority of transactions are payments being made on behalf of Vietnam entities for imported goods, or payments to Vietnamese expats living overseas on behalf of purportedly Vietnam-based senders. This distinct Vietnamese connection indicates the accounts may be controlled or administered from within Vietnam. New Zealand bank accounts were used to receive funds transferred from bank accounts in Latvia, Cambodia and China. The New Zealand accounts are either accounts held by students or by fruit wholesalers and exporters. More than 15 NZ properties have been purchased with funds from the Latvian bank accounts. These property transactions have been undertaken through NZ law firms. Information suggests that the Latvian accounts are also being "topped up" by other shell company bank accounts based in international jurisdictions, indicating a co-ordinated layering process being undertaken.	
Indicators	• Declared income which is inconsistent with their assets, transactions or lifestyle • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Financial activities and transactions inconsistent with the corporate profile • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds are unusual in the context of the client or customer's profile • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre

Case Study 81 – New Zealand	
Companies registered in New Zealand by a Vanuatu-based TCSP operated by New Zealand citizens were suspected of acting as shell companies that facilitate crime in foreign jurisdictions. The TCSP acted as nominee shareholders and provided nominee directors who resided in jurisdictions such as Vanuatu, Panama and the Seychelles – in the case of Company A, the employee recruited to act as a director likely had no knowledge of the activities taking place, as they had no previous involvement in any of the TCSP activities. Crimes include smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and money laundering. Company A was one company set up by the TCSP, which leased the plane that was caught smuggling arms. 73 companies registered in New Zealand by the TCSP were suspected of acting as shell companies which facilitated crime in foreign jurisdictions. Crimes included the smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and money laundering.	
Indicators	• Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Falsified paper trail • Agreements for nominee directors and shareholders • Employees of professional intermediary firms acting as nominee directors or shareholders • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including formal nominees • Address of mass registration

Case Study 82 – Norway	
Seven Norwegian citizens, in different combinations, were the owners of four small Norwegian IT-companies. They were approached by a major Norwegian company (listed on the stock exchange) that wanted to buy shares of all the companies. The price offered was much higher than the share capital in the companies (their input value for taxation). In response to this, the owners established new companies in offshore jurisdictions and sold their shares to those companies with a minimum of profit. The newly established companies then immediately resold the shares to the actual buyer in Norway. The sales profits were realized abroad with no tax.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement conducts a small number of high-value transactions with a small number of recipients • Legal person or arrangement receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere

	in a short period of time without commercial justification • Focused on aggressive tax minimisation strategies • Transaction appears cyclical • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners • Transaction involves the transfer of shares in an off-market sale • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre.

Case Study 83 – Norway	
The CEO of a large Norwegian company transferred significant sums of money to several companies, claiming that this represented payment for services (consultancy fees etc.). Investigation proved that no services were delivered and that the CEO was the beneficial owner of the companies.	
Indicators	• False invoices created for services not carried out • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners

Case Study 84 – Norway	
The suspect was the head of a shipping company, and committed breach of trust by buying ships and equipment intended for the company through a structure of companies that was ultimately under his control. The suspect then sold the assets to the company at an inflated price. He simultaneously committed fraud against the banks that were financing the ships, by alleging the ships were bought at marked price. Although beneficial ownership was determined, legal challenges remain in confiscating assets frozen in foreign bank accounts that were not party to the criminal case.	
Indicators	• Inflated asset sales between entities controlled by the same beneficial owner • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners

Case Study 85 – Panama	
The purported legitimate purpose of the scheme was the development and construction of real estate, based on small investors who injected capital. The funds provided by the settlor or third-party adherents were derived from illegal activities (corruption of public servants and illicit enrichment). The scheme involved a BVI company with nominee directors, ultimately controlled by a PEP who was a client of a bank that had a relationship with the TCSP. The TCSP set up a real estate trust to receive money and assets that come from the business of the settlor and "investors." The assets received were invested in a real estate project, with the same assets given as a warranty to the bank that was financing 60% of the real state project. The ultimate beneficial owner of the real estate project was the son of the PEP. The trustee did not conduct extensive due diligence and relied on the due diligence performed by the bank that referred the client, since both the client and the trustee maintained a business relationship with the bank.	
Indicators	• Client is reluctant or unable to explain their source of wealth/funds • Client is reluctant or unable to explain the nature of their business dealings with third parties • Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. • Falsified paper trail • Nominee owners and directors including formal nominees • An asset is purchased with cash and then used as collateral for a loan within a short period of time

Case Study 86 – Peru
This case concerns a Peruvian PEP, his wife, his mother-in-law and other individuals close to him following the purchase of properties. Two mortgages were paid in advance using funds from a Costa Rican company that had been established only six months before instructions were given for the wire transfers. The loan was paid in just four months by the offshore company, despite the financial loss incurred. The Peruvian authorities established the origin of the funds to be corrupt activities performed by the PEP during his administration. The purchase of a luxury property by the mother-in-law of the PEP, who did not have the economic capacity to make this purchase, led to the opening of a case at the FIU and the issuance of SARs by reporting entities.

Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Financial activities and transactions inconsistent with their customer profile, • Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • A loan or mortgage is paid off ahead of schedule, incurring a loss

Case Study 87 – Russia

A state customer concluded contracts on research work and the development of a special software with Contractor #1 and Contractor # 2. Analysis of financial transactions showed that these contractors did not conduct any research activities themselves, but transferred budgetary funds to subcontractors with real scientific laboratories among them. The majority of funds from Contractor #1 was sent to its subcontractor, who channelled funds to a shadow financial scheme consisting of multiple layers of shell companies. The funds were finally withdrawn in cash. The majority of funds from Contractor # 2 was sent to a real estate company that invested these funds into its business activity, acquired luxury cars and granted zero-interest rate loans to a number of individuals.

Analysis of ownership data, address registry information, an air tickets booking database, financial transactions and law enforcement data showed that Contractor #2 was previously owned by Mr. X, before the ownership was passed to straw men uninvolved with the scheme. The real estate company was formerly owned by Mr. X, before the ownership was transferred to his daughter. Contractor #1 was owned by straw men who had no idea about the company's business activities and received instructions from Mr. X. These straw men received a "salary" from the company's account. The director of the state customer's department responsible for research activities was a brother of Mr. X. A daughter of the state customer department's director acquired expensive real estate using cash that was deposited in advance in her account. The woman who had joint flights with Mr. X acquired expensive real estate using cash that was in advance deposited into her account in advance.

Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • False invoices created for services not carried out • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Nominee owners and directors including informal nominees, such as children,

	spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Loans are received from private third parties without any supporting loan agreements, collateral, or regular interest repayments • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile • Transaction involves the use of multiple large cash payments to pay down a loan or mortgage

Case Study 88 – Russia	
Embezzled public funds worth RUB 300 million (11 million USD) were transferred from the account of Company K to the account of Company R. Company R, a Delaware corporation, was owned and managed by the Russian wife of the suspect, a state official. The same day, Company R transferred USD 11 million as a loan to an account of Company A (BVI) held by a Cypriot bank. Company A then transferred more than USD 11 million to the Company D (US) to purchase real estate in France. Company D transferred more than USD 12 million to a French Notaries Bureau. Information from the FIU of Luxembourg showed that one of the US banks acted as a guarantor for the suspect's wife in a transaction to purchase of shares of a French company – and the holder of the real estate. The transaction was conducted via an S.S. company – a French subsidiary of a Luxembourg S.D. SA., incorporated and owned by the same individual. Analysis showed that these two chains were interrelated and the real estate was purchased with the proceeds of public funds embezzled for the benefit of the state official's wife.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Transaction is occurring between two or more parties that are connected without an apparent business or trade rationale • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile

	• Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 89 – Serbia	
Four transfers from the account of agricultural cooperative "U.B." were made to the account of legal person "P.I.P.H", totalling approximately EUR 200 000. Funds in foreign currency totalling EUR 178 630 were purchased from this money immediately after it was deposited, and after that transferred to the account of Delaware Company M. The account of Company M was held with a bank in Cyprus. The stated purpose of the transactions was payment on basis of trade in goods. Furthermore, there was a transfer from the same account of "P.I.P.H" to the account of Delaware Company S, in the amount EUR 75 175. Company S's account was with a bank in a foreign country. The stated basis for the transfer was payment for trade in goods. Investigation established that this was the case of black market trade. The funds accumulated from trade in goods were transferred to accounts of six legal persons from Serbia (it is suspected that these are front companies). The funds were afterwards transferred to accounts of legal persons abroad and then further to accounts of numerous Chinese citizens assumed to be the real beneficial owners of the goods sold in Serbia.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Corporation maintains a bank balance of close to zero, despite frequent incoming and outgoing transactions • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction involves the transfer of shares in an off-market sale • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 90 – Serbia
Members of an organized crime group devised a scheme involving Serbian banks, with the intention to legalize drug trafficking proceeds through purchasing a company's shares. One of the features of the scheme was the structuring of transactions to avoid reporting transactions to the FIU. The organized crime group found 42 individuals, who agreed to pay deposits into their own accounts, in the amounts below the threshold of EUR 15 000, declaring them their savings. Subsequently, these persons stated that they agreed to have their money used to acquire a company providing services in hospitality industry. At the same time, the organized crime group took over profitable private companies in Serbia, with large capital turnover through accounts, which were performing well and whose owners were ready to sell them.

Indicators	• Under investigation or have known connections with criminals • Falsified records or counterfeited documentation • Finance is provided by a lender, including either a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification • Transaction involves the purchase of high-value goods in cash

Case Study 91 – Slovenia	
EUR 4 million was transferred from a Slovenian company to a Liechtenstein TCSP's account at a Liechtenstein's bank under the guise of "construction consulting." MLA was used to identify the beneficial owner of TCSP, and the FIU identified that another Liechtenstein TCSP with the same trustee had opened a bank account in a Slovenian bank, though the trustee declared himself to be the beneficial owner. A bank statement allowed authorities to identify the beneficial owner as named by the trustee when opening the account. A deal was made with three suspects and authorities retrieved the embezzled assets and levied a penalty of more than EUR 1 million.	
Indicators	• Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client

Case Study 92 – Switzerland	
A lawyer, who had already been convicted of document falsification and misappropriation, hid stolen bearer shares in accounts opened in the name of offshore companies. The bearer shares had been sold and registered shares of the same company had been bought with the proceeds and transferred to other accounts in different jurisdictions. With effective domestic and international co-operation, the suspect was arrested and extradited to Switzerland and is now in prison. Assets in the amount of more than CHE 50 million (Swiss Francs) could also be blocked in all five countries.	
Indicators	• Under investigation or have known connections with criminals • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Multiple bank accounts without good reason • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Transaction appears cyclical

	• Transaction involves the transfer of bearer shares in an off-market sale • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 93 – Switzerland	
An operational coal mining company paid out EUR 800 million to their owner, a Dutch NV over a period of four years. The financial intermediary came across information that there was an ongoing prosecution of the Dutch NV and its owner in a third country and filed a STR for misappropriation of funds. The documentation held by the Swiss financial intermediary showed that this Dutch NV was owned by Mr. A, a citizen of another European country. Over a time period of 10 years CHF 3.5 billion was transferred through a large and complicated structure of 32 companies in different countries including the British Virgin Islands and the Netherlands. The Swiss financial intermediary's documentation identified the beneficial owner of almost all of the companies as Mr. A.	
Indicators	• Foreign nationals with no significant dealings in the country in which they are procuring professional or financial services • Under investigation or have known connections with criminals • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or finance centre • Legal person or arrangement regularly sends money to low-tax jurisdictions or international trade or finance centres or international trade or finance centres • Legal person or arrangement conducts transactions with international companies without sufficient corporate or trade justification • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense or which do not make commercial sense • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners • Transaction involves complicated transaction routings without sufficient explanation or trade records • Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre or international trade or finance centre

Case Study 94 – Switzerland
A Swiss financial intermediary filed a SAR after a deposit of USD 2 million was made into the account of Company A by Company B who is a wholly owned

subsidiary of C Holding. The beneficial owner of company A, Mr. X, justified the incoming funds as being the result of services provided by Company A under a contract between companies A and B. The nature of these services was purported to be the provision business contacts, acquiring potential clients, and negotiation of terms and conditions. Shortly after the deposit, two transfers of USD 1 million were made to two other companies of which Mr. X and Mr. Y –both high-ranking executives of the Dutch company C Holding - were the beneficial owners. The annual report of the Dutch company did not include any information about compensation to Mr. X and Mr. Y. The financial intermediary therefore suspected money laundering and dishonest business management to the disadvantage of the shareholders of company C Holding.	
Indicators	• The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction involves two legal persons with similar or identical directors, shareholders, or beneficial owners • Transaction involves complicated transaction routings without sufficient explanation or trade records

Case Study 95 – Trinidad and Tobago	
The case concerns a US citizen who created a complex scheme to avoid payment of taxes on income earned from a business operated in Trinidad and Tobago. The scheme included the involvement of gatekeepers, multiple individuals and legal structures and use of money remitters. The suspect, "Blackjack", earned millions of dollars over the period 2009-2011 from a Trinidad and Tobago Private Members' Club (similar to a casino). Blackjack took action to conceal his income and assets from the IRS by using unreported bank accounts in Trinidad and Tobago to deposit personal income; using US bank accounts in the names of his New Jersey business entities to receive income from the casino; using those business entities to pay for personal expenses; transferring income from the casino directly to vendors in the US for personal expenses; and directing the casino employees to send cash through wire transfers to individuals in New Jersey who then collected the cash on his behalf.	
Indicators	• Financial activities and transactions inconsistent with the corporate profile • Focused on aggressive tax minimisation strategies • Correct documents not filed with the tax authority • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Transaction is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile • Funds are sent to, or received from, a jurisdiction that is considered to pose a high money laundering or terrorism financing risk

Case Study 96 – Turkey	
The fuel obtained from fuel smuggling was sold through the petrol stations under the control of organised crime. Person A, who is the beneficial owner and the leader of the organisation, disguised his ownership by transferring control of the petrol stations to close associates and by carrying out transactions using cash and straw men.	
Indicators	• Client is reluctant or unable to explain the identity of the beneficial owner • Director or controlling shareholder(s) cannot be located or contacted • Bank balance of close to zero, despite frequent incoming and outgoing transactions • Falsified paper trail • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise

Case Study 97 – Turkey	
A group of persons create and operate websites to provide illegal betting over the internet. In order to hide their identity, these persons use natural persons and shell companies to open bank accounts, and withdraw or transfer the deposited funds. The natural persons are aged around 30, are not registered as taxpayers and do not have social security records, live in different cities, and are generally unemployed, housewives or minimum wage workers. The straw men are paid a certain amount of money for the use of their accounts. The intermediary accounts are changed constantly. The sums collected in the bank accounts of those persons are withdrawn in cash from the banks or from ATMs, transferred to the bank accounts of persons/companies established for this purpose, or transmitted to an offshore corporation.	
Indicators	• Financial activities and transactions inconsistent with their customer profile • Correct documents not filed with the tax authority • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Transaction is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile

Case Study 98 – Ukraine	
The money laundering scheme of former high-ranking officials of Ukraine was conducted via Ukrainian banking institutions and foreign banks. A number of non-resident companies (mostly registered in Panama, Cyprus, BVI, UK and Belize) linked by constituent-officials and business relations invested a considerable amount of funds in Ukraine (bought internal government bonds, transferred significant amounts of funds to deposit accounts in Ukraine and made contributions to the authorised capital of Ukrainian enterprises). According to the analysis of information on IP-addresses used to access business accounts, all the investments were managed from one management centre.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Multiple bank accounts without good reason • Bank accounts in multiple international jurisdictions without good reason • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client • Funds are sent to, or received from, a foreign country when there is no apparent connection between the country and the client

Case Study 99 – United States	
US authorities identified front companies used to conceal the ownership of certain US assets by Bank Melli, which was previously designated by the US authorities for providing financial services to entities involved in Iran's nuclear and ballistic missile program. Bank Melli was also subject to a call for enhanced vigilance in UNSCR 1803. The Department of Justice (DOJ) obtained the forfeiture of substantial assets controlled by the Government of Iran. These assets included a 36-story office tower in Manhattan at 650 5th Avenue having an appraised value of more than USD 500 million, other properties, and several million dollars in cash. The ownership the office tower was split between Bank Melli (40%) and the Alavi Foundation (60%), which provided services to the Iranian government, such as transferring funds from the office tower to Bank Melli.	
Indicators	• Legal person or arrangement incorporated/formed in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk • Correct documents not filed with the tax authority

	• Designated persons or groups • Funds are sent to, or received from, a jurisdiction that is considered to pose a high money laundering or terrorism financing risk

Case Study 100 – United States	
An individual organised a loan-fraud pyramid scheme to falsely inflate the sales and revenues of his company. His company served as a front. The scheme involved his wife and son. The defendants created numerous legal entities, including trusts, corporations/LLCs to open bank accounts to manage the illicit funds and conceal the ownership and involvement in the scheme. The defendants used the help of a legal professional (attorney) to create a number of legal entities, and diverted loans for the company for private benefit, including gems and jewellery. The attorney involved helped to sell the jewellery (which was an asset of the trust). The address of the attorney (then deceased) was used to move money from two different accounts. The investigation obtained legitimate financial records from third parties via subpoena as corporate records held by the organisation were found to be fabricated. The assets held by the defendant were identified by interviewing third parties to determine the true ownership. Additional information was obtained via the interview of tax return preparer. Standard financial investigative techniques were used to identified several trusts/trustees and legal persons.	
Indicators	• Multiple bank accounts without good reason • Correct documents not filed with the tax authority • Discrepancy between purchase and sales invoices • Fabricated corporate ownership records • Family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • Transaction is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile • Transaction involves a professional intermediary without due cause or apparent justification

Case Study 101 – United States
The defendant operated a mortgage broker business and several other companies that owned and managed real estate. He used nominee accounts, shell

Case Study 101 – United States	
corporations and other schemes to conceal his ownership. The scheme involved the purchase of properties owned by entities that the defendant controlled through an employee. The purchases were financed through loans. In connection with the loan applications, the defendant and others submitted fraudulent information related to the financial position of the borrower or purchaser, fraudulent appraisals that overstated the value of the collateral, and other documents that contained other material misrepresentations. The subject would "sell" commercial property owned by an entity he controlled to another entity that he controlled at highly elevated prices. The purchases were financed through fraudulent loan applications and through the submission of fraudulent documents. Also, the defendant altered invoices directed to one of the entities by inflating the cost of the work listed on the original invoices to make it falsely appear as though improvements had been made to the properties serving as collateral for the loans.	
Indicators	• Falsified records or counterfeited documentation • Inflated asset sales between entities controlled by the same beneficial owner • Nominee owners and directors including informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise • No real business activities undertaken

Case Study 102 – United States	
Individual 1, a US Citizen and resident of Belize, incorporated more than 5 000 shell companies in Belize and the West Indies to facilitate numerous securities and tax fraud schemes. Individual 2, a dual US and Canadian citizen, was the secret owner of an international broker-dealer and investment management company based in Panama City, Panama, and Belize City, Belize. There were 3 inter-related schemes: 1) fraudulent stock promotion and price manipulation; 2) circumventing capital gains taxes under the Foreign Account Tax Compliance Act (FATCA); 3) laundering more than USD 250 million in profits through unidentifiable debit cards and attorney escrow accounts. Individual 2 used the services of aUS-based lawyer to launder the more than USD 250 million generated through his stock manipulation of a number of US companies – directing the fraud proceeds to five law firm accounts and transmitting them back to members of the scheme and its co-conspirators. These concealment schemes also enabled Individual 2 to evade reporting requirements to tax authorities.	
Indicators	• Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Correct documents not filed with the tax authority • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense

	• Nominee owners and directors • Transaction involves a professional intermediary without due cause or apparent justification • Transaction involves the transfer of shares in an off-market sale

Case Study 103 – United States	
A Honduran PEP allegedly solicited and accepted USD 2.08 million in bribes from a Honduran technology company, in exchange for prioritising and expediting payments under a USD 19 million contract with the government agency to organise and digitise state records. The technology company allegedly sent wire transfers through another company to the PEP totalling approximately USD 2.08 million through an affiliate company located in Panama, which was owned by nominees. The bribe proceeds were then allegedly laundered into the United States and used to acquire real estate in the New Orleans area. Certain properties were titled in the name of companies controlled by the PEP's brother in an effort to conceal the illicit source of the funds as well as the beneficial ownership. One company used to hold title was a used-car dealership, and the other was a shell company which at one point counted the PEP among its members. Most of the real properties allegedly acquired with bribe proceeds were titled in the names of the companies.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre • Legal person or arrangement regularly sends money to low-tax jurisdictions or international trade or finance centres • Nominee owners and directors • Transfer of real property from a natural to a legal person in an off-market sale

Case Study 104 – United States
The defendants engineered a conspiracy to sell fraudulent renewable energy credits through the use of shell and shelf companies in the United States in order to receive renewable energy tax credits from the US government for renewable fuels never produced, and to launder those illicit proceeds for their own benefit. Among their ill-gotten gains from these proceeds were various assets including real estate, boats, cars, watches, and gold. During the course of their investigation, law enforcement determined that the defendant directed a network of his professional contacts to purchase shelf companies throughout the United States, to serve as purported purchasers of renewable fuel and purported sellers of feedstock. The use of shelf companies was

discovered by interviewing the nominees who had opened bank accounts on behalf of those companies and through search warrants executed on a number of the businesses.	
Indicators	• Long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities • Multiple bank accounts without good reason • Falsified paper trail • Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense • Nominee owners and directors

Case Study 105 – United States	
The US Department of the Treasury's Office of Foreign Assets Control (OFAC) designated a foreign PEP under the Foreign Narcotics Kingpin Designation Act for playing a significant role in international narcotics trafficking, with a straw man also designated for providing material assistance, financial support, or goods or services in support of and acting on behalf of the PEP. In addition, OFAC designated shell companies tied to the straw man that were used to hold real estate.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Designated persons or groups • No real business activities undertaken

Case Study 106 – Vatican	
In this case, Company A incorporated in the Caribbean was entitled to issue bearer shares. Company A was managed by a branch of an international bank registered in the same country whose headquarters is registered in Europe. A South American politically exposed person was appointed as authorised signatory for an account held by company A at the headquarters of the bank. The same PEP was under investigation for racketeering, corruption, and ML. This individual appears to be the beneficial owner of company A. The company attempted a wire transfer of EUR 1 000 0000 from the bank headquarters to a charitable entity in a branch of another European bank. The charitable entity refused the transaction and reported the case to the domestic authorities. Shortly after the attempted transfer, Company A was dissolved.	
Indicators	• Politically exposed persons, or have familial or professional associations with a person who is politically exposed • Under investigation or have known connections with criminals • Legal person or arrangement incorporated/formed in a low-tax jurisdiction

	or international trade or financial centre • The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client

ANNEX D. SOURCES OF INFORMATION AND TECHNIQUES TO DISCOVER BENEFICIAL OWNERSHIP

OVERVIEW

1. During the development of this report, a range of techniques to discover beneficial ownership was identified. However, due to the nature of the analysed case studies, which generally involved active law enforcement investigations, the identified techniques centred primarily on traditional law enforcement capabilities and tools. As such, the tools and techniques available to financial institutions, professional intermediaries, and intelligence agencies to reliably identify and verify beneficial ownership prior to forming a suspicion and commencing a formal investigation are more difficult to ascertain and describe.

2. This is somewhat unsurprising. As this report has demonstrated, the concealment of beneficial ownership information is the cornerstone of many money laundering and terrorism financing schemes, and proving beneficial ownership presents one of the greatest challenges for financial institutions and competent authorities. However, some simple tools are available to financial institutions and competent authorities to assist in the identification of high-risk or suspicious customers and activities. These are outlined in this Annex.

SOURCE OF INFORMATION TO ASSIST IN THE IDENTIFICATION OF BENEFICIAL OWNERSHIP

3. In its 2014 guidance paper on *Transparency and Beneficial Ownership*[78], the FATF outlined some mechanisms and sources for obtaining beneficial ownership information of legal persons, including: company registries, financial institutions, DNFBPs, the legal person itself, and other national authorities, such as tax authorities or stock exchange commissions. These mechanisms are outlined in greater detail in that guidance report; however, the focus of the guidance report is on the implementation of policy initiatives to improve transparency of beneficial ownership, rather than on investigative techniques, and may therefore be of limited value to financial institutions and competent authorities.

4. Analysis of the case studies provided in support of this report identified the following common sources of information used to identify beneficial ownership:

Banks and financial institutions

5. Banks were the most common source of information used by competent authorities to identify beneficial ownership, and were involved in over half of the investigations analysed. Financial institutions represent a key source of information

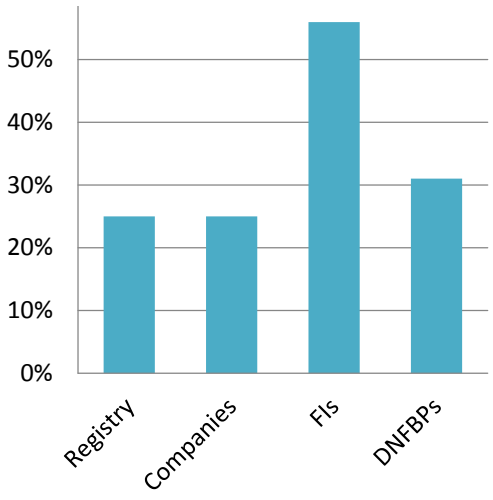
[78] FATF, 2014: p.18

for FIUs and competent authorities; however, there is limited ability for financial institutions to leverage the information held by other financial institutions. Information held by banks also relies on the quality of the information provided by a client. This is particularly relevant for the sharing of suspicions and risk profiles between banks, or within multi-national banks. Further work is being conducted globally to improve private-private and public-private information sharing to alleviate this issue.

Professional intermediaries

6. In approximately one-third of cases, information was provided by DNFBPs. Information held by professional intermediaries can be extensive; however, in countries where DNFBPs are not obliged to conduct CDD, the information held by professionals may not be reliable. Furthermore, the presence of LPP and client confidentiality can inhibit efforts to obtain information from intermediaries.

Figure 3. Sources of beneficial ownership information



Companies and company registries

7. Beneficial ownership information held by companies and in company registries were used in only one-quarter of cases. In many cases, these registries were general property or corporate registries, rather than beneficial ownership registries. However, many of the cases included in the sample predate the work being done globally in this area.

Traditional law enforcement techniques

8. In one-quarter of cases, beneficial ownership was not known, the source of beneficial ownership information was not disclosed, or beneficial ownership was not discovered using information held under Recommendations 24 and 25. Often, in these cases, beneficial ownership was determined through surveillance.

9. Analysis of the case studies demonstrated that competent authorities and law enforcement can more easily obtain accurate beneficial ownership from financial institutions than from DNFBPs. Banks featured in 90% of cases, and were a source of beneficial ownership in over half the case studies. While 76% of cases included some type of DNFBP, in only one third did DNFBPs act as a source of beneficial ownership information for authorities – perhaps due to issues of complicity, legal professional privilege, or simply a lack of implementation of beneficial ownership record-keeping requirements in these sectors.

10. Other sources of beneficial ownership include:

Registers of Beneficial Ownership

11. In recent years, and particularly after the *Anti-Corruption Summit* held in London in 2016, many countries have implemented, or commenced work to implement, registers of beneficial ownership. In countries where they have been implemented, registers of beneficial ownership will contain useful information relevant to determining true beneficial ownership and control. However, care should be taken to analyse the veracity of the information held on registers of beneficial ownership, as it is often self-reported and rarely vetted by a central administrating body.

Shareholder register

12. In some instances, particularly in jurisdictions that require companies to actively collect such information up front, shareholder registers will contain sufficient information to identify controlling interests in a company. However, many criminals will seek to limit their exposure by concealing their share ownership. In these instances, the shareholder register may indicate other controlling persons (natural or legal) who may be acting on behalf of the beneficial owner, or may be controlled by the beneficial owner.

Commercial databases

13. A large number of commercial databases are available to law enforcement in developing their investigations and to financial institutions in identifying risk. Use of these databases provides a quick means of obtaining a wide variety of useful information and leads. A lack of information on commercial databases can be an indicator of the use of a shell or a shelf corporation. This information, along with other investigative techniques can be an effective tool to unravel the legal arrangement of an entity.

Professional nominees

14. As discussed in this report, some countries require all legal persons incorporated under domestic laws to maintain a physical presence in that country. In some instances, these countries also require a domestic national to serve as a director or controlling shareholder of the company. Many professional intermediaries, particularly TCSPs, offer nominee directorship and company management services to foreign clients to assist in meeting these legal requirements. These professional nominees will often maintain records of their customer, and while these records may not prove true beneficial ownership and control, they will assist in tracing and unravelling the broader control structure of the company.

MECHANISMS AVAILABLE TO COMPETENT AUTHORITIES

15. While there is a range of information sources available to assist in the identification of beneficial ownership, the reliability of some of these sources is often questionable. In order to fully unravel complicated ownership structures and prove ownership and control (and thereby prove criminality where relevant) law

enforcement and competent authorities require access to a broader range of intelligence and evidence collection capabilities. The key capabilities relevant to the identification and verification of beneficial ownership are outlined below.

Mutual legal assistance

16. Mutual legal assistance is the cornerstone of most major investigations that involve a transnational corporate structure or international financial flows. However, many law enforcement and intelligence practitioners have reported that delays in mutual legal assistance requests are one of the key inhibiters in an investigation. Therefore, while the information available via mutual legal assistance is often invaluable, it is not necessarily a quick or easy solution to unravelling opaque transnational ownership structures.

Intelligence disclosures and sharing

17. In addition to mutual legal assistance, which is often used to exchange information for evidentiary purposes, FIUs and competent authorities will regularly exchange information with international partners for intelligence purposes only. These intelligence exchanges can be spontaneous or subsequent to a request, and can greatly assist FIUs to understand the ownership and control of complex international structures, or the financial activities of those structures.

Taxation databases

18. Taxation databases are a useful means of identifying indicators of criminality and schemes designed to obscure beneficial ownership. By comparing previous tax assessments to bank statements, financial transactions, assets, and the lifestyle of an individual, it is possible to identify anomalous financial activities. Further investigation often uncovers dubious control structures or corporate dealings designed to conceal beneficial ownership.

Asset disclosure databases

19. Many countries require public officials to disclose their assets on publicly accessible databases. These databases can be a useful tool to gauge the wealth and asset holdings of public officials, and can assist in identifying anomalous financial activities. Furthermore, the absence of an asset that is clearly controlled by the official, their family, or their corporate interests from the registry may be an indication of efforts to conceal their ownership of the asset.

Subpoenas for information

20. Subpoenas are often coercive in nature, and are generally used to compel the recipient to provide the required information. However, they can also offer a range of protections and indemnities to the recipient. For this reason, subpoenas are often used in situations where a competent authority and financial institution are working collaboratively on an investigation, despite the fact that the financial institution is a willing party to the investigation.

Covert surveillance

21. Most law enforcement and intelligence agencies have access to covert surveillance capabilities, including telecommunication interception and physical surveillance. These techniques can be used to identify connections between associates and identify control over assets or companies.

Informants and witnesses

22. Some intelligence and law enforcement agencies have the capability to coerce witnesses to give information or documents relating to an investigation. Often, these capabilities can only be utilised in certain limited circumstances, and the information gathered from these witnesses can often be used for intelligence purposes only (not evidence). However, these capabilities can be highly valuable in dissecting and understanding complicated corporate structures designed to conceal beneficial ownership and frustrate investigations.

Search Warrants

23. Search warrants are a standard law enforcement capability; however, they are an overt and intrusive capability that immediately announces law enforcement's interests and investigation into a person or company. For this reason, search warrants are often used towards the end of an investigation, rather than at the commencement. While search warrants are valuable evidence gathering tools, and can assist in proving beneficial ownership in court, they may have limited value in identifying beneficial ownership in the early stages of an investigation.

Multi-agency task forces

24. It is rare that any single agency has all of the information and capabilities required to unravel, understand, and prosecute complicated money laundering schemes designed to obscure beneficial ownership. Often, law enforcement agencies, intelligence agencies, taxation authorities, securities regulators, and other competent authorities are all required to successfully discover, understand and disrupt complex transnational schemes. Multi-agency task forces are a useful mechanism to co-ordinate investigative efforts, share information, and reduce duplication. The presence of a standing taskforce within a country allows for the quick deployment of resources and capabilities in response to emerging threats and opportunities.

Tools to identify potential efforts to obscure beneficial ownership

25. In addition to the sources of information described above, law enforcement and private sector have identified a number of novel approaches to collecting information relevant to the identification of risk indicators. In most cases, these tools are not suitable to discovering true beneficial ownership and control; however, they may reveal anomalous activities and indices that could assist in recognising high-risk individuals and companies. These tools are outlined below:

IP addresses

26. Many financial institutions and law enforcement agencies have begun to collect and analyse the Internet Protocol (IP) address of customers involved in a transaction. As the majority of financial transactions are now conducted online, the collection of IP address information can provide valuable insights into who is ordering a transaction, and where that transaction is being ordered from. It is likely that careful analysis of IP address information could identify situations where control is being exerted by an unknown third party, where control shifts from one person to another, where control of a domestic account is being exerted by a foreign influence, or where a person may be seeking to conceal their IP through the use of a virtual private network (VPN).

27. Furthermore, analysis of IP addresses collected by a financial institution may identify commonalities and control nexuses, where a single IP address is responsible for transaction requests for multiple accounts, customers, and beneficial owners. Instances of repeat IP addresses across numerous accounts may be indicative of a professional nominee, professional intermediary, or professional money launderer, and these accounts may deserve close monitoring.

Online maps and street-level images

28. Online maps and street-level images (such as those developed by Google and other search engines) are readily available online for a significant proportion of countries across the globe. These capabilities can serve a range of useful purposes, including the verification and analysis of addresses provided by customers and clients. In the past, service providers and financial institutions were often limited in their ability to critically analyse the address of an individual or company, particularly when engaging with customers and companies based in a foreign country. Today, a simple search of a company address has significant analytical potential.

29. By analysing the location of an address provided by a customer or company, as well as the physical appearance of that address from the street (where images are available), it is often possible to identify anomalies indicative of a shell company or an attempt to conceal the customer's true identity. Anomalies may include:

- the location is inconsistent with the financial profile of the customer
- the location is inconsistent with business profile of the company
- the physical appearance of the address is inconsistent with the size and nature of the company
- the address is a post box.

30. Addresses that appear anomalous may warrant enhanced due diligence and closer monitoring.

Media reporting

31. A number of cases analysed for this report involved financial institutions and professional intermediaries that identified suspicious transactions as a result of media reporting. Media reporting is a useful means of identifying potential

corruption, high-value government contracts, and high-profile corporate activities. While media reporting is not an indication of suspicious activities, it may assist in the identification of anomalous or high-risk activities.

32. Some media reporting is more specific and incriminating. In recent years, global consortiums of journalists, such as the International Consortium of Investigative Journalists, have undertaken widespread investigations into corruption, tax evasion, and money laundering. In two key instances[79], the investigations released leaked documents relating to the establishment of complex corporate structures and companies in low-tax jurisdictions by law firms on behalf of high-wealth individuals. While these leaked documents are not evidence of criminality or wrong-doing, they may be indicative of risk, and may warrant close consideration from a risk analysis perspective.

33. It is important to consider the source of the media reporting when assessing the validity and reliability of the information. Not all media sources are reliable, and care should be taken to validate or verify any intelligence derived from open sources.

Techniques to identify potential efforts to obscure beneficial ownership

34. There is a broad range of analytical techniques available to identify activities and trends indicative of the concealment of beneficial ownership, and of money laundering more broadly. This report will not attempt to list all such techniques; however, some key techniques identified by FIUs, competent authorities, and private sector representatives have been included below:

Identifying the beneficial owners of legal arrangements

35. Identifying the beneficial ownership of legal arrangements can pose significant challenges due to the number of actors that can exercise control or benefit from the arrangement. When considering the beneficial ownership of a trust, asking the following key questions may assist financial institutions and professional intermediaries to better understand key features of the arrangement:

- Who is the real settlor and what is the real source of funds?
- Who are the real beneficiaries i.e. for whose benefit are the trust assets managed?
- What is the trust's governance system and who are the real "natural persons exercising effective control"?

36. Seeking copies or extracts of tax or legal advice on the formation of the trust or an explanation from current advisers as to the purpose behind the formation of the trust will assist in answering some of these questions. Where such advice is not available, it may be possible to draw inferences from background information, although this can be less reliable.

[79] The 2015 leak of confidential documents from Panama-based law firm Mossack Fonseca, and the 2017 leak from Bermuda-based law firm, Appleby.

In the absence of the ability to identify BO, identify senior management personnel

37. As explained previously, beneficial ownership must involve some level of ultimate control, whether direct or indirect control. While the beneficial owner of a company may not be visible, the management structure is generally easier to ascertain. By analysing the directors and senior management of a company, it may be possible to discern whether one of them is the ultimate beneficial owner. Conversely, analysis of the activities and financial dealings of the management personnel may identify a third party exerting control from outside of the company.

In the absence of the ability to identify BO, identify individuals with control over transaction accounts/power of attorney

38. As with identifying the director and senior management of a company, identifying individuals who exert control over financial transaction accounts, or who have power of attorney over the company, may assist in identifying the beneficial owner. Although more difficult to discern, individuals with control over transaction accounts, and those with power of attorney, often have the power to exert control over a company or its finances. While many of these individuals will be employed in legitimate finance and legal areas of larger companies, those with no apparent connection to the company, or who are seemingly employed in unrelated areas of the company, could potentially be the beneficial owner of the company.

Search existing records for the same addresses or telephone numbers

39. As identified in this report, numerous professional intermediaries, particularly TCSPs, provide directorship and company management services to their clients. A key indicator of this activity is the use of a mailbox service for multiple clients. As a result, large numbers of shell companies, particularly those with foreign beneficial owners, will be registered to the same address and telephone number. By identifying commonly used addresses and numbers, it is possible to identify companies that utilise a directorship or company management service. It may also indicate the use of professional nominees, and the fact that the company is a shell company.

40. Companies that are established and managed by TCSPs will often share the same bulk address. Additionally, these TCSPs will often establish banking relationships for their clients at the same financial institutions. Analysis of customer databases by these financial institutions is likely to identify commonly used addresses and telephone numbers indicative of bulk company incorporation and management. These customers may warrant enhanced due diligence to ensure that beneficial ownership and control details are recorded correctly.

Meet high-risk clients face-to-face

41. One of the findings of this report has been that the increased use of internet communications and the decrease in face-to-face client interactions have exacerbated challenges associated with identifying and proving beneficial ownership and control. This is largely due to the ease with which individuals can conceal their identity in the absence of face-to-face interactions. While governments and FinTech companies are investing significant resources to improve identification

processes in the digital age, including the provision of document verification systems and digital identities, the lack of face-to-face interactions will continue to pose a vulnerability to CDD and KYC processes.

42. One solution is to increase face-to-face interactions with high-risk clients or customers, including through the use of publicly available video-conference facilities. By meeting with the client directly, the financial institution can verify their identity against photographic identification documentation and better understand the level of control they exert over the company or assets involved. It is likely that even a brief discussion with a client about their activities and business dealings will allow the financial institution to identify indicators of the use of nominee directors and indirect control by a third party.

Analysis of cross-border wire transfers

43. The regular and proactive analysis of cross-border wire transfers is often instrumental in identifying true ownership and control structures. Those FIUs that receive cross-border wire transfer reports have reported the importance of those reports and their value in tracing money flows and identifying likely beneficial ownership. Financial institutions have direct and unfettered access to cross-border wire transfer information, and are therefore ideally placed to identify anomalous money flows on a global scale. Indicators of suspicious activities indicative of an attempt to conceal beneficial ownership are outlined in Annex E to this report.

Additional resources

44. For more examples of, and ideas on, the use of technology to verify beneficial ownership, see the Tax Justice Network's *Technology and Online Beneficial Ownership Registries: Easier to create companies and better at preventing financial crimes* report[80] and the FATF 2014 guidance on *Transparency and Beneficial Ownership*.[81]

80 Knobel, A., 2017.

81 FATF, 2014.

ANNEX E. INDICATORS OF CONCEALED BENEFICIAL OWNERSHIP

During the development of the report on the vulnerabilities associated with the concealment of beneficial ownership, 106 case studies were submitted by the FATF and Egmont Group members. Through the analysis of these case studies, as well as discussions with financial intelligence units (FIUs), competent authorities, and the private sector, a range of indicators of the concealment of beneficial ownership was identified. These risk indicators are summarised below. It is important to note that this list is not exhaustive, and other indicators may be identified.

Indicators about the client or customer

1. The client is reluctant to provide personal information.
2. The client is reluctant or unable to explain:
    - their business activities and corporate history
    - the identity of the beneficial owner
    - their source of wealth/funds
    - why they are conducting their activities in a certain manner
    - who they are transacting with
    - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
3. Individuals or connected persons:
    - insist on the use of an intermediary (either professional or informal) in all interactions without sufficient justification
    - are actively avoiding personal contact without sufficient justification
    - are foreign nationals with no significant dealings in the country in which they are procuring professional or financial services
    - refuse to co-operate or provide information, data, and documents usually required to facilitate a transaction
    - are politically exposed persons, or have familial or professional associations with a person who is politically exposed
    - are conducting transactions which appear strange given an individual's age (this is particularly relevant for underage customers)
    - have previously been convicted for fraud, tax evasion, or serious crimes
    - are under investigation or have known connections with criminals
    - have previously been prohibited from holding a directorship role in a company or operating a Trust and company service provider (TCSP)
    - are the signatory to company accounts without sufficient explanation

- conduct financial activities and transactions inconsistent with their customer profile
- have declared income which is inconsistent with their assets, transactions, or lifestyle.

4. Legal persons or legal arrangements:

- have demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities
- describe themselves as a commercial business but cannot be found on the internet or social business network platforms (such as LinkedIn, XING, etc.)
- are registered under a name that does not indicate the activity of the company
- are registered under a name that indicates that the company performs activities or services that it does not provide
- are registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations
- use an email address with an unusual domain (such as Hotmail, Gmail, Yahoo, etc.)
- are registered at an address that does not match the profile of the company
- are registered at an address that cannot be located on internet mapping services (such as Google Maps)
- are registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service
- where the director or controlling shareholder(s) cannot be located or contacted
- where the director or controlling shareholder(s) do not appear to have an active role in the company
- where the director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees
- have declared an unusually large number of beneficiaries and other controlling interests
- have authorised numerous signatories without sufficient explanation or business justification
- are incorporated/formed in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk
- are incorporated/formed in a low-tax jurisdiction or international trade or finance centre
- regularly send money to low-tax jurisdictions or international trade or finance centre

- conduct a large number of transactions with a small number of recipients
- conduct a small number of high-value transactions with a small number of recipients
- regularly conduct transactions with international companies without sufficient corporate or trade justification
- maintain relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation
- receive large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification
- maintain a bank balance of close to zero, despite frequent incoming and outgoing transactions
- conduct financial activities and transactions inconsistent with the corporate profile
- are incorporated/formed in a jurisdiction that does not require companies to report beneficial owners to a central registry
- operate using accounts opened in countries other than the country in which the company is registered
- involve multiple shareholders who each hold an ownership interest just below the threshold required to trigger enhanced due diligence measures.

5. There is a discrepancy between the supposed wealth of the settlor and the object of the settlement.

6. Individuals, legal persons and/or legal arrangements:

- make frequent payments to foreign professional intermediaries
- are using multiple bank accounts without good reason
- are using bank accounts in multiple international jurisdictions without good reason
- appear focused on aggressive tax minimisation strategies
- are interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without sufficient commercial explanation
- demonstrate limited business acumen despite substantial interests in legal persons
- ask for short-cuts or excessively quick transactions, even when it poses an unnecessary business risk or expense
- appear uninterested in the structure of a company they are establishing
- require introduction to financial institutions to help secure banking facilities

- request the formation of complex company structures without sufficient business rationale
- have not filed correct documents with the tax authority
- provide falsified records or counterfeit documentation
- are designated persons or groups
- appear to engage multiple professionals in the same country to facilitate the same (or closely related) aspects of a transaction without a clear reason for doing so.

7. Examination of business records indicate:

- a discrepancy between purchase and sales invoices
- double invoicing between jurisdictions
- fabricated corporate ownership records
- false invoices created for services not carried out
- falsified paper trail
- inflated asset sales between entities controlled by the same beneficial owner
- agreements for nominee directors and shareholders
- family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements
- employees of professional intermediary firms acting as nominee directors and shareholders
- the resignation and replacement of directors or key shareholders shortly after incorporation
- the location of the business changes frequently without an apparent business justification
- officials or board members change frequently without an appropriate rationale.

8. Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense.

9. Simple banking relationships are established using professional intermediaries.

Indicators of shell companies

10. Nominee owners and directors:

- formal nominees (formal nominees may be “mass” nominees who are nominated agents for a large number of shell companies)
- informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise.

11. Address of mass registration (usually the address of a TCSP that manages a number of shell companies on behalf of its customers)

12. Only a post-box address (often used in the absence of professional TCSP services and in conjunction with informal nominees)

13. No real business activities undertaken

14. Exclusively facilitates transit transactions and does not appear to generate wealth or income (transactions appear to flow through the company in a short period of time with little other perceived purpose)

15. No personnel (or only a single person as a staff member)

16. Pays no taxes, superannuation, retirement fund contributions or social benefits

17. Does not have a physical presence.

Indicators about the transaction

18. The customer is both the ordering and beneficiary customer for multiple outgoing international funds transfers

19. The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client

20. Finance is provided by a lender, whether a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification

21. Loans are received from private third parties without any supporting loan agreements, collateral, or regular interest repayments

22. The transaction:

- is occurring between two or more parties that are connected without an apparent business or trade rationale
- is a business transaction that involves family members of one or more of the parties without a legitimate business rationale
- is a repeat transaction between parties over a contracted period of time
- is a large or repeat transaction, and the executing customer is a signatory to the account, but is not listed as having a controlling interest in the company or assets
- is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile
- is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile

- appears cyclical (outgoing and incoming transactions are similar in size and are sent to, and received from, the same accounts, indicating that outgoing funds are being returned with little loss) (aka "round-robin" transactions)
- involves the two-way transfer of funds between a client and a professional intermediary for similar sums of money
- involves two legal persons with similar or identical directors, shareholders, or beneficial owners
- involves a professional intermediary without due cause or apparent justification
- involves complicated transaction routings without sufficient explanation or trade records
- involves the transfer of real property from a natural to a legal person in an off-market sale
- involves the use of multiple large cash payments to pay down a loan or mortgage
- involves a numbered account
- involves licensing contracts between corporations owned by the same individual
- involves the purchase of high-value goods in cash
- involves the transfer of (bearer) shares in an off-market sale
- a loan or mortgage is paid off ahead of schedule, incurring a loss
- includes contractual agreements with terms that do not make business sense for the parties involved
- includes contractual agreements with unusual clauses allowing for parties to be shielded from liability but make the majority of profits at the beginning of the deal
- is transacted via a digital wallet.

23. The funds involved in the transaction:

- are unusual in the context of the client or customer's profile
- are anomalous in comparison to previous transactions
- are sent to, or received from, a foreign country when there is no apparent connection between the country and the client, and/or
- are sent to, or received from, a low-tax jurisdiction or international trade or finance centre
- are sent to, or received from, a jurisdiction that is considered to pose a high money laundering or terrorism financing risk.

24. An asset is purchased with cash and then used as collateral for a loan within a short period of time.

25. Unexplained use of powers of attorney or other delegation processes (for example, the use of representative offices).

26. Unexplained use of express trusts, and/or incongruous or unexplained relationships between beneficiaries (or persons who are objects of a power) and the settlor.

27. Unexplained or incongruous classes of beneficiaries in a trust.

www.fatf-gafi.org
egmontgroup.org

July 2018

Concealment of Beneficial Ownership

Legal persons, legal arrangements and professional intermediaries play important roles in facilitating business growth and development. But, they can also be misused, providing criminals with structures that help them conceal the proceeds of crime.

This joint FATF-Egmont Group study looks at the mechanisms and techniques that can be used to obscure the ownership and control of illicitly obtained assets, drawing on over 100 case studies, the experiences of law enforcement experts, the outcomes of FATF Mutual Evaluation Reports, and the insights provided by academic reports and other studies.

The report aims to raise awareness with national authorities, financial institutions and other professional service providers about the risks involved.

Appendix V:

CFATF & FATF, *FATF Report: Money Laundering Using Trust and Company Service Providers* (Paris: FATF, 2010)

CARIBBEAN FINANCIAL ACTION TASK FORCE

FINANCIAL ACTION TASK FORCE GROUPE D'ACTION FINANCIÈRE

FATF Report

Money Laundering Using Trust and Company Service Providers

October 2010

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

THE CARIBBEAN FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the CFATF, please visit the website:

WWW.FATF-GAFI.ORG

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS AND ACRONYMS

AML/CFT	Anti-Money Laundering/Counter-Terrorism Financing
CDD	Customer due diligence
CFATF	Caribbean Financial Action Task Force
CSP	Company Service Provider
G-20	Group of Twenty Finance Ministers and Central Bank Governors
FATF	Financial Action Task Force
FSF	Financial Stability Forum
IAIS	International Association of Insurance Supervisors
IOSCO	International Organisation of Securities Commissions
KYC	Know your customer
ML/FT	Money Laundering/Financing Terrorism
OECD	Organisation for Economic Co-operation and Development
OGBS	Offshore Group of Banking Supervisors
PEP	Politically Exposed Person
RBA	Risk Based Approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
TSP	Trust Service Provider
WGEI	Working Group on Evaluations and Implementation (FATF Working Group)

EXECUTIVE SUMMARY

1. Trust and Company Service Providers (TCSPs) play a key role in the global economy as financial intermediaries, providing an important link between financial institutions and many of their customers. They provide often invaluable assistance to clients in the management of their financial affairs and can therefore significantly impact transactional flows through the financial system.

2. There have been a number of studies over the years which highlight the use of legal persons and legal arrangements to facilitate money laundering. Little information is available at the current time with regard to the use of such structures in the financing of terrorism but this does not mean that such vehicles have not or cannot be used in this regard. Therefore, although the research provided will centre on the role that TCSPs have played with regard to combating money laundering, it is hoped that this report will be of value in relation to the fight against both money laundering and terrorist financing.

3. TCSPs are often involved in some way in the establishment and administration of most legal persons and arrangements; and accordingly in many jurisdictions they play a key role as the gatekeepers for the financial sector. This report provides a number of case studies which demonstrate that TCSPs have often been used, wittingly or unwittingly, in the conduct of money laundering activities. The following factors are borne out by the case studies as contributing to the crime of money laundering:-

- Weak or ineffective Anti-Money Laundering/Counter-Terrorism Financing (AML/CFT) frameworks in some jurisdictions, in areas which can impact the operation of TCSPs;
- The presence in the TCSP sector of persons that are willing to get involved in or to perpetrate criminal activities; and
- The proliferation of TCSPs whose management/staff do not have the required expertise, knowledge or understanding of key matters that are relevant to the operation of their business, such as their clients' affairs. This lack of knowledge and skill can promote and facilitate illegal activities.

4. In this regard, it is important to note that a number of jurisdictions have chosen not to recognise or put in place an AML/CFT supervisory framework for the TCSP sector because of the nature of their legal systems. However, there are still persons in those jurisdictions that are carrying out, as a business, the activities that can be attributed to this sector. Other jurisdictions have had difficulty in developing an appropriate oversight regime for TCSPs due to various complexities related to the number and type of persons carrying out the related services. These issues have resulted in potentially important gaps in the global network to address the money laundering risks associated with this sector.

5. The FATF has already established standards which apply to this sector. In addition there are other bodies that have done significant work in this area and have developed some key principles and guidelines that can positively impact the operation of TCSPs. Notwithstanding, consideration should be given to additional work to enhance the international requirements that apply to TCSPs, so that jurisdictions can implement more effective AML/CFT measures in relation to their TCSP sectors.

CHAPTER 1: INTRODUCTION AND BACKGROUND

1.1 Introduction

6. Over the last five years, a number of important studies have been conducted that have explored issues relating to the misuse of corporate vehicles for illicit purposes including money laundering and terrorist financing. Despite the considerable body of work in this area, there remains a need for further research into the operation, regulation and supervision of TCSPs; the challenges caused by the illegal use of TCSPs; and the ineffective implementation of the international AML/CFT requirements relating to TCSPs.

7. This typologies research project will therefore evaluate the effectiveness of the practical implementation of the Financial Action Task Force Forty Recommendations and Nine Special Recommendations (the FATF 40 + 9 Recommendations) as they relate to TCSPs. The FATF Recommendations relating to beneficial ownership information, governance and transparency will also be used to determine what is necessary to ensure there is effective cooperation between agencies and jurisdictions. Currently, as part of the preparation for the 4th Round of country evaluations, the FATF is assessing and clarifying Recommendations 33 and 34 in order to determine how the important purposes of these Recommendations can be most effectively achieved. The key findings from this typology study will be fed into these discussions. In addition, consideration will be given to whether the international standards relating to the oversight and operation of TCSPs should contain some of the requirements imposed regarding oversight of financial institutions.

1.2 Need for Typology

8. There has been an increasing international focus on the misuse of legal vehicles and, more specifically, the use of TCSPs to help facilitate this misuse. In recent years, the use of complex multi-jurisdictional legal structures has continued to cause concern for many international organisations, governments and national regulatory authorities. The international bodies which are often seeking to exert pressure for more transparency in the formation and administration of legal vehicles include the G20, the Financial Stability Forum (FSF), the European Commission, the International Organisation of Securities Commissions (IOSCO) and the Organization for Economic Co-operation and Development (OECD). The need for enhanced effective international cooperation in this regard has also been frequently highlighted.

9. By way of background and for the purposes of this project, the term 'Trust and Company Service Providers' has the meaning used by the FATF[1] and thus includes **all** those persons and entities that, on a professional basis, participate in the creation, administration and management of trusts and corporate vehicles. There are a considerable number of jurisdictions, both large and small, with sizeable TCSP sectors and many are still grappling with how to best exercise effective control over the activities of TCSPs. It is important to note that there are also many jurisdictions that do not specifically classify TCSPs as a separate and distinct sector. However, in these jurisdictions trust and company services may well be provided by lawyers and other professionals, who may be regulated.

10. Whilst the majority of TCSPs appear to be established for legitimate purposes, it is clear from the research that some TCSPs are being used, unwittingly or otherwise, to help facilitate the

[1] As defined in FATF Recommendation 12 and the Glossary to the FATF 40+9 Recommendations.

misuse of trust and corporate vehicles. Criminal organisations and individuals may use TCSPs to assist with illicit activities by seeking professional services and advice on the most appropriate vehicles or jurisdictions to use to further their ill-intended agendas. This potential for misuse of TCSPs has contributed to the extension of the scope of the FATF 40 + 9 Recommendations to lawyers, accountants and other TCSPs. The changes relate particularly to Recommendation 5, which addresses customer due diligence and record-keeping; and Recommendations 33 and 34, which address transparency of legal persons and arrangements.

11. Although a number of jurisdictions do license and regulate TCSPs, there are no internationally agreed "fit and proper" requirements[2] imposed on the providers of these services. Further, other than the requirements set out by the FATF, the Offshore Group of Banking Supervisors is the only body which has done work to develop standards for the establishment and overall operation of these entities to enhance their integrity, transparency and effectiveness, particularly with regard to addressing money laundering and terrorist financing. Their work will be discussed later in this report.

1.3 Scope

12. The overarching aim of this project is to consider, with the support of cases, how the effectiveness of the FATF and other international standards, as applied to the TCSPs, can be enhanced. The project will seek to evaluate:

i. The role of TCSPs in the detection, prevention and prosecution of money laundering and terrorist financing;

ii. The effectiveness of the FATF 40 + 9 Recommendations as they apply to TCSPs; and

iii. The potential need for additional international requirements or sector-specific international standards for TCSPs.

13. The following are key issues that need to be addressed:

i. Assessment of the adequacy and role that the information, required from TCSPs in accordance with the FATF 40 + 9 Recommendations, plays in combating money laundering and terrorist financing.

ii. Determination of the difficulties experienced by TCSPs in obtaining the FATF required information from clients and the steps that need to be taken to overcome these difficulties.

iii. Assessment of the national and international cooperation issues ensuring and/or enhancing access to and exchange of, in particular, information on beneficial owners.

iv. Evaluation of the following standard-setting related questions:

   a. How can the FATF Recommendations and guidance more effectively address the role of TCSPs in the combating of money laundering and terrorist financing?

---

[2] As referred to in the interpretative note of FATF Recommendation 23: www.fatf-gafi.org/document/28/0,3343,en_32250379_32236920_33988956_1_1_1_1,00.html#Interpretative_Note_to_r_23

b. Is there a need for an international standard for TCSPs to address issues such as the "fit and proper" prerequisite and other minimum requirements (*e.g.*, Systems and Controls, Corporate Governance, Authorization criteria)?

v. Assessment of what steps can and should be taken to ensure effective implementation of the international requirements.

14. Other benefits which may result from the project include:

- Addressing concerns about the impact of the operation of TCSPs on Money Laundering and Terrorist Financing;
- Enhancing the framework under which TCSPs operate; and
- Broadening the knowledge and understanding of TCSPs more generally.

1.4 Methodology

15. This typology is in essence a follow up to the October 2006 FATF Typologies Study on "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" that highlights the vital role that beneficial ownership information can play in the detection and prevention of the misuse of corporate vehicles. Other studies in this area were also taken into consideration, and they are discussed in further detail below.

16. Between late September and early October 2009, a Concept Note regarding the proposed TCSP typologies exercise was developed. During the 30th Plenary Meeting of the Caribbean Financial Action Task Force (CFATF) in October 2009, the Concept Note was distributed to delegates to encourage discussion and garner support for the initiative. At the FATF/CFATF Joint Typologies meeting held in the Cayman Islands in November 2009, representatives from Belgium, Belize, Bermuda, CFATF, the Cayman Islands, the Channel Islands, Italy, the Netherlands, the Netherlands Antilles, St. Vincent and the Grenadines, the United States of America, the British Virgin Islands, as well as an industry representative from the TCSP sector in one of these jurisdictions, all attended and participated in a workshop focussed on the TCSP sector. During the workshop, the TCSP Project Working Group was created with the objective of conducting research and preparing a report on money laundering and terrorist financing using TCSPs. The following jurisdictions joined the working group and contributed to the study: Bermuda (as project Chair), the British Virgin Islands, the Cayman Islands, Jersey, the Netherlands Antilles, and the United States of America. During the course of the study, the project working group also received assistance from Austria, the World Bank, Guernsey and the Offshore Group of Banking Supervisors (OGBS). The secretariats of both the FATF and CFATF provided invaluable assistance and support throughout the various stages of the project.

17. As the starting point for the research project, the Project Working Group agreed that questionnaires would be developed and circulated to FATF and CFATF members, requesting that they provide relevant information on their TCSP sectors. In particular, information was sought on the breadth and scope of the services provided by this sector; the legislative framework vis-à-vis corporate vehicles; the nature of regulatory and AML/CFT supervision and monitoring for this sector, if any; and any problems being encountered by the sector in fulfilling mandated requirements. Most importantly, questionnaire respondents were required to provide case studies demonstrating either the misuse of TCSPs for AML/CFT purposes, or their importance in stemming the money laundering and financing of terrorism (ML/FT) tide.

18. The questionnaire was designed in two formats: a long-form, comprehensive version and a short-form, streamlined version. It was envisaged that by using two versions of the questionnaire, the Project Working Group would be able to broaden its sample in efforts to capture a wider audience.

Given this, the long form was sent to all thirty (30) CFATF member jurisdictions, the United Kingdom Crown Dependencies, the United Kingdom, the United States of America, Canada, Australia, Switzerland, Ireland and Singapore. The short-form was sent to other members of the FATF that are not listed above and CFATF observer organisations.

19. Responses have been received from thirty-seven (37) jurisdictions representing some of the membership of both CFATF and the FATF, as well as other FATF Style Regional Bodies (FSRB). Twenty-two (22) jurisdictions provided information using the long form questionnaire and fifteen (15) answered the short form questionnaire.

20. The Project Working Group wishes to thank the FATF and CFATF Secretariats and all those who participated in and contributed to this study.

1.5 Structure and Nature of the Sector

21. The FATF 40 + 9 Recommendations refer to TCSPs as being persons and businesses that, by way of business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements;
- Acting as (or arranging for another person to act as) a trustee of an express trust;
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

22. TCSPs are categorized in the FATF Methodology as Designated Non-Financial Businesses and Professions (DNFBPs). Countries are therefore required under Recommendation 24 to ensure that this class of business is subject to effective systems for monitoring and is compliant with AML/CFT measures. TCSPs are often subsidiaries of banks, financial services businesses, law or accountancy firms; but they may also be single person stand-alone operations. In some jurisdictions TCSPs carry out a broad range of corporate services, but this may account for only a portion of the primary business of the entity. The variety and scope in the nature of the business and the structural makeup of TCSPs contribute to variations in the degree of regulation of corporate vehicles from jurisdiction to jurisdiction. A few jurisdictions regulate TCSPs in a manner similar to the internationally recognized and required prudential regulation of financial institutions. However, it has previously been found that a majority of jurisdictions still do not regulate or in any way supervise the operation of TCSPs[3], despite the fact that lawyers and other professionals are providing trust and company services. For example, in almost all jurisdictions lawyers will be involved in the formation of foreign companies for clients. The same is true for trusts, as lawyers or other professionals within the jurisdiction may well be engaged in the administration of trusts, even if the jurisdiction does not recognize this. However, there may be no barrier in such jurisdictions to a resident professional acting as a trustee for a trust

[3] OGBS (2004)

established under the law of a jurisdiction that does recognize trusts.[4] Given this, the effectiveness of the FATF Recommendations and guidance (as they apply to TCSPs) can be challenging to measure.

1.6 Overview of previous work

23. The FATF has issued guidance on the risk based approach for legal professionals, accountants and other TCSPs.[5] Other work has been carried out on matters pertaining to TCSPs by various groups and individuals. As can be seen below from the summaries of a few studies done in this area, many issues remain unresolved today. This project will seek to provide a timely follow-up to some of the key outstanding issues which are outlined below, as well as addressing some of the concerns expressed by the G20, and others, relating to international cooperation and the prevention of the misuse of TCSPs and AML/CFT efforts more generally.

1.6.1 OECD: Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes, 2001

24. In May 2000, the Financial Stability Forum (FSF) asked the Organisation for Economic Co-operation and Development (OECD) to undertake the drafting of a report to develop mechanisms to reduce the vulnerability of corporate vehicles being misused for illicit purposes. The OECD Steering Group on Corporate Governance drafted this report which was submitted to the OECD Ministers, G-7 Finance Ministers and FSF. The report was recognised at the May 2001 OECD annual meeting. The paper stated that in order to develop mechanisms to prevent the misuse of corporate vehicles, supervisors and law enforcement authorities should ensure that they are able to obtain, on a timely basis, information on the beneficial ownership and control of corporate vehicles and to share that information with foreign authorities.

1.6.2 FATF: The Misuse of Corporate Vehicles, Including Trust and Company Service Providers, 2006

25. One of the more recent studies, the October 2006 FATF Typologies Study on "The Misuse of Corporate Vehicles, including Trust and Company Service Providers", highlights the vital role that beneficial ownership information can play in the detection and prevention of the misuse of corporate vehicles. This study led to the following conclusions:

- The level of misuse of corporate vehicles could be significantly reduced if the information regarding the ultimate beneficial owner, knowledge of the source of assets and the business objective of the company or a trust within a structure were readily available to the authorities that might need it.
- It matters less who maintains the required information, provided that the information on beneficial ownership exists, that it is complete and up-to-date and that it is available to competent authorities.
- Company registers are an important source of information on legal ownership. Legal ownership information held by other public entities such as filings with financial regulatory authorities or stock exchanges should also be accurate and current.
- Individuals and corporate vehicles have legitimate expectations of privacy and business confidentiality in their affairs and, from the information obtained through the survey, it is evident that jurisdictions adopt different approaches to protect legitimate privacy interests.

---

4 FATF (2006)

5 FATF (2008a, 2008b, 2008c)

- Certain of the arrangements and practices however, including the absence of appropriate regulation/supervision, would appear to contribute to the potential for corporate vehicle misuse by making it very difficult, and perhaps even impossible, for the authorities to identify beneficial owners and controllers.

- There is a need to strike a balance between the need for robust regulation and/or supervision to prevent corporate vehicle misuse and the need to avoid unnecessary restrictions on legitimate business.

26. The findings also indicated that in order to provide a more robust framework for the prevention of money laundering and terrorist financing in the area of TCSPs, there are various matters which need to be explored in greater depth. In particular:

- Are the existing AML/CFT standards as a whole adequate to discourage the misuse of corporate vehicles?

- Are the specific FATF Recommendations 12, 16 and 24 sufficient as a basis for dealing with the issue of corporate vehicle misuse?

- What more can be done to ensure that adequate, accurate and timely information on the beneficial ownership and control of legal persons/legal arrangements may be obtained or accessed in a timely fashion by competent authorities?

- What can be done to ensure that those engaged in the formation and administration of corporate vehicles are "fit and proper"? Is there a need for an international standard for TCSPs or professionals engaged in providing trust and company services?

- What steps can and should be taken to ensure that the actions of those engaged in the formation and administration of corporate vehicles are properly monitored or subject to investigation as necessary?

- Should TCSPs be regulated or should there be enhanced regulation of such service providers, including lawyers and accountants where they offer similar services?

- Should existing corporate governance standards (such as the OECD Principles) be extended to include factors relating to the role of TCSPs, lawyers and accountants in relation to the potential misuse of corporate vehicles?

- Should guidance in other forms be produced – for example risk assessment check lists – to help the competent authorities focus their risk-based approaches in relation to the different types of misuse of legal persons and legal arrangements?

- Where should beneficial ownership information be held?

- What more needs to be done to enhance the effectiveness of company registers and other publicly available information?

- Is there any practical action that needs to be or can be taken, to enhance the information publicly available in respect of legal arrangements?

27. With this current typologies exercise being undertaken, many of these findings and questions will be examined in greater detail.

1.6.3 OGBS: Trust and Company Service Providers: Statement of Best Practice, 2002

28. The Offshore Group of Banking Supervisors' (OGBS) working group consisted of representation from France, Italy, Netherlands, the United Kingdom, FATF, the International Monetary Fund, OECD and the OGBS. This group acknowledged and agreed that inclusion of TCSPs in the regulatory net is important to the effectiveness of financial services regulation as regards AML and CFT, given that TCSPs are intermediaries and introducers of businesses to institutions that handle/manage funds or assets.

29. The group's Statement of Best Practice,[6] which was completed in September 2002, highlighted that the same degree of regulation was not necessarily appropriate for those TCSPs that do not engage in the management of client funds. These types of TCSPs were described as carrying out "lower risk" business, which, it was suggested, may justify a lighter touch being applied. Lower risk business includes business that consists solely of:

- Company, partnership formation;
- Provision of registered office or business address;
- Providing corporate services, not including discretionary services, to local trading companies.

30. The document also addresses the core areas of regulatory concern and suggests best practices for licensees in the following areas:

i. Fitness and propriety of individuals that are involved in managing assets/funds;

ii. Structure and established controls for a TCSP;

iii. Requirements for TCSPs to know their customer per the Basel Committee's CDD paper[7] of October 2001;

iv. Proper business conduct;

v. Maintenance of financial soundness by the TCSP;

vi. Proper systems and procedures to ensure such financial integrity; and

vii. Storing and accessing information to accommodate easy, unimpeded sharing of information, including transactional information, with relevant authorities.

31. The document also highlighted some best practice considerations, namely that jurisdictions should have to:

i. Establish safeguards for clients when the TCSPs, for whatever reason, are no longer able to conduct business;

ii. Utilize auditors and give them the necessary statutory protections to report breaches of relevant legislation or other material concern;

iii. Conduct regular independent reviews of TCSPs; and

---

6 Attached as Annex IV

7 Basil Committee on Banking Supervision (2001)

iv. Ensure that TCSPs are caught by **national** AML legislation.

1.6.4 OGBS: Securing Effective Exchange of Information and Supervision, 2004

32. At the meeting of the OGBS Trust and Company Service Providers Working Group held on the 8th January 2003, it was agreed that a paper should be prepared to address the following matters relating to TCSP business:-

- Existing restrictions on the flow of information;
- The necessary gateways for effective consolidated supervision; and
- Whether information exchange should be restricted to information on the TCSPs rather than their clients.

33. Studies by the Working Group concluded that there were significant restrictions on the flow of information in this sector. The restrictions arise for a number of reasons springing largely from:

- A lack of a universally accepted and understood definition of what constitutes trust and corporate services;
- The very diverse range of ownership and control of the entities that might be carrying out the activities of TCSPs; and
- According to the nature of that ownership and control, a correspondingly diverse range of regulatory controls and oversights which may already be in place. These range from (in the case of activity carried out by a bank) full consolidated supervision, to (in the case of the activity carried out by an independent small company) no supervisory oversight at all in most jurisdictions globally.

34. The Working Group concluded that such restrictions led to ineffective co-operation, representing a significant weakness in the global defences against money laundering and the financing of terrorism, as well as a genuine lack of customer protection in respect of the sector's clients.

35. The overriding recommendation by the Working Group was the call for regulation of this sector to be introduced. In the absence of such regulations, the Working Group stated that responsibility should be allocated to a competent authority to ensure such TCSPs are monitored for compliance with anti-money laundering legislation and legislation designed to combat the financing of terrorism. The competent authority should preferably be one with gateways to exchange information with regulators of this sector in other jurisdictions.

1.7 Current complementary work

36. As stated by the FATF President Paul Vlaanderen in October 2009,[8] there are currently three transparency related issues already under review within the FATF. *"The first issue relates to **customer due diligence** obligations and **beneficial ownership**. One of the main principles of the FATF standards is the obligation for financial institutions to identify their customers and underlying beneficial owners. The FATF is revisiting its recommendations to consider whether the current standard still is the best tool for providing maximum customer transparency. This question of customer due diligence is closely related to the second issue, that deals with the transparency of **legal persons and legal arrangements**. The review of the recommendations dealing with this topic will seek*

[8] At the XVI Caribbean Financial Action Task Force (CFATF) Council of Ministers Meeting, Willemstad, Curaçao, Netherlands Antilles

to improve the transparency of such persons and arrangements. That should provide authorities with better and more timely access to beneficial ownership information. Finally, ***financial institution secrecy laws and cross-border exchange of information*** *will also be looked at. The FATF will examine whether certain types of laws may inhibit the implementation of the FATF recommendations."* The FATF is actively reviewing the scope of Recommendations 33 and 34 which state that countries should take measures to prevent the unlawful use of legal persons/legal arrangements by money launderers. Results and recommendations from this typologies exercise may assist in that undertaking.

1.8 The Project

37. This typologies exercise will draw from the research and conclusions that were made in the previous work and literature referred to above. In the chapters which will follow, the role of the TCSP industry will be examined, in relation to the detection, prevention and prosecution of money laundering. This will be done through analysing the jurisdictions' responses to the questionnaire as well as the case studies obtained from various sources. Additionally, key findings and observations related to the money laundering vulnerabilities of the TCSP sector will be extrapolated from the information provided by the various sources. In concluding, issues for further consideration will be presented which it is hoped will help to reduce the use of TCSPs for money laundering purposes.

CHAPTER 2: ANALYSIS OF QUESTIONNAIRE RESPONSES

38. This section of the report will focus on the jurisdictions' responses to the questionnaires, and will summarise and analyse the information provided. It is evident from the responses, that the jurisdictions that participated in this research project have adopted varying approaches to protecting their TCSP sectors from the money laundering and terrorism financing threat. The decision by any jurisdiction to subject its TCSP sector to any form of legislation is dependent on the type and sophistication of the business conducted within the sector, and also on the jurisdiction's risk tolerance and priority ranking. Notwithstanding, wherever TCSPs operate it is expected that some level of vulnerability to the risk of money laundering and terrorism financing is also likely to exist. This section therefore aims to ascertain the following from the responses to the questionnaire:

i. The definition of TCSP in different jurisdictions

ii. The types of services generally provided by TCSPs;

iii. The persons who act as TCSPs;

iv. The use of TCSPs for incorporation/registration of a company;

v. Licensing requirements for and supervision of TCSPs;

vi. The information that TCSPs are required to maintain;

vii. ML/FT vulnerabilities faced by TCSPs;

viii. The role played by TCSPs in the detection and investigation of ML/FT; and

ix. The adequacy of international standards pertaining to TCSPs.

39. As previously mentioned, jurisdictions provided responses to either a long form or a short form questionnaire.[9] The more comprehensive long form questionnaire had a total of 33 questions comprised in six parts. Part A required background information related to the responding jurisdiction; Part B required details on the TCSP sector within each jurisdiction; while Part C required information on the oversight or regulation of this sector for AML/CFT purposes. Part D required jurisdictions to indicate what type of information and other requirements, if any, apply to their TCSP sectors, while Part E required case studies as well as information and statistics on suspicious activity reporting and investigations relating to AML/CFT in the TCSP sector. Part F required jurisdictions to provide their views on the adequacy and role of international standards in relation to this sector and on whether or not additional standards or a purpose-created international body was necessary for TCSPs. The short form questionnaire did not require any information on the areas covered by Parts C, D and E of the long form, but did require the jurisdictions that responded to this version of the questionnaire to give some information about the definition of TCSP in their laws, this being the first question in Part B in the long form version. The short form questionnaire also covered all the questions addressed in Part F of the long form version.

9 See Annex III - Questionnaire

2.1 Definition of TCSP

40. Jurisdictions were asked to give the definition of TCSP provided for under their legislation. Thirty-six jurisdictions responded to this question. Of that number, five jurisdictions indicated that their legislation recognised and defined the specific concept of TCSPs,[10] and, for the most part, the definitions were consistent with or exact duplications of the definition of the term found within the FATF Methodology. Sixteen jurisdictions indicated that while there was no specific definition for TCSP per se, their laws did recognise and distinguish the sector by virtue of the types of services provided by them[11]. While the essential features of the FATF definition of TCSP are for the most part present in the definition of the services provided by specified sectors in the sixteen 16 responding jurisdictions, there are cases where the definitions either expand on or restrict the scope of services covered. For instance, in one jurisdiction in addition to the FATF-defined services, the definition of 'regulated fiduciary services' includes acting as executor of a will or administrator for an estate;[12] and in another jurisdiction, 'company management business' includes corporate services involving the control of the whole or substantial part of the assets of a company.[13] On the other hand, in another jurisdiction, the definition of 'TCSP' did not refer to the provision of directorial and secretarial services, nor did it refer to the provision of nominee shareholder services.[14]

41. Among the jurisdictions that define by reference to the services, certain terms and concepts were common within their laws, namely: trust business/trust company/trust service provider[15]; registered agents[16]; and company management business/service.[17]

42. Of the remaining 15 jurisdictions, 7 respondents indicated that while TCSPs are not recognised or regulated under their laws as a separate business sector, nevertheless lawyers, accountants and notaries or fiduciaries in some cases carry out the services identified in the FATF definition of TCSPs in the jurisdictions.[18] Two of the respondents identified trust services as the only TCSP-type service recognised under the laws in their jurisdictions, and that only certain financial institutions were permitted to act as trustees.[19] Two jurisdictions specified that no provisions were

---

10 BG, DK, EE, IT & GB

11 AI, AT, BS, BM, VG, KY, GG, JP, JE, LI, NL, AN, LC, VC, TC and US

12 GG

13 KY

14 BG

15 AI, BS, BM, VG, KY, JP, JE, NL, AN, VC and US. In LI they have what is called 'trust enterprises'. It should be noted that though the terms 'trust company' and 'trust service provider' are used in the laws of NL and AN respectively, these businesses essentially operate as company service providers as the concept of 'trusts' is not known in NL and AN law. It should be noted, however, that the Dutch regime recognizes the trustee services provided by Dutch TCSPs to foreign trusts.

16 VC and US

17 AI, VG and BS

18 AU, BE, CA, DO, HK, MO and CH. It should be noted however, that the corporate service business referred to by DO involved law firms buying and selling companies incorporated in foreign jurisdictions; while trusts are not known to DO law. In CH, some fiduciaries carry out TCSP services, and the class of professionals that make up this group is dependent on the specific services that they offer, whether it be administrative, trust or payment services. It should be noted that it is not possible to set up a trust under CH law

19 GT and MX

made under their laws for TCSPs, but did not clarify whether the services were being provided within other sectors.[20] Four of the respondents did not provide sufficient information for analytical purposes.

43. From these responses, it can be seen that the majority of jurisdictions have attempted to make some provision within their laws for TCSPs, whether by adopting the FATF terminology and definition, or by extracting from the Methodology the services that are relevant to the business carried on in their jurisdictions and making specific provisions for the persons and entities that provide those services. Either approach has merit depending on the individual circumstances in each jurisdiction, but a more tailored approach may be more suitable to address the specific sectoral features in respective jurisdictions. In the case of one jurisdiction,[21] although TCSP is defined and regulated under the law as if it is a discrete sector, that jurisdiction's response to a later question in the questionnaire indicates that the term, "TCSP", does not always fit with practice in that jurisdiction. This is demonstrated by the fact that some of the TCSP services, particularly in the area of trusts, are offered only as an ancillary activity to the business of many firms; and because trusts have such wide-ranging uses in that jurisdiction, a very wide range of professions and companies will be involved in some way in trust business.

44. While the tailored approach may be more attractive for many jurisdictions, variations in the approach to defining the sector in different jurisdictions may also result in a confusing array of laws governing an international industry that is becoming increasingly more globalised, as TCSPs in different countries engage in business overseas or court foreign clients.

2.2 Services generally provided by TCSPs

2.2.1 Common types of TCSP businesses found in jurisdictions

45. Responses to the questionnaire show that the services provided by TCSPs vary from jurisdiction to jurisdiction. The nature, size and complexity of the economies of respective jurisdictions affect the type of services that are provided by the TCSP sector. Jurisdictions were therefore asked to classify and rank their TCSP sector based on whether or not they carried out solely trust business or corporate services business or a mixture of both. Twenty-one jurisdictions responded to this question, and, from their answers, it is evident that the most prevalent TCSPs are those that carry on both trust business and corporate services business. This class of TCSP business ranked as the most prevalent in nine jurisdictions.[22] TCSPs that provide only corporate services are ranked as the next most common type of TCSP business, with six respondents ranking them as the most common TCSP business in their jurisdiction.[23] The third most common TCSP businesses are those that are licensed financial institutions or are subsidiaries or branches of local or foreign financial institutions which are also permitted to carry on TCSP business. Three jurisdictions ranked this type of TCSP business as the most prevalent.[24] There were a few jurisdictions where it was most common for TCSP to carry out only Trust business, and TCSP Business to be provided by only licensed financial institutions, or by other professionals such as lawyers and accountants.

2.2.2 Services provided by TCSPs

46. By reference to the TCSP services as defined in the FATF Methodology, jurisdictions were asked to indicate whether or not TCSPs provided these types of services and to provide some statistics

---

20 LV and NP

21 GB

22 AI, VG, KY, CA, GG, HN, JE, CH and TC

23 BS, BM, NL, AN, LC and US

24 GT, PA and VE

on the number of TCSPs within the jurisdictions to provide the respective services listed. Twenty-one jurisdictions responded to this question. TCSP's provide various services and this is evidenced by the responses received to the questionnaire.[25]

47. In the majority of jurisdictions some type of TCSP business in the jurisdiction provides variants of all of the above services,[26] but there are two respondent jurisdictions where only the trust related service is recognised as being provided in those jurisdictions, and then only by financial institutions.[27]

2.3 Persons who can act as TCSPs

48. Jurisdictions were asked whether there were any limitations on the types of persons who could carry on TCSP business by reference also to the categories of service provided. Eighteen jurisdictions responded to this question, indicating that Corporations, Accountants, Lawyers and non-professional individuals were the persons providing these services. In some cases, the jurisdiction also required the person in question to be licensed or otherwise duly authorised to carry on the business. The table below provides an overview of the information received and indicates not only how many jurisdictions use the above-noted entities as TCSP's, but also indicates the types of TCSP business that the respective entities provide.

49. The responses indicated that in some jurisdictions the various entities were subject to specified conditions in order to act as TCSPs. Therefore, they had to either be licensed pursuant to domestic legislation; registered with a relevant supervisory authority under ML regulations; or have a trust license or dispensation. Additionally, the other entities that were able to act as TCSP's included: licensed and unlicensed individuals and partnerships; natural persons with trust licenses or dispensations; authorized persons; trust companies; and consultants. The table below provides a comprehensive breakdown of the information.

Who can act in capacity of: (yes or no)	**Jurisdictions allowing Corporations to be TCSPs**	**Jurisdictions allowing Accountants to be TCSPs**	**Jurisdictions allowing Lawyers to be TCSPs**	**Jurisdictions allowing Others to be TCSPs**
TCSP: Incorporating a Company	**16** (**6** of these require licence /other form of authorisation)	**10** (**3** of these require licence/other form of authorisation)	**12** (**4** of these require licence/ other form of authorisation)	**7**[a]
TCSP: providing Company Administration/Corporate Services Business	**16** (**7** of these require licence /other form of authorisation)	**11** (**3** of these require licence/ other form of authorisation)	**12** (**4** of these require licence/ other form of authorisation)	**6**[b]
TCSP: acting as a Trustee	**15** (**6** of these require licence/other form of authorisation)	**11** (**3** of these require licence/other form of authorisation)	**12** (**4** of these require licence/ other form of authorisation)	**6**[c]

25 See Annex I – Table 1

26 With the exception of the jurisdictions mentioned in footnote 27below; and NL and AN, as trusts cannot be formed under Dutch or AN law.

27 GT and HN

Who can act in capacity of: (yes or no)	Jurisdictions allowing Corporations to be TCSPs	Jurisdictions allowing Accountants to be TCSPs	Jurisdictions allowing Lawyers to be TCSPs	Jurisdictions allowing Others to be TCSPs
TCSP: providing Trust Administration Services/ Trust Business	**15** (**7** of these require licence/other form of authorisation)	**9** (**3** of these require licence /other form of authorisation)	**11** (**4** of these require licence/ other form of authorisation)	**6**[d]

Table notes:

a. These included: - partnerships or individuals (one required they be licensed); consultants; licensed individuals; natural persons that have a trust license or dispensation; managers; persons authorized by FSA; and one Jurisdiction allowed any individual to incorporate a company.

b. These included: - licensed partnerships or individuals; consultants; licensed individuals; natural persons that have a trust license or dispensation; managers; persons authorized by FSA; and one jurisdiction had no specific requirements to be a company service provider.

c. These included: - licensed partnerships or individuals; trust companies and consultants; individuals; any individual or company; managers; and persons authorized by FSA.

d. These entities included: - licensed partnerships or individuals; trust companies and consultants; individuals; only banks; managers; persons authorized by FSA.

2.4 Use of a TCSP for incorporation/registration of a company

50. Jurisdictions were asked to provide information on their incorporation process and specifically to address whether TCSPs are required to be used to incorporate a company or whether this can be done by direct central registration. Sixteen jurisdictions gave relevant responses to this question, and from this it is evident that jurisdictions tend to adopt one of two alternate routes to incorporation.

Route 1: TCSPs are required in the incorporation process of all companies; and

Route 2: Direct central registration is available as an option even though TCSPs may also be used.

51. As highlighted in the table below, a larger number of jurisdictions, as an option, allow for incorporation by direct registration, while only five jurisdictions by law mandate incorporation of all companies by a TCSP. Direct central registration is typified by the direct approach to the authorities during the incorporation process by the individuals who are forming their own companies.

	Route 1 **TCSP Required for Company Incorporation**	Route 2 **Direct Central Registration for Company Incorporation is available as an option**
Number of Jurisdictions	**5**	**11**
Jurisdictions	AI, VG, GG, LC, VC	BS, BM, CA, KY, JE, NL, AN, CH, TC, GB and US

52. It is interesting to note that the five jurisdictions that mandate the involvement of TCSPs in the incorporation process are all jurisdictions that impose licensing requirements on TCSPs, which are also subjected to prudential and AML/CFT supervision. Further, some of the jurisdictions that allow direct central registration of companies as an option require a TCSP to be used in the incorporation of an international business company (IBC). However, for those jurisdictions, local companies that are not classed as IBCs or exempt companies can be registered without the involvement of a TCSP. Like the jurisdictions that adopt Route 1 as their required means of incorporation, these jurisdictions also operate a licensing and prudential supervision regime for all TCSPs.

53. In one jurisdiction, although direct central registration is an option and no TCSP is required to be involved in the incorporation of any type of company, the practice in the jurisdiction is that 99% of all companies incorporated are done using a TCSP, with additional scrutiny being carried out by a regulatory body. Furthermore, the authorities automatically subject applications that do not come from TCSPs to a higher level of review.[28]

54. In two jurisdictions where TCSPs are not required for the incorporation of companies, it was noted that notaries have to be involved in some way. However, it is not in the capacity of a person providing TCSP services but more for the purpose of notarising required documents. In one of these jurisdictions, although TCSPs are not separately defined and supervised as a discrete sector, it was recognised that lawyers and other professionals carry out the services and they are all subject to AML laws. In the other, "Trust Offices" are defined and regulated as a separate sector providing corporate services; and companies, partnerships and natural persons can be permitted to act as Trust Offices.

55. In another major financial centre, direct central registration is the norm and is done at a state, rather than at a federal, level. However, in the states where there appears to be a proliferation of 'registered agents' providing corporate registration services to clients, the concept of 'commercial registered agents' has been developed, which recognises such persons or entities that have numerous clients[29] on whose behalf they act as registered agents. In these states it is therefore likely that TCSPs have a higher frequency of involvement in the corporate registration process.

2.5 Licensing and Supervision of TCSPs

56. Eighteen out of twenty of those who responded to this section of the questionnaire indicated that TCSPs are required to be licensed in their jurisdiction. However, a closer review of the responses revealed that in some jurisdictions where licensing is required, the licences do not pertain specifically to the provision of the TCSP services. Additionally, some jurisdictions require licensing and regulation of trust service providers but there are no licensing requirements for corporate service providers.[30] In some jurisdictions, only financial service intermediaries and banks[31] that are licensed under separate legislation are allowed to provide services akin to those described by the FATF as being provided by TCSPs, in particular trust services.

57. In jurisdictions that choose to directly licence TCSPs, these are subject to fit and proper assessment and ongoing prudential supervision. Such fit and proper tests are applied to directors, senior officers, shareholders and other connected persons. In relation to the ongoing supervision of TCSPs in countries that have licensing criteria, most respondents indicated that those entities are also subject to onsite supervision to ensure compliance.

58. In jurisdictions that have chosen to licence TCSPs, the implementation of licensing and regulation of TCSPs appears to have had marginal impact on the number of TCSPs operating in the jurisdiction. Statistical data provided indicates that in most cases, there was not a noticeable decline in the number of TCSPs after the introduction of licensing requirements or regulation to this sector. However, a few respondents did indicate that the introduction of regulation of TCSPs may have inspired consolidation within the sector, whereby the smaller operators exited or were taken over by larger TCSPs. Respondents have also indicated that a positive result of the regulation of TCSPs is the

---

28 BM

29 In the US, in the state of DE a commercial registered agent represents more than 50 legal entities. In the state of WY the minimum number is 10.

30 BM and US

31 Of the respondents to the question on whether TCSPs are subject to licensing requirements, 5 of the 23 respondents indicated this is only so where the institution is a financial institution or Bank, meaning that they were licensed under banking legislation.

improvement in the quality of information now available to competent authorities from TCSPs. That is, better information is available to facilitate exchange of information and international cooperation with other regulators and law enforcement agencies.

59. In many jurisdictions lawyers, accountants and other such professionals provide the TCSP services as defined by the FATF. In relation to this class of TCSP, the responses to the questionnaire show that, in many jurisdictions, the licensing and/or authorization and oversight of these persons generally come within the purview of their respective professional bodies.

60. The FATF requirements stipulate that designated non-financial businesses and professions (DNFBP) should be subjected to effective mechanisms for the prevention of money laundering and terrorism financing. As TCSPs come within the FATF's definition of DNFBPs, jurisdictions are required to apply the requirements in the FATF's Recommendations 5, 6, 8, 11, 13, 15 and 21 to the TCSP sector. The questionnaire therefore required jurisdictions to indicate whether TCSPs are subject to any AML/CFT legislation and requirements and, if so, to provide some details of this. Twenty respondents addressed this question and of that number, 18 indicated that TCSPs, by whatever definition, are subject to AML/CFT requirements.[32] In the remaining two jurisdictions, only trust service providers are subjected to the AML/CFT requirements.[33] In one of the two jurisdictions, it was indicated that all persons in business, including CSPs, are subject to various currency transaction reporting requirements and are prohibited from engaging in transactions with persons and countries identified on a terrorist list; but there are no specific AML/CFT requirements applied to CSPs in that jurisdiction as contemplated by the relevant FATF Recommendations.[34] In the other jurisdiction the only AML/CFT obligation imposed on CSPs relates to suspicious activity reporting, as all persons in a business, profession, trade or employment are subject to the requirement to report suspicious transactions to the national FIU.

61. Where TCSPs are subject to AML/CFT legislation, this should include penalties for non-compliance. All the responding jurisdictions, with one exception, reported that a variety of criminal penalties, including fines, were available to be imposed for breaches of the legislation by TCSPs. Additionally, those jurisdictions that have licensing criteria for TCSPs, also have additional regulatory mechanisms for dealing with regulatory breaches or issues of compliance identified at TCSPs. The administrative penalties span a range from minor to serious, with the ultimate penalty being licence revocation.

62. Jurisdictions were also asked to indicate whether TCSPs are subject to ongoing monitoring and supervision and if so to name the competent authority responsible for carrying out this function. Details on the nature and requirements of ongoing monitoring and supervision were also requested. There were 20 respondents to this question, 15 of whom indicated that full prudential supervision, including AML/CFT monitoring, of TCSPs is conducted on an ongoing basis in their jurisdictions. This type of supervision involves both onsite and off-site inspections; consultations with management; review of audited or other financial statements; and review of records and policies and procedures. One jurisdiction carries out AML/CFT supervision only. There are four jurisdictions which differentiate between trust service providers and company service providers for ongoing monitoring and supervision purposes, in that trust service providers, being licensed, are subjected to both prudential and AML/CFT supervision and monitoring in all four jurisdictions. However, the

---

32 AI, BS, BM, VG, CA, KY, GT, GG, HN, JE, NL, AN, PA, LC, VC, CH, TC, GB and VE. In the case of BM all of the AML/CFT requirements had not yet been extended to CSPs in that jurisdiction.

33 BM and US

34 US did indicate in the introductory remarks in their response that trust companies are licensed to provide certain fiduciary services and for AML/CFT purposes were classified as banks. The remainder of their response was directed at addressing the CSP sector.

company service providers in one jurisdiction are not supervised at all;[35] in two jurisdictions they are licensed and only subjected to AML/CFT supervision;[36] and in the other case, in two regions of that jurisdiction[37] they are subjected to some level of conduct of business review.[38]

63. Table 2 of Annex I provides details of the jurisdictions' responses to the questions pertaining to licensing and ongoing monitoring and supervision.

2.6 Information required to be gathered by TCSPs

2.6.1 What information is required of TCSPs?

64. The FATF Recommendations 33 and 34 stipulate that jurisdictions should take measures to prevent the unlawful use of legal persons/legal arrangements by money launderers. Jurisdictions are also required to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons; and in the case of legal arrangements or express trusts, adequate, accurate and up-to-date information on the settlor, trustee and beneficiaries should be obtained in a timely manner and made available in a timely fashion to competent authorities.

65. The jurisdictions were asked to indicate whether beneficial ownership information is required to be disclosed to competent authorities at the time of all company formations; and whether information on settlors and beneficiaries is required to be disclosed to competent authorities at the time of all trust formations. The questionnaire also called for information on whether the terms 'beneficial ownership', settlors' and 'beneficiaries' are defined in the laws of the responding jurisdictions. Twenty jurisdictions responded to these questions with seven of them requiring automatic disclosure of beneficial ownership information to competent authorities at the time of company formation[39]; and another eight not requiring such disclosure.[40] One jurisdiction has adopted a unique approach,[41] in that all of its companies are required to obtain consent from the regulator to issue shares and admit members; and this is only one of three methods used by the regulator to capture this information. This process involves disclosure to the regulator of the ownership and control structure of the company, which the regulator will then verify before granting consent. This process is also applicable whenever a company seeks to change ownership, unless the company is administered by a TCSP, in which event the need for consent is waived but the TCSP is required to capture and verify the information themselves.

66. Among the jurisdictions that had no requirement for the disclosure of such information to the authorities at the time of incorporation, six [42] required TCSPs to obtain this information, verify its accuracy, retain it in their records, update the information periodically and make the information available to competent authorities upon request. From the responses it can be seen that the majority of jurisdictions mandated that this information be disclosed at the time of incorporation either to a

---

35 BM

36 BS and CA

37 US – in the states of DE and WY

38 Conduct of business supervision focuses on ensuring orderly and transparent financial market processes, proper relationships between market participants and the exercise of due care by financial undertakings in dealing with clients.

39 AI, BS, BM, KY, JE, NL and AN. CA required only information on the directors, not shareholders, while LC permitted public filing of such information but did not mandate it.

40 VG, GT, GG, VC, CH, TC, GB and US. Five other respondents failed to provide relevant responses.

41 JE

42 VG, GT, GG, VC, TC and GB

competent authority or to a TCSP. Within these jurisdictions that required the capture of beneficial ownership information by either method, provisions were made in their laws to define or describe the terms relevant for an appropriate understanding of beneficial ownership.

67. In relation to trusts, only one jurisdiction indicated that it had a Registrar of Trusts, to whom disclosure had to be made of the beneficial ownership information pertaining to all trusts, including information on the settlor and beneficiary.[43] This necessitated the filing of the trust deed or settlement with the Registrar and included the filing of any resolution that resulted in changes being made to the ownership and beneficial interest in the trust. Fourteen jurisdictions indicated that they had no central registry for trusts and that therefore no information on the beneficial ownership details of trusts was required to be automatically disclosed to a competent authority. However, this information was required to be maintained by TCSPs in 12 of these 14 jurisdictions.

68. Nineteen jurisdictions indicated that under AML/CFT and/or other regulatory laws, TCSPs are required to request information on beneficial ownership, as well as information on settlors and beneficiaries of trusts and to conduct CDD, verification and record retention in relation to such information and to make this information available to competent authorities upon request.[44] Many of these jurisdictions also require TCSPs to request information from their clients on their source of funds and the nature of the business undertaken by them; and such information is required to be maintained and kept up-to-date. In this regard, 16 jurisdictions require TCSPs to capture information on source of funds; 17 jurisdictions require TCSPs to capture information on the nature of the business being undertaken; and 16 of these jurisdictions require TCSPs to keep the required information up-to-date.

69. Jurisdictions were also asked whether TCSPs were experiencing any difficulties in obtaining the FATF required information from clients. Ten [45] of the 29 respondents to this question indicated that TCSPs in their jurisdictions experienced no difficulties in this regard. Of the respondents that indicated that there was some degree of difficulty, four [46] highlighted problems related to trusts, three[47] noted difficulties connected to obtaining information from long-standing clients and one advised of difficulties in identifying PEPs.[48] Other issues raised were:

- client confidentiality and professional relationship conflicts;
- clients unwillingness to provide information out of legitimate fears of identity theft;
- obtaining sufficient detail about the intended purpose and/or activities of a proposed legal person or legal arrangement;
- lack of statutory record-keeping and CDD requirements for TCSPs, and absence of legal backing for TCSPs to obtain the required information;
- lack of awareness and full knowledge by TCSPs of their obligations; and

---

43 VC

44 AI, BS, BM, VG, CA, KY, GT, GG, HN, JE, NL, AN, PA, LC, VC, CH, TC, GB and VE

45 AI, BS, KY, EE, GT, HN, LV, LI, PA, and VC

46 BE, CH, GB, and VE

47 BM, AN and TC

48 BG

- the unwilling attitude of some TCSPs under supervision and the need to threaten the possibility of imposing Cease and Desist Orders to get the relevant information.

70. Whatever approach is adopted by the jurisdiction and regardless of the attendant difficulties in obtaining the required information, a matter of signal importance in the capture and maintenance of beneficial ownership information is the accuracy of the information and whether or not it is current. Jurisdictions that supervise TCSPs and subject them to periodic onsite and offsite inspections, stand a better chance of ensuring that TCSPs take appropriate steps to verify and update the information that is subjected to the record-keeping requirements; thereby assuring a higher quality of information available for disclosure and international exchange.

2.6.2 The Adequacy of the Information Requirements

71. Jurisdictions were asked to provide an assessment of the adequacy and role in AML/CFT efforts of the information required from TCSPs in accordance with the FATF Recommendations. The majority of respondents to this question expressed the view that the information captured by TCSPs plays an essential role in the efforts to effectively combat money laundering and terrorist financing. The fact that TCSPs can alert authorities to suspicious activity through filing Suspicious Activity Reports (SARs), as well as the fact that they can provide detailed information on beneficial ownership and the source of funds, in circumstances where competent authorities require this information to assist in enquiries about suspected money laundering activity, are both powerful tools in the AML/CFT arsenal. One respondent highlighted the fact that the information available to TCSPs is not only a tool for the authorities in combating money laundering and terrorist financing, but also beneficial for the TCSPs themselves in creating risk profiles of clients to assist them in determining whether to commence business relationships or terminate them, as well as to assess what level of CDD and monitoring of those client accounts ought to take place.

72. In relation to the question on the adequacy of the information, most jurisdictions were of the view that the information required to satisfy the FATF requirements is adequate to meet the needs of combating money laundering and terrorist financing. While a few respondents did express concern about the limitations of the information available through TCSPs, these limitations for the most part appeared to be a result of non-compliance or less than full compliance with the FATF requirements rather than an inadequacy in the requirements themselves.

2.7 Vulnerabilities faced by TCSPs

73. The questionnaire required respondents to give their opinions on what constitutes the greatest threats to money laundering and terrorist financing in their jurisdictions. Eighteen jurisdictions responded to this question, providing a diverse array of perspectives on the issue. Aside from two jurisdictions, both of which indicated a significant minimisation of AML/CFT risk to their TCSP sectors[49], the remaining 16 respondents provided input on the areas of potential weakness for TCSPs. An area of weakness that seems to concern several jurisdictions pertains to customer due diligence and the reliability of information obtained on customers/clients/beneficial owners. In this regard, there is also concern that lack of resources for TCSPs to access intelligence tools such as World-Check and C6; as well as inadequate training for TCSP employees, both contribute to weakness in the verification of know your customer (KYC) documents and information. Another resource issue pertains to smaller TCSP businesses, in that they often do not have the capacity to fully apprise themselves of their obligations under AML/CFT legislation. Several jurisdictions[50] also

[49] BS indicated that the reduction in ML/FT risk resulted from the application to the TCSP sector of the same AML/CFT obligations to which the prudentially regulated sectors are subjected. GT indicated that the minimisation of ML/FT risk to trust providers results from the fact that only banks and financial companies are permitted to act as trustees.

[50] BM, LC, VC, GB and VE

expressed concern about the ability of TCSPs to gather reliable information on individuals and beneficial owners of companies and trusts, thereby leaving them open to be abused or misused by criminals.

74. The area of training was also cited as another potential area of vulnerability for TCSPs, in that inadequacy in the training of TCSP staff to assist them to more effectively conduct CDD and verification of CDD information; and to enable them to more readily identify how vehicles are structured for use in supporting both ML and TF schemes, has the potential to greatly reduce a TCSP's ability to effectively vet clients and circumvent risky schemes. As an adjunct to the training issue, a point was raised in respect of the probity and character of TCSP employees, in that the TCSP and the jurisdiction as a whole can be more vulnerable to ML/TF where employees misrepresent the level of skill or competence they have in relation to AML/CFT matters; or they deliberately flout AML/CFT policies, procedures and obligations. It was also suggested that TCSPs may be undermined by their inability to maintain up to date information on international actions to sanction individuals, companies or countries. This, of course, is a burgeoning area of concern given the increasing spate of international sanctions applied to individuals and entities in countries where terrorist financing and proliferation financing in particular are deemed to be significant threats.[51]

75. It was also suggested that another great challenge faced by TCSPs relates to their ability to effectively conduct ongoing monitoring of the business activities of underlying businesses and arrangements. It is often difficult enough for TCSPs to do due diligence and monitoring for their clients in relation to the primary business conducted by them; it is therefore easy to see how going beneath that surface to vet secondary or ancillary businesses can potentially pose even greater problems. Another potential challenge for many TCSPs results from their involvement in international business in various jurisdictions, all of which have varying standards on AML/CFT. It is understandable how this unlevel playing field can mystify and undermine TCSPs trying to navigate through this uneven terrain.

76. One jurisdiction suggested that TCSPs are vulnerable in complex or difficult cases where they are unable to fully understand the purpose or activities of wider structures with which they are involved. Such transactions will require more tenacious checks for information on both the clients and the wider purpose and structure of the scheme, beyond the confines of the TCSP's direct involvement. But even this can pose resource challenges and raise questions as to how wide the net for information ought to be cast.

77. Several jurisdictions also identified a number of red-flag indicators where TCSPs may be utilised in money laundering schemes:[52]

- Transactions that utilise complex and opaque legal entities and arrangements;
- Cases of corruption where the company paying the bribe to secure a contract or the person brokering a contract will seek to secure a successful outcome by utilising a TCSP to operate a trust with the funds held on deposit for the benefit of the person approving the contract;
- The use of foreign private foundations that operate in jurisdictions with secrecy laws;

---

51 Referring in particular to UNSC Resolution 1737 (2006) and its associated UNSC Resolutions up to and including UNSCR 1929 (2010) pertaining to IR; and UNSC Resolution 1267 (1999) and the resulting associated UNSC Resolutions up to and including UNSCR 1904(2009) pertaining to Al'Qaida and the Taliban.

52 CA, JE, NL, AN and US

- The use by prospective clients of nominee agreements to hide from the TCSP the beneficial ownership of client companies;
- Clients who allow TCSPs to have full discretionary authority over the client's accounts may entice unethical TCSP principals or employees to conduct unauthorised/illegal transactions from these accounts;
- The carrying out of intercompany loan transactions and/or multijurisdictional wire transfers;
- The operation of virtual offices overseas which provide TCSP services;
- The formation by TCSPs of shell companies that can then be used by money launderers.

2.8 TCSP's role in detection and investigation of Money Laundering

78. The questionnaire required jurisdictions to provide information on whether or not TCSPs are required to file SARs and to give statistics on the number of SARs filed by the sector between the years 2006 and 2009. An important gauge of the significance of TCSPs in detecting money laundering or terrorist financing was the request for information on the percentage of total SARs that was represented by TCSP filings for that period. Twenty of 21 responding jurisdictions indicated that TCSPs in their jurisdictions were required to file SARs.[53] For the jurisdiction that answered in the negative, this would only apply to their company service providers, because trust companies are classified as banks and would therefore be subject to the same reporting obligations as banks.[54]

79. In relation to statistics, the same 20 jurisdictions responded to this query, with 13 of them being able to provide statistics for the relevant period[55]. One jurisdiction was distinct, in that its TCSP sector accounted for between 71% to 84% of the SAR filings in that jurisdiction for the relevant period.[56] This may be an indicator of the relative importance of this sector in that economy, when compared to the banking sectors in most other jurisdictions which generally account for the largest percentage of SARs filed. Only two of the responding jurisdictions indicated that no SARs were filed for this period but no explanation was provided for why this was likely to be so. Four jurisdictions provided no statistics on TCSP-filed SARs[57], with at least one of them[58] indicating that they were unable to answer given the fact that the majority of TCSPs are not standalone firms and it was impossible to distinguish between the SARs filed under their TCSP functions and those under their other functions. See Table 3 in Annex I for a compilation of these statistics.

---

53 AI, BS, BM, VG, CA, KY, GT, GG, HN, JE, NL, AN, PA, LC, VC, CH, TC, GB and VE. HK, in responding to the short form questionnaire, also volunteered this information in response to another question. In subsequent correspondence JP also indicated that trust companies are also required to file SARs under their law.

54 The US prefaced its response to the questionnaire by indicating that trust companies are licensed to provide certain fiduciary services and for AML/CFT purposes were classified as banks. The remainder of their response was directed at addressing the CSP sector.

55 AI, BM, VG, KY, GG, HN, HK, JE, NL, AN, CH, TC and VE. CH gave aggregate statistics for number of SARs attributed to fiduciaries and legal professionals, with the proviso that there was no way of telling what proportion of the number related exclusively to TCSP activity.

56 VG

57 BS, CA, PA and GB

58 GB

80. Respondents also provided information on the typical subject areas of TCSP SAR filings in their jurisdictions. The following is a sampling of these responses:

- Unusually large transactions;
- Suspected fraud offences;
- Suspected politically exposed persons;
- Suspected securities fraud;
- Suspected tax offences;
- Suspected corruption;
- Suspected money laundering;
- Subject of transaction name appearing on international database;
- Subject of transaction suspected of involvement in international fraud;
- Trust account opened which then receives multiple cash deposits;
- Trust accounts opened with high amounts that are inconsistent with customer profile;
- Trust accounts opened with funds originating from foreign banks;
- Opening of trust accounts for civil projects, the representatives of which are people with criminal records or are alleged fraudsters;
- Multiple trusts accounts opened with the same beneficiary; and
- Natural persons who open multiple trust accounts with different businesses declared upon each opening.

81. In respect of the level of cooperation received from TCSPs when competent authorities follow up on SARs or conduct ML investigations, 12 jurisdictions reported having no difficulties with their TCSPs in this regard.

82. In general, responding jurisdictions appeared to be of the view that TCSPs can play a significant role in the detection and investigation of money laundering offences which take place within their domain. Through case studies and otherwise, some jurisdictions confirmed their positive involvement. TCSPs act as intermediaries both as introducers of business to other institutions and as entities responsible for handling and managing assets. As gate keepers to the financial sector, they are uniquely placed to observe the behaviour and activities of their clients, enquire into their background and business activities, collect due diligence information and evaluate the rationale of prospective and ongoing business. One jurisdiction has taken the unique approach of encouraging its TCSP sector to establish and maintain "Declined Business Logs"[59]; examination of which has satisfied the authorities there that numerous cases had been turned away, which more than likely would have involved financial crime. This is an encouraging sign that regulation of the sector and implementation of

[59] In GG this practice started after the introduction of AML/CFT regulation in 2001

measures such as this can have a positive impact on reducing crime and in providing signals of this trend to both the authorities and practitioners/service providers.

83. The role of TCSPs in detection and investigation is twofold. Firstly, they must implement effective due diligence measures to capture accurate information on clients and beneficial owners, to enable competent authorities to expeditiously obtain key information during an investigation or enquiry. Secondly, TCSPs' proper fulfilment of their duty to file SARs is equally important as they have the earliest opportunity to identify suspect schemes and arrangements. It has been suggested that not only do these obligations assist in the detection of money laundering and other crimes but can also operate to mitigate the risk of a TCSP being misused in this way. Where detailed information is obtained on the individuals who are to own and control a company, or are to settle and benefit from a trust; and a service provider has a full understanding of the service they are to provide and why they are to provide it, this should serve to mitigate the risk that any company formed or trust settled will be used for illicit purposes.

84. Jurisdictions provided several case studies to demonstrate the role played by TCSPs in detecting money laundering schemes. These will be discussed in Chapter 3.

2.9 Adequacy of international standards pertaining to TCSPs

85. Jurisdictions were asked whether the FATF Recommendations and guidance need to more effectively address the role of TCSPs in AML/CFT efforts. Thirty jurisdictions responded, with 11 of them responding in the negative and one providing a non-applicable response. The minority view seemed to coalesce around the notion that the existing FATF Recommendations and guidance are adequate and that the measures to enhance effectiveness had to take place at the jurisdictional level. One of the reasons given for this latter view was that, at the jurisdictional level, company formation, trust law and AML/CFT controls vary considerably as a result of the differences in legal traditions in each jurisdiction.

86. Varied replies from the remaining 18 respondents provide some insight into the areas of concern of the individual jurisdictions. The suggestions provided in these responses are outlined below.

i. The FATF guidance on the relevant Recommendations should be more specifically tailored to TCSP activities to ensure that TCSPs have clear and unambiguous direction on what is required of them. Additionally, updated Recommendations and guidance should more comprehensively capture the role of TCSPs.

ii. The FATF should give strong consideration to extending the "fit and proper" requirements to TCSPs. This is necessary because considerable expertise is required to understand business structures and their intended purposes; as well as to conduct effective vetting of owners. It is important to ensure that the persons carrying out senior roles in TCSPs therefore have the relevant experience, knowledge and good character. This type of requirement applied to senior executives and board members of TCSPs will help to ensure that a positive AML/CFT compliance culture will start in the Board room and executive offices and filter down to the persons who carry out the day to day interface with clients and operation of the services.

iii. Recognising the international and fiduciary nature of many trust companies, in particular, extending the FATF requirements regarding branches and subsidiaries to the TCSP sector would also be beneficial.

iv. The FATF should give consideration to reclassifying TCSPs as financial services businesses as this better reflects the risks involved in the TCSP business.[60] This will give due value to the efforts of jurisdictions that require TCSPs to operate within a regulated environment. As currently classified in the Methodology within the DNFBP grouping, many jurisdictions do not get credit for the AML/CFT measures applied in the regulation of the TCSP sector as examiners are not allowed to weigh the ratings to take account of this fact.

v. Ongoing work in the context of the development of the FATF's 4th Round Methodology should clarify the beneficial owners' requirement under Recommendations 5, 33 and 34, as well as the meaning of 'beneficiary'. In particular, should 'beneficiary' be understood to cover identification only of classes of beneficiaries or specific individuals?

vi. It would be helpful to have some guidance on the persons to be identified in the case of legal persons and arrangements that are not companies and trusts. In particular, who are the persons on which CDD is to be done in the case of 'foundations'?

vii. Consideration should be given to requiring the imposition of an obligation to centralise the records of trusts.[61]

viii. Allowance should be made to enable financial institutions to apply reduced or simplified CDD measures under Recommendation 5 to relationships established with trust company businesses.

ix. Further guidance is required in the FATF Methodology to bring clarity to the conflict between legal professional privilege and the obligation to report suspicious transactions. The FATF should conduct a study on this issue and provide more sophisticated guidance for jurisdictions to follow.[62]

87. Jurisdictions were also asked whether there appeared to be a need for the establishment of an international body dedicated solely to TCSPs; and whether there is a need for the development of international standards specifically for TCSPs to address issues such as fitness and propriety, systems and controls, corporate governance, authorisation and information sharing. There were 34 respondents to these questions providing an illuminating array of viewpoints.

88. The majority[63] of respondents were of the view that no international governing body for TCSPs is necessary. It is necessary to note however, that among this group are respondents whose views on this are informed by the fact that in their jurisdictions the trust sector and, in some cases, other TCSP activities are carried out primarily by financial institutions, all of which are already well overseen by recognised specialist international standards bodies.[64] The other 19 jurisdictions that are against the idea of a new international body are generally of the view that the FATF alongside the

---

60 This suggestion was put forward by VG, KY and GG, all of which operate full licensing regimes with supervision of TCSPs.

61 This suggestion comes from HN in which only specified banks are authorized to carry out trust business.

62 This is a suggestion from MO which expressed concern over the ongoing conflict between the requirement to file SARs and professional codes of conduct requiring lawyers to protect clients' information.

63 Twenty-two out of 34 respondents.

64 HN, GT and PA. MO also made a similar point indicating that a dedicated international body for TCSPs could therefore result in duplication of the work of Basel and others.

other international bodies that provide standards in the areas of banking and other key financial sectors, are sufficient to meet the needs of the TCSP sector. Nevertheless, it was suggested that it would be beneficial were the FATF to pursue additional work on TCSPs to enhance the sector specific guidance available for TCSPs; and also if some thematic approach were adopted by international organisations – *e.g.*, to consider the abuse of trusts in concealing the proceeds of corruption.[65] In this regard, it was suggested that this type of analysis could be carried out by existing organisations in the anti-corruption framework.

89. On the other hand, ten jurisdictions have expressed the view that an international body would be beneficial to this sector.[66] The reasoning articulated for this view is that an international body would serve to develop a uniform set of internationally accepted minimum standards and best practices, as well as to provide typologies on an ongoing basis for TCSPs; also to serve as a forum for regulatory agencies to discuss trends that are unique to this industry. The prospect of such a body being well poised to provide guidance for the establishment of regulatory agencies in jurisdictions that have not yet established a regulatory framework for the sector, is of particular value. Some jurisdictions are of the view that the standards set by such a body should of necessity include minimum requirements in relation to licensing and supervision. However, one jurisdiction went further in suggesting that membership to this body should be circumscribed by these minimum requirements as there is no advantage, and possibly even some disadvantage to well-regulated jurisdictions, to have a body which would be open to jurisdictions that do not have a high standard of supervision for TCSPs. In that regard it was being suggested that admission to membership to this body should be predicated on the jurisdiction having a high standard for regulation and supervision of this sector. The view was also expressed that having only a handful of jurisdictions, all of which are non-OECD countries, applying licensing and prudential regulation to this sector, opens this sector up to greater vulnerability to money laundering and other crimes. It should be noted that of the ten jurisdictions that favour the establishment of such a body, the majority of that group would be classified as major offshore financial centres and they subject their significant TCSP sectors to vigorous prudential and AML/CFT oversight. However, it should be highlighted that two of the jurisdictions that support this position are onshore jurisdictions, one of which is an OECD member country.

90. In relation to the development of international standards specifically for TCSPs, a large majority of the responding jurisdictions, including all of those with rigorous prudential/licensing regimes for TCSPs, strongly supported this idea. It was suggested that international standards would help to harmonise performance and assessment criteria for TCSPs; and in time would close the loopholes and eliminate the opportunities for regulatory arbitrage. Respondents were strongly in favour of the requirement for the application to this sector of fit and proper assessment, as well as other more general supervisory requirements akin to those recommended by the Basel Committee, International Association of Insurance Supervisors (IAIS) and International Organisation for Securities Commissions (IOSCO).

---

65 This was a suggestion from the GB

66 BE, VG, BG, KY, GG, JE, AN, LC, VC and TC. Though BM responded in the negative, in its response it pointed to the views of TSPs in BM that are in favour of the institution of an international body.

CHAPTER 3: ANALYSIS OF MONEY LAUNDERING TYPOLOGIES

91. In the responses to the questionnaire, several jurisdictions provided case studies to demonstrate the misuse of TCSPs in their jurisdictions and in others, as well as to show how the implementation of AML/CFT requirements in this sector, together with the conduct of supervisory arrangements for TCSPs, contribute to the fight against money laundering. No case studies were provided on terrorism financing and so the ensuing chapter will focus only on the money laundering vulnerabilities of TCSPs. The typologies presented and discussed in this chapter are based on these case studies.

92. However, it should be noted that, in addition to the cases provided in the responses to the questionnaire, case studies were also extracted from a number of other sources, including the 2006 FATF Typologies Study on the *Misuse of Corporate Vehicles*, the Egmont Group website,[67] publications of the United States Senate's Permanent Sub-Committee on Investigations and the website of the Jersey Financial Services Commission[68]. The case studies used within this chapter are only a representation of all the cases gathered from the sources mentioned above. Other relevant cases are included in Annex II to this report.

93. This chapter has been divided into two main sections; the first section dealing with money laundering threats and the second section dealing with combating the money laundering threats. The typologies addressed in the first section relate to the threats that have been identified in the case studies received. The threats have been sub-divided in the following three main categories:

A. Threats posed by the jurisdiction as a whole;

B. Threats posed by TCSPs; and

C. Threats posed by professional intermediaries.

94. Category (A) highlights the importance of a robust AML/CFT regime at a national level and underscores the money laundering vulnerabilities that emanate from less vigorous AML/CFT regimes. Categories (B) and (C) focus on the threats and vulnerabilities posed by TCSPs and professional intermediaries as facilitators or perpetrators of money laundering. Throughout this report, professionals such as lawyers and accountants have been considered as part of the TCSP landscape whenever they perform the designated services. However, for the purpose of analysis of the typologies, they have been separately considered to take account of the fact that, in many jurisdictions, professionals are treated separately from the rest of the TCSP sector whether or not their services account for a significant portion of the TCSP services provided in the jurisdiction. The case studies may help to demonstrate their relative role within that sector.

95. Finally, in the second section of this chapter, the case studies dealt with in Category D are used to highlight ameliorative measures that can be taken to address the threats identified in the cases.

---

67 The Egmont Group (2006)

68 www.jerseyfsc.org

3.1 Money Laundering Threats

3.1.1 Threats posed by the jurisdiction as a whole

96. Deficiencies within the national laws and systems of a jurisdiction can pose a threat to the international financial system where there is weakness in AML/CFT laws and procedures. This has been highlighted in the FATF NCCT[69] process and more recently in the FATF's work to name and shame jurisdictions through the International Co-operation Review Group's (ICRG) review process and the public statement mechanism. There are obvious ways in which jurisdictions can constitute a threat, primarily among which is no or inadequate AML/CFT laws as well as no or ineffective regulation of the financial sector. However, even where the laws in place conform to the FATF 40+9 standards, there are other less obvious ways in which the legal or regulatory environment can motivate and attract criminals to bring business within that country's borders. Lack of financial or technical resources to enforce and give effect to laws and regulations are issues that affect many jurisdictions, especially those that have poorer economies or overwhelming social problems that utilise the bulk of limited resources.

97. The case studies considered in this section focus on how weaknesses within the AML/CFT regime of the jurisdiction as a whole, encourages the misuse of TCSPs for ML/FT purposes, or facilitates rogue TCSPs in their bid to establish schemes that assist criminals to have easier access to their criminal proceeds and/or to legitimise them. The typologies below focus in on factors such as bank secrecy laws and poor bank regulation; inadequate corporate registration requirements and weak regulation of TCSPs; and the use and proliferation of shell companies.

i. The presence of bank secrecy laws, poor bank regulation and other areas of deficiency in certain jurisdictions facilitate money laundering schemes created by or participated in by TCSPs; and can prevent or prolong detection by or cooperation with the home State of the money launderer.

98. Bank secrecy has a history spanning many decades and emanates from jurisdictions with extensive banking sectors that emphasised confidentiality for their clients through devices such as the use of numbered bank accounts to facilitate anonymity. Historically, bank secrecy laws have become notorious for providing cover for war operatives to funnel and secure money procured by them through looting the property of war prisoners; for enabling rogue leaders and dictators from impoverished countries to find a secure resting place for the millions of dollars of corruptly obtained lucre which further impoverished their nations; and more recently for becoming a harbour for criminal/money laundering schemes.

99. Secrecy in the banking sector restricts competent authorities from obtaining or sharing information on banking relationships and account activities; thereby preventing local or foreign authorities from ferreting out inappropriate or criminal behaviour within the banking sector. Unrestrained bank secrecy is therefore an area of AML/CFT vulnerability for jurisdictions; because criminals will seek out such jurisdictions in order to gain the protection afforded them from free exchange of information with other jurisdictions and law enforcement authorities. The case study below exemplifies how bank secrecy, exacerbated by extremely weak bank regulation and supervision can be misused by money launderers, predicate criminals and collusive banking officials. See also Case A in Annex II.

---

69 This process was undertaken by the FATF between 2000 and 2006 to identify non compliant countries and territories (NCCT). During this time 23 countries were listed due to lack of an effective AML/CFT system and they were subjected to annual review during this period to determine whether they could be removed from the list. The last country was removed from the list in 2006. Visit the FATF website at www.fatf-gafi.org for more information on this.

Example Case Study

Case No. 1: TCSPs role in laundering fraud proceeds and the benefits of bank secrecy laws

Bank X was an offshore bank licensed in 1997 to operate in a small jurisdiction which was known at the relevant time for its bank secrecy laws. One of Bank X's wholly owned affiliates was a corporate service company which was used primarily to form the trusts and corporations that made up Bank X's accountholders. These trusts and corporations, known as International Business Corporations (IBC), routinely received nominee director and shareholder services from the corporate service company. In 1998 Bank X became the fulcrum for a money laundering scheme established by Mr. K, a US citizen who operated a fraudulent high yield investment programme that targeted victims in the US. Mr. K relied on the bank and the corporate service company to establish IBCs for himself, his victims and co-conspirators; to open accounts for these IBCs with Bank X; to receive the 'investment' funds from victims and to transfer them into various accounts belonging to himself and his conspirators for onward transmission to other accounts and locations. Investigation by US law enforcement resulted in money laundering and fraud charges being laid against Mr. K. During the course of the investigation, numerous efforts through legal channels to procure information from Bank X about Mr. K's activities were refused by Bank X on the basis of the secrecy laws. US law enforcement was unable to obtain the detailed information about the transactions and the movement of the funds in Mr. K's bank accounts until Mr. K cooperated and instructed the Bank to provide the requested information. At the material time, although one of only seven (7) offshore banks licensed in that jurisdiction, BANK X was subjected to very minimal regulatory oversight.

Source: Extrapolated from Minority Staff of the Permanent Subcommittee on Investigations (US Senate)

100. In this case it is evident that the TCSP, which was closely affiliated with the poorly regulated offshore bank, was utilised to establish the corporate network to facilitate the activities of both the banks and the criminal players using the banks. The TCSP played an integral role in establishing and managing the accounts used by the criminal network to defraud its victims and then carry out the laundering process which followed. The TCSPs involved carried out the bidding of senior banking officials who were their principals, and in so doing appeared to have little separate corporate identity or independence.

ii. Jurisdictions with limited corporate registration requirements; unrestricted bearer share usage; limited beneficial ownership information requirements; and/or lax regulation of TCSPs.

101. The case studies reviewed in this regard highlight that regulatory and supervisory deficiencies in relevant sectors represent AML/CFT risk. The deficiencies in the cases relate to: the use of intermediaries in circumstances where there is an insufficiency in the corporate registration requirements; the unrestricted use of bearer shares; and inadequate requirements relating to beneficial ownership; and what can only be overall weaknesses in the regulation or supervision of TCSPs. Because TCSPs provide services in relation to the establishment and management of corporate structures, trusts/foundations, and structuring of investments, criminals will often target TCSPs or other intermediaries in jurisdictions that have weak laws and/or inadequate enforcement of laws in these areas. They will seek to capitalise on these weaknesses and use the intermediaries to distance themselves from the money laundering and other criminal schemes established on their behalf. The cases also show that while some offshore jurisdictions have been vulnerable to misuse in this way, TCSPs in onshore jurisdictions were at liberty to take advantage of these circumstances due to inadequate restrictions on their operations.

Example Case Study – Jurisdictions that have insufficient beneficial ownership requirements to facilitate international cooperation

Case No. 2: Inadequate beneficial ownership information requirements

Acting on information from the foreign Central Bank and STR from an Austrian Bank, the Austrian FIU conducted enquiries into suspected cases of tax evasion and money laundering being carried out by foreign banks with correspondent relationships with banks in Austria. The STR related to transactions by the foreign banks involving different offshore companies amounting to about USD 45 000 000.

The A-FIU analysed the transactions relating to the correspondent banking accounts and tried to link these transactions with a predicate offence. The A-FIU also made requests to several FIUs in other jurisdictions.

The responses received from these foreign FIUs, and also the A-FIU's own investigations, confirmed that the transactions involved approximately 72 offshore companies (as sender and receiver) but no information regarding the beneficial owner or the registration country of the different offshore companies involved was able to be obtained. The A-FIU were able to establish and trace the existence of only six offshore companies (receiver of the money) and made requests for further information. However unfortunately the only information available was that the companies were registered but the work regarding the due diligence and the real beneficial owners was done in another jurisdiction by lawyer companies.

Source: submitted by AT

102. Bearer shares are shares that can be readily moved from share holder to share holder without any requirements for the recording of the ownership details with the company or any competent authority. Ownership of these shares vests in the person or entity that has physical possession of the shares at any given time. This type of share ownership affords anonymity to the shareholder who can freely obtain and pass on these shares. The unrestricted use of bearer shares not only prevents competent authorities from being able to identify the legal or beneficial ownership of corporate structures, but in tandem with inadequate AML/CFT requirements for and oversight of TCSPs, it also provides a veritable blank cheque for rogue TCSPs to design and operate money laundering schemes using corporate vehicles for the benefit of their criminal clients.

Example Case Study – Jurisdictions that allow unrestricted use of bearer shares

Case 3: Concealment of beneficial ownership information through use of bearer shares

As a result of a drug importation investigation, approximately USD 1.73 million was restrained in combined assets from residential property and bank accounts. These assets were located in four countries in various regions. Significant assets restrained involved two offshore companies incorporated in Country A. Investigators also seized original bearer shares of three offshore companies and original articles of incorporation. The investigation revealed that one of the suspects used the services of a lawyer from Country B to design a money laundering scheme that included the incorporation of offshore companies with bearer shares. The lawyer hired the services of a management company in Country C, who in turn used the services of a company in Country A to incorporate bearer share companies in Country A.

There was no requirement to register the names of the shareholders at the corporate registry office, company head office or anywhere else. The only names that appeared were the original incorporators of the company in Country A, who then forwarded the bearer shares and articles of incorporation to the Country B management company. The management company then forwarded the original bearer shares and articles of incorporation to the lawyer, who in turn handed them over to his client. The files held by the management company only contained the names of the nominee directors, nominee administrators and the directions given by the Country B lawyer who acted on behalf of the suspect shareholder.

The use of bearer shares companies and professional intermediaries in this investigation almost offered absolute anonymity to the person in possession of the bearer shares and is clearly a powerful tool to conceal proceeds of crime. If investigators had not seized the bearer shares in the possession of the suspect, it would have been impossible to determine the owner of these companies and ultimately to identify and restrain their assets as proceeds of crime. In this case, the offshore companies held significant assets alleged to be the proceeds of crime - bank accounts in Country C, and residential property in Country B and Country D.

Source: extracted from website of JE Financial Services Commission [a]

a. Found on the JE FSC website in **"Anti-Money Laundering/Countering the Financing of Terrorism Typologies from a Jersey perspective"** published on October 28, 2008 and produced by BakerPlatt on behalf of the Law Officers, Joint Financial Crimes Unit and the JE Financial Services Commission. The purpose of the publication was to raise awareness of typologies that are relevant to JE including the risks arising from the nature of the customer base and products associated with Jersey as an international finance centre. Both local and international cases were used. The cases included within this report with the annotation "Extracted from website of JE Financial Services Commission" are the international cases referenced in the October 2008 publication. The origins of the international cases used in the publication are not noted therein.

103. Many jurisdictions operate central registries of companies, requiring a record of all corporate structures established in the jurisdiction to be stored there. Company registries may have various minimum requirements for the information that needs to be submitted to them. Beneficial ownership information is often one type of information required to be submitted to a company registry at the time of a company's formation. However, as can be seen from the responses to the questionnaire, many jurisdictions choose to either share between TCSPs and the company registry the responsibility for capturing and maintaining beneficial ownership information; or they place the entire

responsibility on TCSPs alone. However, there are jurisdictions where no one is charged with this duty and this becomes an area of vulnerability as it provides anonymity for beneficial owners of companies formed in the jurisdiction. This can become an allurement for money launderers and other criminals who wish to use corporate structures to launder their criminal proceeds, as they are no doubt aware that secrecy surrounding company ownership is a significant obstacle in combating money laundering and other financial crimes.

Example Case Study– Jurisdictions whose corporate registration processes do not require the submission of beneficial ownership information to competent authorities or the capture by TCSPs of such information

Case No. 4: Registration process that does not require identification of beneficial ownership

In 2002, U.S. Immigration and Customs Enforcement (ICE) (through its legacy agency U.S. Customs) received a request for assistance from a foreign customs service concerning alleged customs fraud with respect to the importation of various kinds of used trailers, semi-trailers, container-transporters, and transport-vehicles equipped with supplemental cranes. The foreign customs service alleged that the invoices and customs entry documents undervalued the actual cost of the vehicles, and misrepresented the country of origin of the merchandise. The customs entry documents and accompanying invoices identified a US-based company in Washington DC as the exporter of the vehicles.

As a result of the foreign request, ICE was asked to interview company officers located in Washington, DC, in an attempt to determine the origin of the suspected fraudulent invoices. The investigation revealed that the suspect company was incorporated in the District of Columbia and the Registered Agent was a Washington, DC "corporate registration agency." The President of this corporate registration agency was interviewed and told agents that his company "provides assistance to mostly foreign companies with U.S. export documentation, and serves as a U.S. incorporation agent." He went on to advise that his company had been requested by a corporate registration agency from Delaware to assist in filing the District of Columbia incorporation papers on behalf of the suspect company. He advised that approximately 60% of his business was referrals from the Delaware corporate registration agency. The agents were told that no documents relating to the suspect company were maintained by his registration agency and they should contact the Delaware registration agency for those documents.

Agents contacted the Delaware registration agency and were told the suspect company was "ordered and paid for" by a foreign corporation registration agent. The agents were told that if they wanted additional information, they would have to contact the foreign corporate registration agency located in an offshore jurisdiction. According to its website, the foreign corporate registration agency provides advisory, management, and administrative services relating to offshore companies.

Because there is no requirement in the U.S. for the identification of beneficial ownership at the time of incorporation, the ICE investigation was unable to obtain the information that the foreign customs authorities had requested.

Source: submitted by US

iii Use of Shell companies

104. Shell companies are corporate entities that are used for legitimate purposes such as to hold stock or intangible assets of another business entity. However, they can also be misused by illicit actors and have no legitimate commercial purpose. While it is arguable whether shell corporations can have appropriate application in the operations of legitimate corporate groups, they can be used by white-collar criminals in money-laundering operations, mutual-fund schemes, tax fraud and internal business fraud. To facilitate these types of schemes, shell companies may be used to generate false invoices, fictitious consultancy fees or bogus loans.[70] Where shell companies are permitted under the corporate registration laws of a jurisdiction or where its usage is unrestricted, this may present a money laundering and financial crime vulnerability which criminals will take advantage of. It has

[70] This issue was discussed in the APG/FATF "*Anti-Corruption/AML/CFT Research Paper*", 2007 prepared for the FATF/APG Project Group on Corruption and Money Laundering by Dr. David Chaikin and Dr. Jason Sharman (7 September 2007). This paper was presented to the FATF Plenary in 2007 and the APG Plenary in 2008.

been acknowledged that tackling the problem of anonymous shell companies is a crucial factor in combating a range of high priority international problems such as organised crime, tax evasion, corruption and money laundering.[71]

105. Shell companies together with other tools used in financial crimes, can be used in both the placement and layering phases of the money laundering process to disguise the trail of evidence. The cases below show various ways in which shell companies have been used to establish layers between the criminal and the laundering, fraudulent or corrupt transaction; and between the predicate crime and the criminal proceeds. Where jurisdictions allow their incorporation processes to be indiscriminately used in this way, TCSPs will have no reason to self regulate to prevent criminals from taking advantage of this facility.

Example Case Studies

Case No. 5: Use of shell companies to facilitate corrupt payments

An operational business goes through a TCSP with the objective of getting control (via a fiduciary/trust contract) of a shell company domiciled under European law, giving it the appearance of being operational. The objective is to pay the shell company a compensation for fictitious consulting services. This fee is then paid by the TCSP, on behalf of the shell company, to a third person who in turn is responsible for bribing a public official who grants access to a public exchange to the above-mentioned operational business. This corruption can be done with or without the knowledge of the TCSP.

Source: submitted by CH

Case No. 6: Use of domestic and foreign shell companies in the placement and layering stages of money laundering

ICE initiated an investigation against a criminal organisation involved with defrauding investors out of millions of dollars and laundering the fraudulently obtained proceeds. The investigation revealed an enterprise of individuals offering fictitious instruments for investment programs described as "currency leasing trading programs," leading to more than USD 14 million in fraudulent transactions. These funds were laundered through a network of domestic and foreign bank accounts utilizing shell corporations, many of which had been established in the United States.

The perpetrators of the scheme operated an Internet web site out of Las Vegas, Nevada, which offered investors the opportunity to "lease" $1 million for a fee of USD 35 000. Once "leased," victims were told these funds would be placed into a high yield international trading program. The contracts provided to the investors indicated an expected return on their investment of as much as 25 percent every two weeks.

An additional co-conspirator in the scheme was responsible for establishing a complex web of bank and brokerage accounts, and shell companies. This individual established corporations in Delaware, Nevada, California, and Massachusetts in the United States along with companies in several foreign jurisdictions. Another co-conspirator opened cash management accounts at brokerages utilizing the shell corporations. Investors were told to send their USD 35 000 fee to the accounts established utilizing the shell corporation names. Once in this account, the funds were transferred to secondary accounts. From these accounts, the funds were then disbursed to various foreign and domestic accounts and liquidated through the use of checks, debit cards, and ATM cards.

In the end, six individuals pled or were found guilty in the United States of violating money laundering, wire fraud, and international transportation of stolen funds statutes. The defendant's use of domestic and foreign shell companies to layer the funds prevented full recovery of the fraudulently obtained funds.

Source: submitted by US

[71] Sharman, Dr. Jason C. *"Behind the Corporate Veil: Financial Anonymity and Crime"*, 2008. Dr. Sharman is a Professor at Griffith University in Brisbane, Australia and works jointly with the Centre for Governance and Public Policy and the Griffith Asia Institute. This paper is based on research done to assess the effectiveness of international standards that prohibit anonymity within the global financial system.

106. These cases show that money launderers and other criminals will use TCSPs to take advantage of systems that allow for the establishment of corporate structures with no apparent legitimate commercial purpose.

3.1.2 Threats posed by TCSPs

107. The typologies addressed in this section relate to the threats posed by TCSPs, which have been identified from the case studies and responses. These typologies address the vulnerability of TCSPs for being used by both internal and external persons/entities for money laundering purposes.

i. Criminal culpability of TCSPs involved in money laundering schemes or the predicate crimes which give rise to it

108. The responses received from the jurisdictions that participated in this typologies exercise, reveal that TCSPs are increasingly involved in money laundering schemes. TCSPs and/or their principals have in many jurisdictions been under investigation, and at times convicted, for money laundering and proceeds of crime related offences. While some countries have reported more cases of misuse of TCSPs by criminals for money laundering purposes than others, it remains undoubtedly the case that the potential risk for misuse is evident across jurisdictions. Given the diverse nature of activities of TCSPs within and across jurisdictions and the diverse oversight regime governing these activities, it is difficult to determine whether the lack of money laundering cases in some jurisdictions is due to the absence of abuses within those jurisdictions or the inability thus far of regulatory and law enforcement authorities to detect such abuses. Nonetheless, the threat resulting from the potential role of TCSPs in facilitating money laundering and terrorist financing constitutes a major concern among jurisdictions where TCSP businesses are prevalent.

109. It is in this context that this typologies exercise sought to understand the types of misuse of TCSPs for money laundering and terrorist financing purposes and the specific "red flags" that may be indicative of it. More specifically, the potential vulnerabilities that appear to be inherent to the very nature of the activities of TCSPs have been examined.

110. Although TCSPs are less conducive to the initial placement of criminally derived funds than for example, banking institutions, they are prone to be used particularly in the layering stage of money laundering. TCSPs possess many characteristics that make them vulnerable to misuse for money laundering and terrorist financing purposes. Their fiduciary responsibility allow them often times to have discretionary control over the accounts and funds of their clients. Due to the broad scope of their fiduciary responsibility, the risk exists that TCSPs may abuse this responsibility entrusted to them. Furthermore, the ease with which the sources and uses of funds as well as legal beneficial ownership information can be concealed through the establishment of multiple accounts and the conduct of complex transactions on behalf of clients, constitutes another area of potential threat.

111. The case examples presented in this section highlight the areas of vulnerability to money laundering of TCSPs, as well as the risk of being misused in a variety of ways and for different purposes within the framework of money laundering. More specifically, the cases highlight the following money laundering related misconducts: misappropriation of clients' assets, and facilitation of money laundering for organised crime groups by abusing discretionary control over clients' funds. Case F and others in Annex II also demonstrate money laundering misconduct by TCSPs through misrepresentation of clients' beneficial ownership information, among other things.

Example Case Studies

Case No. 7: Criminal culpability of TCSPs based on co-mingling of clients' funds

A company service provider on the island State of Country A embezzled USD 35 million from its clients over an 11-month period. The money was sent to some international criminal network organisations in Country B. The CSP was co-mingling its clients' funds with its own assets. The owner of the CSP was convicted and sent

to prison.

Source: submitted by AN

Case No. 8: Criminal culpability of TCSPs as facilitator of ML

A Company Formation Agent involved in the financial services sector was prosecuted for money laundering offences, for laundering funds on behalf of organised crime groups. He carried out a complex process of funnelling criminal proceeds through a system of trusts and front and shell companies, linked to a complex matrix of inter-account bank transfers. As administrator of all the trusts used in the scheme he exercised full control of the funds flowing through them. Trusts, as well as front and shell companies were used deliberately to disguise the source of the money, and to provide a veil of legitimacy to the financial transactions.

Source: submitted by the GB

112. From the cases it is evident that TCSPs can play a significant role in facilitating money laundering and that the perpetration of money laundering crimes can take place in various forms. Cases such as the White Whale case[72] also highlight the fact that not only can TCSPs be used by criminals for the entering or mediation of transactions from or intended for criminal activities, but also their principals and/or employees can play an important facilitating role in the money laundering process. This internal risk factor is one that should be monitored closely.

ii. Misuse of TCSPs by money launderers and terrorists to establish sophisticated/complex legal structures to facilitate money laundering.

113. Although the nature of the services provided by TCSPs vary from one institution to another and at times from one jurisdiction to another, it is generally noted that TCSPs are prone to be used for the set up and management of complicated structures through which money may be laundered or terrorist funds channelled. Structures created by TCSPs to facilitate legitimate business activities might also be attractive to money launderers and terrorists, particularly at the layering stage. A money launderer may seek the service of a TCSP to set up legal structures or arrangements in multiple jurisdictions. Jurisdictions that do not require identification of beneficial owners; or that refuse to disclose such information when requested by competent authorities; or that do not have a robust regime of combating money laundering and terrorist financing, are jurisdictions often times of particular interest to the money launderers and terrorists. Once the legal entities or legal arrangements are established, the money launderer or terrorist typically uses the companies or legal arrangements, by moving funds through the various company accounts, for money laundering or terrorist financing purposes.

114. It should also be noted that money launderers are well aware of the fact that investigation of a money laundering scheme is more complicated when there are more jurisdictions involved, since some jurisdictions may be unable or unwilling to provide information on the legal entities or arrangements. As a result, the authorities investigating a particular money laundering scheme will be unable to establish the link between the funds and the criminal.

115. The ease of formation of companies and legal arrangements in various jurisdictions, some of which have a less robust oversight regime than others, make it also easier for money launderers to layer the proceeds of their criminal activities and integrate them into the financial system. Furthermore, advances in technology, financial engineering and innovation, have contributed significantly to the use of sophisticated legal structures and multiple accounts to facilitate money laundering and terrorist financing. This has made it more difficult to identify who is actually controlling the structures and accounts thereby contributing to a lack of transparency.

---

[72] See Case No. 11: *TCSPs obscuring beneficial ownership through the use of pre-constituted companies*

116. Although it is likely that a majority of the sophisticated/complex structures established by TCSPs for their clients are set up for legitimate purposes, the obvious potential for abuse nevertheless remains a concern. The following case, along with others in this report, highlights the money laundering risk inherent in these complex structures that are created and/or administered by TCSPs.

Example Case Studies

Case No. 9: Complex multijurisdictional structures to facilitate money laundering

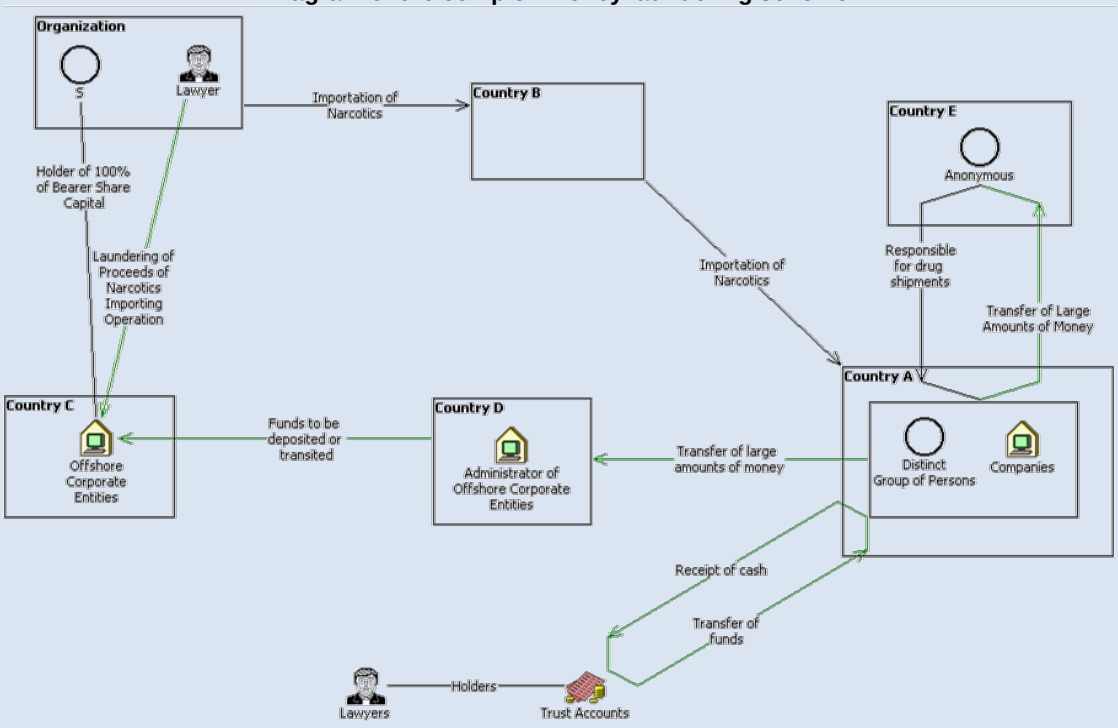
S headed an organisation importing narcotics into Country A, from Country B. A lawyer was employed by S to launder the proceeds of this operation.

To launder the proceeds of the narcotics importing operation, the lawyer established a web of offshore corporate entities. These entities were incorporated in Country C, where scrutiny of ownership, records, and finances was not strong. A local management company in Country D administered these companies. These entities were used to camouflage movement of illicit funds, acquisition of assets, and financing criminal activities. S was the holder of 100% of the bearer share capital of these offshore entities.

In Country A, a distinct group of persons and companies without any apparent association to S transferred large amounts of money to Country D where it was deposited in, or transited through S's offshore companies. This same web network was found to have been used to transfer large amounts of money to a person in Country E who was later found to be responsible for drug shipments destined for Country A.

Several other lawyers and their trust accounts were used to receive cash and transfer funds, ostensibly for the benefit of commercial clients in Country A. When they were approached by law enforcement during the investigation, many of these lawyers cited "privilege" in their refusal to cooperate. Concurrently, the lawyer established a separate similar network (which included other lawyers' trust accounts) to purchase assets and place funds in vehicles and instruments designed to mask the beneficial owner's identity. The lawyer has not been convicted of any crime in Country A. Investigators allege however that his connection to and actions on behalf of S are irrefutable.

Diagram of the complex money laundering scheme



Source: extracted from website of JE Financial Services Commission [a]

a. Found on the JE FSC website in **"Anti-Money Laundering/Countering the Financing of Terrorism Typologies from a Jersey perspective"** published on October 28, 2008 and produced by BakerPlatt on behalf of the Law Officers, Joint Financial Crimes Unit and the JE Financial Services Commission. The purpose of the publication was to raise awareness of typologies that are relevant to JE including the risks arising from the nature of the customer base and products associated with Jersey as an international finance centre. Both local and international cases were used. The cases included within this report with the annotation "Extracted from website of JE Financial Services Commission" are the international cases referenced in the October 2008 publication. The origins of the international cases used in the publication are not noted therein.

Case No. 10: Complex structures to facilitate money laundering

This case is concerned with the use of seven (7) International Business Companies which were incorporated in AI by a foreign national, Mr. D, using a local TCSP. The seven companies were then used to open bank accounts in AI at two local private banks; these accounts were then utilized as the flow through points for money obtained from elaborate investment wire fraud scheme targeting persons from across the Americas, Asia and Europe. The monies would flow through bank accounts in AI and another jurisdiction then onwards to accounts in Europe. Over USD 4 million was defrauded from investors who were investing into the schemes of Mr. D. Mr. D was arrested by the authorities in the other jurisdiction and extradited to the USA for prosecution for fraud and money laundering. The remaining USD 80 000 which Mr. D had in AI was subject to a civil recovery process for forfeiture to the State.

Source: submitted by AI

iii. Complex methodology used by TCSPs on behalf of money launderers to obscure beneficial ownership of legal structures used in money laundering schemes

117. A subject closely related to the lack of transparency in complex structures which was addressed above, is the risk involved with the concealment of beneficial ownership of legal structures. This is a subject that has been significantly debated over the past years, considering the perceived confidentiality inherent in the services provided by TCSPs. The reduction or elimination of face-to-face contact between the service provider and its customer has made it even more difficult to know who is actually controlling the structures and/or accounts.

118. The responses received highlight the fact that the identification of a customer at the beginning of a business relationship may not be sufficient for the detection of serious or organised money laundering crimes developed after the client acceptance phase. Both the relationship and the beneficial ownership must continue to be monitored after the initial client acceptance stage. If not adequately monitored, the TCSP may lose sight of the true person(s) controlling the legal structure.

119. Although the concealment of beneficial ownership may take place in various forms, as reflected in the cases below, the concern was also raised during this typology exercise of the difficulty in identifying beneficial owners, particularly in the case of legal entities, such as foundations; and legal arrangements, such as trusts. In those cases, there is no generally agreed upon definition of beneficial ownership. The issuance of bearer shares also seems to be an area of risk that may obscure beneficial ownership.

Example Case Studies

Case No. 11: TCSPs obscuring beneficial ownership through the use of pre-constituted companies

THE WHITE WHALE CASE

The investigations started in September 2003 by cross referencing data from an investigation on drug trafficking, with information coming from another investigation on assets owned by Eastern European citizens living in the Costa del Sol (Malaga). In such cross referencing of information, it arose that [H] appeared as administrator of more than 300 companies established through [R], a lawyer's office in Marbella (Malaga). All of the companies had similarities: companies established off-shore, except one held by [H] who was the single administrator of the companies and, at the same time, an employee of [R]. Giving support to clients of [H] by establishing companies was one of the activities of [R], which also offered the management of client's bank accounts and real estate buying and selling. The investigators knew that several clients of [R] were allegedly connected with international organized crime groups and/or with people involved in serious crimes in Spain and abroad.

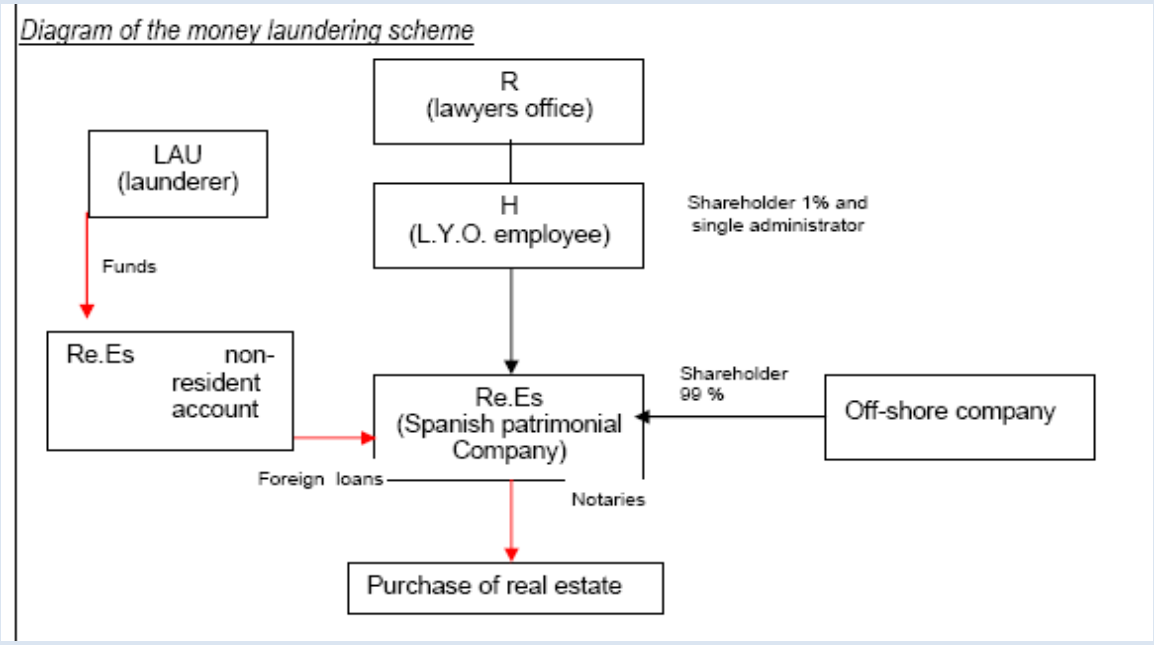
The board of [R] was aware of the likely criminal activities of some of H's clients, because they had been the subject of media and press reports as possible criminals, and because the board knew that some clients were in prison in Spain or in other countries since documents had been sent to them there. In other cases, members of the board were called to testify as witnesses in judicial proceedings against those clients. Additionally, the board deliberately ignored the activities of their clients. In their advertisements they even advertised that the office conducted company´ "engineering", that they guaranteed anonymity and that they did not ask any questions or respond to requests for information.

The Spanish companies were established for use as an instrument for money laundering schemes based on the real estate market. They were companies created exclusively for the management and administration of real estate properties. Re.Es. was one of these companies. The off-shore companies which participated in the Spanish companies were "shell companies" established in an American State whose laws allow a special tax regime for these companies and for their transactions. The companies were pre-constituted in the name of an agent (usually a lawyer) before the incorporation of the company. In other words, the document of incorporation of the company would remain inactive in the hands of the agent until the company was bought by a client, and at that moment the company would be effective.

Therefore, the board of the companies when first registered was made up of the agent and his associate, without any link with the real owners of the company who subsequently purchased the shell. Consequently, the ultimate beneficiaries of the off-shore companies and, consequently, of the Spanish companies, remained hidden. The launderer (LAU) transferred funds from a foreign country to a non-resident account owned by Spanish company Re.Es. The use of non-resident accounts provided other advantages, including the advantage of being subject to less control by the tax authorities. The funds described above were gathered in the account of Re.Es under the guise of foreign loans received. The destination of the funds received was the purchase of real estate properties in the name of Re.Es. in the last stage of the money laundering process, taking advantage of the hidden situation of the launderer and of the beneficial owners.

Three public notaries documented all the transactions, from the incorporation of the companies to the purchase of real estate. The suspicion of money laundering was clear: incorporation of several companies by the same persons in a short period of time, concurrence of the same partners in several companies, several real estate purchases in a short period of time, etc. Despite this, and even though the public notaries were obliged to report under the Spanish anti-money laundering law, such transactions were not disclosed to the Spanish FIU

Diagram of the money laundering scheme



Source: extracted from 2006 FATF Typologies Study – Submitted by ES

Case No. 12: TCSPs instrumental in obscuring beneficial ownership by PEP

Mr. X, a foreign lawyer, utilized the services of several Trust and Company Service Providers to set up several offshore entities in various offshore Financial Services Centres including Countries A, B and C.
The offshore entities included a private growth Fund which was registered in Country B. The subscriptions which were paid into the Fund were routed through the various offshore entities in order to obscure the true source of the funds. At least two of the offshore entities were known to have bank accounts at a financial institution in Country B, where significant funds were located.

A joint investigation was subsequently initiated by authorities in Countries A and B, following allegations that the structures were set up to disguise the true source of the funds which allegedly came from a PEP in an Eastern European country and that these funds were the proceeds of corruption. Information regarding the true ownership and purpose of the offshore entities was requested from TCSPs in the respective jurisdictions. The resultant information was incomplete. Though the foreign Lawyer claimed ultimate beneficial ownership of the entities, the authorities believed he was acting on behalf of the PEP. Investigation indicated that the private growth fund was established on behalf of a prominent Minister of Government in the Eastern European

country, who used the fund and the several other offshore entities to create a number of fictitious consultancy agreement entities, for the purpose of concealing millions of dollars he made as a result of investments in the sector which fell under his ministerial portfolio during his time as Minister.

The investigation ultimately resulted in criminal charges being brought against several of Country A registered offshore entities. These charges led to the successful prosecution and confiscation of USD 47 000 000.00 which was shared equally between the Countries A and B.

Source: submitted by the VG

3.1.3 Threats posed by Professional Intermediaries

i. Use of professional intermediaries to facilitate money laundering.

120. Lawyers, accountants, notaries and other such professionals provide services to clients to help them navigate the often complex and sometimes treacherous world of finance, law and corporate governance. They have essential knowledge and expertise in relation to the technical rules and regulations that pertain to the operation of business, as well as experience in crafting legal strategies in relation to investment, mergers and acquisitions, tax liability, corporate structuring, among others. These professionals can be important service providers for businesses, high net worth investors and anyone who has wealth or assets which need to be managed or channelled appropriately. However, these same skills and expertise are attributes that are desired by criminals, who require assistance in organizing their affairs, to enable them to distance proceeds from their criminal origins; and to liberate these proceeds for eventual use in 'legitimate' endeavours. For this purpose criminals seek out the services of professional intermediaries to help them establish corporate structures, set up trusts, transfer funds and negotiate deals. The important advantages to the criminal are: the concealment of the proceeds of crime; the granting of access to various financial centres through the diverse mechanisms which can be used by these intermediaries; and the creation of confusing audit trails to stymie law enforcement's efforts with regard to these transactions.

121. The nature of the relationship established with the professional, the integrity of the individuals involved and the level of regulation and regulatory oversight can all affect the degree of knowledge or involvement of the professional in the criminal scheme being pursued. However, it is safe to say that the more complex the scheme being established and the more economically senseless the approach adopted, then the more likely it is that the professional intermediary involved knows, strongly suspects or is wilfully blind to the true nature of the activities which underpin the professional services being provided.

122. The following cases provide some examples of the role played by professional intermediaries in money laundering schemes.

Example Case Study

Case No. 13: Use of professional intermediaries to facilitate money laundering

A law enforcement operation identified an accountant, J, who was believed to be part of the criminal organisation involved in money laundering and re-investment of illicit proceeds derived from drugs trafficking led by X. J's role was mainly that of a "legal and financial consultant". His task was to analyse the technical and legal aspects of the investments planned by the organisation and identify the most appropriate financial techniques to make these investments appear legitimate from a fiscal stance. He was also to try, as much as possible, to make these investments profitable. J was an expert in banking procedures and most sophisticated international financial instruments. He was the actual financial "mind" of the network involved in the re-investment of proceeds available to X. J operated by sub-dividing the financial transactions among different geographical areas through triangle transactions among companies and foreign credit institutions, by electronic transfers and stand-by credit letters as a warrant for commercial contracts which were later invested in other commercial activities.

Source: extracted from website of JE Financial Services Commission[a]

a. See Case No. 3: *Concealment of beneficial ownership information through use of bearer shares*, note a

Case No. 14: Use of professional intermediaries to facilitate money laundering

A criminal involved in smuggling into GB set up a Trust in order to launder the proceeds of his crime, with the assistance of a collusive Independent Financial Adviser (IFA) and a Solicitor, who also appeared to be acting in the knowledge that the individual was a criminal. The Trust was discretionary and therefore power over the management of the fund was vested in the Trustees, namely the criminal, his wife and the IFA. This example illustrates the complexity of Trusts used to hide the origins of funds from any law enforcement scrutiny. One way in which this was done was through the purchase of a garage. The criminal's daughter, who was a beneficiary, was given the property by her father and she in turn leased it to a company. The property was eventually sold to this company, the purchase funded by a loan provided by the Trust. The company subsequently made repayments of several thousand pounds a month, ostensibly to the Trust, but in practice to the criminal. Thus the criminal who had originally owned the garage probably maintained control despite his daughter's ownership. Through controlling the Trust he was able to funnel funds back to himself through loaning funds from the Trust and receive payments on that loan.

Source: submitted by GB

3.2 Countering the Money Laundering Threats

3.2.1 Measures that can reduce money laundering threats

i. Application of suspicious transaction reporting, CDD and other such measures enhance TCSPs role in the detection, investigation and/or prosecution of players in the money laundering scheme

123. The cases below are good examples of how the operation of an appropriate AML system within TCSPs can facilitate law enforcement's efforts to address money laundering transactions and activities which might otherwise go undetected. The cases below range from instances of mere suspicion triggered by unusual or questionable transactions resulting in the filing of STRs, to active instances of sleuthing by the TCSP as a result of suspicion aroused through implementation of regular CDD procedures or because of suspicious activity.

Example Case Studies

Case No. 15: Detection of illegal activities by TCSP, reporting to the FIU, and international cooperation between FIUs

Mr. A established a KY revocable trust in 2004, with himself as settlor and a local Trust Company B as service provider acting as trustee. Mr. A also arranged for the incorporation of a KY company known as company C, with the Trust Company B also acting as registered office.

In 2008, Trust Company B, in conducting its risk assessment of its clients, became aware of allegations relating to Mr. A and his involvement in an oil and gas contract scam which also involved members of a foreign jurisdiction's government. Mr. A was the representative of the oil and gas company and was allegedly involved in a kickback scandal in which his company was awarded a contract by the foreign jurisdiction's government.

According to allegations in media reports, Mr. A was the money source who provided several officials from the foreign jurisdiction's government with the means to buy the support of other government officials, in order for them to participate in the scam.

Trust company B reported in its suspicious activity report, that between 2004 and late 2005, Mr. A's trust and underlying company had received numerous transfers of funds and property from what was now deemed to be questionable sources, which in turn heightened its suspicions, thereby prompting its reporting to the FRA.

An analysis of the trust accounts, undertaken by the FRA, reflected outgoing funds to individuals named in numerous media reports who allegedly took part in the kickback scandal. The FRA in turn requested information from the FIU of the foreign jurisdiction to enquire if there were any investigations or criminal proceedings underway involving Mr. A. The foreign FIU responded that Mr. A was being investigated for money laundering and corruption of government officials. The FRA was also able to construct a timeline of events which revealed that funds and other assets were being added to the trust around the same time the alleged criminal activity of Mr. A and others was reported.

As a result of the FRA's analysis and information from the FIU of the foreign jurisdiction, a disclosure was made to that FIU based on the premise that a KY trust and company was being used to house the proceeds of Mr. A's criminal activity. The information disclosed by the FRA was useful to the overseas FIU and the

investigations of the foreign jurisdiction, and the matters before the courts are still pending.

Source: submitted by KY

Case No. 16: Detection of fraudulent malpractice insurance and international cooperation

Mr. L, a citizen of country A with prior criminal convictions, set up two medical liability insurance companies in third countries and offered fraudulent malpractice insurance coverage to medical practitioners and practices in Country A. Mr. L also opened two bank accounts in BM in the name of two of the insurance companies controlled by him, along with a mailing drop box account with a local mailbox service in BM, thereby establishing a nominal office in Bermuda for each of these insurance companies. Both the drop box and the bank accounts were managed by a BM corporate service provider. Mr. L also had other similar drop box and bank account schemes in Country A and in several countries. Premiums collected under these fraudulent insurance contracts were paid through the network of mailing/drop box accounts into related bank accounts. Through ongoing due diligence, the BM service provider became unhappy with responses from Mr. L arising from questions/complaints from customers of the insurance companies. The service provider therefore made a suspicious activity report triggering an investigation locally. This tied in with suspicions originating from a potential customer in Country A, who was also approached and offered insurance coverage, thereby resulting in investigations by local authorities in Country A. The net result was that, in cooperation with law enforcement authorities in Country A, BM secured in excess of $5,000,000.00 by restraining the accounts of Mr. L's insurance companies in BM, and this amount was eventually repatriated to Country A to assist in making restitution to the victims. BM authorities provided significant evidence to Authorities in Country A via mutual legal assistance to facilitate Mr. L's prosecution for fraud and money laundering.

Source: submitted by BM

ii Benefits of sound regulation of TCSPs

124. The FATF Recommendation 24 requires that TCSPs be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. There should be a designated competent authority or SRO responsible for monitoring and ensuring compliance of TCSPs. The authority or SRO should have adequate powers to perform its functions, including powers to monitor and sanction. The "Risk-Based Approach Guidance for Trust and Companies Service Providers issued by the FATF on June 17, 2008"[73] has also highlighted the fact that the regulation and oversight of TCSPs should have a risk-based character. The regulation and oversight regime should have a targeted function and focus on areas of high risk.

125. From the responses received from the jurisdictions participating in this typology exercise, it is evident that the nature, level and scope of the regulatory and oversight regime applicable to TCSPs, vary from jurisdiction to jurisdiction. Some jurisdictions have a more robust regulatory framework, while others do not. In the responding jurisdictions that have a regulatory framework for TCSPs, this framework more often than not encompasses both off-site and on-site supervision. Some countries have a long-standing history of active regulatory oversight of trust and/or company service providers, while other countries concentrate more on criminal investigation and detailed record-keeping requirements. Other countries have implemented regulatory systems that comprise of aspects such as licensing of both trust service providers and company service providers, detailed customer due diligence requirements, record keeping and reporting requirements, auditing requirements, sanctions and enforcement.

126. Although there are differences in the regulatory approaches of the various countries, the overriding consensus is that additional regulatory guidance will likely be needed to reduce vulnerabilities of TCSPs to misuse for money laundering and terrorist financing purposes. An effective regulatory regime commands a premium. The questionnaire responses from those jurisdictions that have implemented an effective regulatory regime, suggest that they have significantly strengthened their ability to deter and address money laundering and terrorist financing abuse in their jurisdictions. Countries must implement regulatory and supervisory policies and

[73] Available on the FATF website at http://www.fatf-gafi.org/dataoecd/19/44/41092947.pdf

practices that conform to the scope and complexity of their specific sector. Public confidence in TCSPs, and hence their stability, can even be undermined by adverse publicity as a result of their unwitting use by criminals for money laundering and terrorist financing purposes.

127. The cases below shed further light on this important subject of effective regulatory oversight. They underline the fact that if TCSPs are not subject to an effective and adequate regulatory regime, they may be exposed to a greater level of money laundering and terrorist financing risk.

Example Case Studies

Case No. 17: Effectiveness of on-site inspections to prevent and detect money laundering

Corporate Service Providers (CSP) and Trust Service Providers (TSP) are under regulatory control in the IM. One entity licensed as a CSP was found, at its first full supervisory visit by the Regulator, to have serious Customer Due Diligence (CDD) problems, especially entailing lack of beneficial ownership details. A remedial programme was agreed and put in place with the CSP.

Subsequent supervisory inspections showed that the CSP was not making satisfactory improvements and formal Directions and reporting requirements were issued to them to fully comply and record progress with the remediation programme. A Direction was also issued that no new business was allowed to be taken on.

In the meantime the CSP applied for a licence to carry out TSP work. The Regulatory authority refused to process this application until the CSP side of the business was put in order.

The CSP submitted its required reports on the progress made in improving its CDD standards. A further supervisory visit showed some positive improvements but not as much as had been indicated in the company's reports. The visit also found evidence of further examples of poor CDD standards and lack of beneficial ownership details being obtained.

A formal warning notice was issued to the directors of the company informing them that the regulator found their conduct to be unsatisfactory and future action could be taken against them if the situation did not improve. A Direction was also issued for the appointment of an external compliance resource (pre-approved by the regulator) and paid for by the CSP.

At the present time the IM regulator will not issue a TSP licence to the entity and has informed those involved that consideration was being given to starting action on any one, or combination, of the following; -

a. to take from them their CSP licence;

b. to formally refuse their application for a TSP licence;

c. to start legal proceedings against the company for breach of the IM's AML/CFT legislation, especially with regard to their lack of identification of beneficial ownership when taking on previous business;

d. to take disqualification action against the company officials for failing to undertake their statutory duties, such as complying with the AML/CFT requirements.

As a direct result of regulatory intervention, the people running the business are now actively working to sell the CSP and the situation is being closely monitored by the Regulator.

Source: submitted by the IM

Case No. 18: Vulnerability arising from lack of AML/CFT oversight

This case occurred in 2002, when one of the directors of a trust company business operating in Country X was approached to set up a discretionary trust by a solicitor in Country Y. The solicitor advised that one of his clients, Mr. A, was acting on behalf of another individual, Mr. B. Mr. A had received monies from the sale of sauna business, which was owned by Mr. B. The solicitor wished to hold the sale proceeds through an offshore trust. The solicitor sent through documents to identify Mr. A, but none in relation to the ultimate client Mr. B. A few days later, over $850,000 was sent from the solicitor's account to the trust company's client account. Two days later, the solicitor requested the trust company to pay the bulk of those monies to four named entities, none of which had any connection to the trust and which were unknown to the trust company. The trust was established with Mr. A as the sole beneficiary. On the next working day, the trust company made the four payments as requested.

The High Court of Country X found both the trust company and the director of the trust company guilty of failing to comply with client identification requirements of the anti-money laundering law, a decision which was

upheld by the Court of Appeal. The Court of Appeal found that an isolated failure to comply with client identification procedures in the context of financial services business can amount to a criminal offence and that a systemic failure is not required. It was held that Client identification procedures prescribed by the anti-money laundering law must be kept up and that a single breach, provided that it was more than a mere oversight, is sufficient to constitute an offence.

Submitted by JE

CHAPTER 4: KEY FINDINGS

128. The types of entities that operate as Trust and Corporate Service Providers and the depth and nature of supervision to which they are subject, vary from jurisdiction to jurisdiction. Notwithstanding the fact that some jurisdictions do not recognise TCSPs as a formal sector or indeed that the laws of some jurisdictions do not recognise certain types of legal structures, such as trusts, these factors do not preclude the existence of TCSPs or the provision of these services in some way in these jurisdictions. The variance in supervision and the breadth of technical/complex services available from this sector are matters that feed into the money laundering vulnerabilities to which TCSPs are subject.

129. In addition, a review of money laundering cases illustrated how the services offered by TCSPs had been used in obscuring illegal activities in both the regulated and unregulated environments. Other cases highlighted that persons holding positions of trust and/or authority had themselves knowingly assisted in perpetrating money laundering crimes. The following are the key findings from a review of the questionnaire responses and an analysis of the various cases studies.

4.1 Description of Money Laundering Vulnerabilities/Observations

130. Though some jurisdictions do not recognise trusts in their laws, nevertheless case studies show that persons providing the services of a TCSP are able to provide trust vehicles to clients using the laws of other countries to do so. This can make it difficult for the authorities in the TCSP's home country to provide oversight for a legal structure established under foreign law. Additionally, the foreign country under whose laws the trust is established may have lacunae in their laws which allows the foreign TCSP to avoid oversight or supervision for the trusts established in that country. This type of lacuna is a vulnerability that criminals/money launderers capitalise on.

131. Pre-constituted companies are companies that TCSPs incorporate and hold as assets for sale or transfer to clients. After the company is sold there may be no requirement for the information on the new owners to be collected and submitted to the authorities to update the information on the corporation. Jurisdictions that allow TCSPs or professional intermediaries to establish pre-constituted companies, without the need for the ownership structure of those companies to be updated after the company has been sold to clients, might provide a cover to criminals and other persons who wish to use corporate structures to obscure beneficial ownership and thereby hide assets.

132. As the creation of complex structures can often generate higher fees for TCSPs, this can make such structures more attractive to TCSPs thereby potentially reducing their ability to associate an increased use of complex structures with a higher money laundering risk. TCSPs may not have a sufficiently robust risk framework in place that mitigates against the increased risk that may be posed by more sophisticated schemes. The provision of value-added services to a client base by TCSPs may also expose them to regulatory and reputational risks where a client has been found to be carrying out ML/FT.

133. TCSPs operating in highly competitive environments, both regulated and unregulated, may also experience additional challenges in obtaining adequate CDD, where there may be no minimum standard that has been clearly communicated or otherwise established that is in keeping with the FATF Recommendations, particularly Recommendation 5. Further, given the potential in some cases

for "flight to quality" of service providers, in order to attract business, certain TCSPs may operate on CDD requirements that would not be adequate under the FATF Recommendation 5.

134. Vulnerabilities of Regulated Regime – The regulated environment does not guarantee the absence of ML/FT activities. In the face of regulation and more consistent application of AML/CFT measures, the ML/FT activities tend to become more sophisticated and complex. As such, the emerging trends of movement from known ML/FT typologies may not be readily detected and discernable by TCSP. This is so because:

- More sophisticated vehicles are being established through TCSPs and ultimately used to perpetrate ML/FT activities;
- TCSP employees may knowingly assist the concealment of ML/FT activities, which may ultimately be more difficult to detect in light of the knowledge of employees; and/or
- Sanctioning powers on rogue individuals within TCSPs may be limited or difficult to apply.

135. **Vulnerabilities of an Unregulated Regime** – Within an unregulated environment, the risk of TCSPs not adequately applying the relevant FATF Recommendations to their operations and client base is greater than that of the regulated environment. Additionally, TCSP practitioners, who have not been subjected to fit and proper testing, may be uneducated about the ML/FT risks and the known typologies for the misuse of corporate vehicles. As such, their operating policies and procedures may be deficient in this regard. Therefore, some of the vulnerabilities include:

- Unknown and/or inconsistent application of the FATF 40 + 9 Recommendations to client base, and in particular Recommendations 5, 6, 8 & 11;
- Little market restriction on practitioners – lack of fit and proper assessment to ensure practitioners have adequate skills, competence and integrity;
- Inconsistent record keeping across practitioners may hamper investigations that do arise;
- TCSPs operating in an unlicensed environment appear to be more susceptible to being misused by money launderers, which may be indicative of the need for appropriate training, as well as the review and/or implementation of robust procedures;
- TCSPs may also rely on other financial institutions to carry out CDD on clients, which have been sourced through related or unrelated financial institutions; and
- Limited dialogue between competent authorities and TCSPs as well as amongst TCSPs from varied backgrounds.

136. Within unregulated environments, nuances in legislation from jurisdiction to jurisdiction can serve to assist in the obscuring of beneficial ownership information. This will be further compounded by the use of unrestricted/mobile bearer shares[74] within the ownership structures of corporate vehicles thereby opening them up to misuse for ML/FT.

---

[74] It is acknowledged that aside from the use of bearer shares, concealing beneficial ownership is also possible with other forms of shares *e.g.*, where nominal shares are used and documents are falsified by a nominee.

137. **Vulnerabilities of Direct Incorporation / Central Registry** - the following vulnerabilities were identified:

- Registry may be under-resourced to perform supervisory functions in the absence of a regulated environment;
- Registry does not conduct CDD and EDD where applicable, or verify the accuracy and completeness of data; and.
- CDD information may become outdated and incorrect, which may also impede investigations where the need arises.

4.2 Other Findings

138. Some of the respondents to the questionnaire believe that proper regulation and/or supervision of TCSPs by jurisdictions according to the FATF standards related to regulation and supervision in Recommendation 23 would provide a better safeguard against money laundering risks.

139. There was insufficient information available from responses to the questionnaire, in relation to jurisdictions that operate a central registry system, on their capacity to verify beneficial ownership and other information, provided to the registry by TCSPs or other persons, on corporate structures established within the jurisdiction. Therefore it is difficult to determine the effectiveness of central registry systems.

140. The questionnaire also highlighted the varied positions amongst jurisdictions on who/what is a TCSP. Some jurisdictions went wider in scope than the FATF definition required, while others applied a more restrictive definition. Therefore, for broad analytical purposes, this could make it difficult to evaluate the application of the FATF Recommendations, whether by competent authorities, examiners or self regulating organisations, and the assessment of whether or otherwise there are appropriate measures in place.

4.3 Money Laundering Indicators

141. The following are money laundering indicators that can be gleaned from the responses to the questionnaire and the case studies provided:-

- Transactions that require the use of complex and opaque legal entities and arrangements;
- The payment of “consultancy fees” to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies;
- The transfer of funds in the form of “loans” to individuals from trusts and non-bank shell companies. These non-traditional “loans” then facilitate a system of regular transfers to these corporate vehicles from the “borrowing” individuals in the form of “loan repayments”;
- Cases of corruption where the company paying the bribe to secure a contract or the person brokering a contract will seek to secure a successful outcome by utilising a TCSP to operate a trust with the funds held on deposit for the benefit of the person approving the contract;

- The use of TCSPs in jurisdictions that do not require TCSPs to capture, retain or submit to competent authorities information on the beneficial ownership of corporate structures formed by them;

- The use of legal persons and legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs;

- The use of legal persons or legal arrangements that operate in jurisdictions with secrecy laws;

- The use by prospective clients of nominee agreements to hide from the TCSP the beneficial ownership of client companies;

- The carrying out of multiple intercompany loan transactions and/or multijurisdictional wire transfers that have no apparent legal or commercial purpose;

- Clients who require the use of pre-constituted shell companies in jurisdictions that allow their use but do not require updating of ownership information; and

- TCSPs that market themselves and/or their jurisdictions as facilitating anonymity and disguised asset ownership.

CHAPTER 5: CONCLUSIONS

142. This section details significant conclusions arising from the responses to the questionnaire and the analysis of the cases presented.

143. TCSPs vary from jurisdiction to jurisdiction in the types of persons and entities that make up the sector; the definition and scope of services provided; as well as in the nature and effectiveness of regulation and supervision by the competent authorities. This variation in the industry on an international level poses difficulties for appropriately managing the AML/CFT risk that this sector faces, particularly since in many jurisdictions the services offered by TCSPs have an international component.

144. Although TCSPs may play marginally important roles in some larger jurisdictions, they do play a significant role in the economies of many smaller jurisdictions where the financial services industry is a key source of income. In these jurisdictions TCSPs are significant in that they introduce international business to the jurisdiction and facilitate a smoother journey into and through these business relationships.

145. The Questionnaire responses indicate that in jurisdictions that operate unregulated regimes for their TCSP sectors, there is inconsistent application of the FATF 40+9 requirements. Also, in the jurisdictions that do regulate, there are sometimes variations in the approach to regulation, as some jurisdictions fully regulate the entire sector while others do it on a partial basis.

146. For the most part, the information that TCSPs should be required to capture in accordance with the FATF Recommendations, appears to be adequate to assist in AML/CFT efforts. However, more guidance is necessary to clarify the meaning and scope of 'beneficial ownership'; and to specify the categories of persons on whom information is needed in relation to legal persons such as foundations or legal arrangements.

147. Although considerable work has already been done by the FATF to include TCSPs in the AML/CFT framework requirements, the current recommendations and guidance by the FATF need to more effectively address the risks associated with this sector and to comprehend the role of TCSPs in AML/CFT efforts. In this regard, the TCSP sector may benefit from the application of certain specific recommendations that already apply to the financial sector. For instance, the fit and proper requirements and the rules relating to branches and subsidiaries would be greatly beneficial to ensuring that jurisdictions are able to effectively combat money laundering and terrorist financing through this sector.

148. Given the disparity in the nature of the TCSP sectors and their supervision in various jurisdictions, many stakeholders in this industry support the development of sector-specific international standards for TCSPs, whether formulated through the FATF or through an international body established primarily to focus on this sector. Creating or implementing international standards for TCSPs will provide clarity to countries/jurisdictions and ultimately strengthen the application of the FATF Recommendations. The work of the OGBS in developing a Statement of Best Practices for this sector, although not having achieved the status of recognised international standard, is an important step in this direction. To promote consistency in the regulation of TCSPs internationally, most jurisdictions that operate fully licensed and regulated TCSP regimes recommend that such an international body should establish minimum standards for the regulation of TCSPs and should act as

a forum to encourage dialogue between regulators and to facilitate the establishment of new regulatory agencies in jurisdictions that currently do not regulate.

149. Supervision of TCSPs, whether on a prudential level or only for AML/CFT purposes, will be greatly enhanced with the implementation of supervisory requirements that oblige TCSPs, to establish separate legal identity from other companies within their corporate group; and require them to ensure that the mind and management of the TCSP is also separate and/or has appropriate degrees of autonomy and independence.

150. Additionally, supervision of TCSPs should of necessity include the implementation of 'fit and proper' requirements in relation to the mind and management of TCSPs. This will increase the likelihood of sound business management; adherence to regulatory requirements; and appropriate implementation of AML/CFT measures including more rigorous and discerning measures to vet clients. It should also decrease the likelihood of mindless conformity to improper policies/instructions laid down by parent companies or clients.

151. Although the responses to the questionnaire, the case studies and the literature review do not readily suggest that the TCSP sector lends itself to terrorist financing, it remains a serious risk given the fact that the methods used for money laundering and terrorist financing can be similar. In particular, there is a potential vulnerability in the use of opaque corporate structures and/or charities, combined with the transfer of value via TCSPs. In addition, the FATF Special Recommendations relating to terrorist financing are newer than those for money laundering, and thus further trends may become apparent as suspicious transaction reporting regimes mature.

CHAPTER 6: ISSUES FOR CONSIDERATION

152. This report has highlighted the vulnerabilities inherent in the TCSP sector and the policy considerations outlined below suggest that additional work may need to be done by the FATF and other stakeholders to address the issues raised there.

6.1 Policy Considerations

153. The findings show that TCSPs internationally play a central role in the formation and administration of trusts and corporations. When trust and corporate vehicles are misused for money laundering, there will almost always be a connection to a TCSP that was either knowingly or otherwise involved in the establishment or administration of the misused trust or corporate vehicle. Steps taken to require that those engaged in the provision of trust and corporate services meet appropriate fit and proper standards could reduce the money laundering risk. It may be useful therefore, to consider establishing minimum standards to restrict persons from operating as TCSPs unless they are properly qualified professionals; and having provisions that might permit monitoring of their activities and ensure their compliance with international standards. In the light of this, the project team has identified the following policy implications that flow from the analysis of the questionnaire responses and the case studies presented,

i. The FATF may wish to consider whether any gaps exist in Recommendations 12, 16 and 24 as they apply to TCSPs,

ii. The FATF may wish to consider whether the Recommendations relating to TCSPs should be applied according to the nature of the activities in which a TCSP is engaged.

iii. Trust service providers hold and manage assets, and are engaged in financial transactions in respect of the trusts they form and/or administer. The FATF may wish to consider whether such providers should still be classified as DNFBPs.

iv. While in some jurisdictions trust service providers are also corporate service providers, the research shows that several jurisdictions do distinguish between trust service providers and corporate service providers. Within the broad scope of the services that can be provided by corporate service providers, it may be beneficial to consider whether there should be a differentiation between:

   a. Corporate Service Providers that provide management and administration services, particularly when they fulfil a fiduciary responsibility. It might be appropriate to consider making these CSPs subject to additional requirements above those specified in Recommendations 12 and 16; such as Recommendations 22 and 23. Recommendation 23 dealing with fitness and propriety may be especially important to safeguard this class of CSPs from being involved in, or misused for money laundering and other criminal purposes; and

b. Corporate Service Providers that provide only basic incorporation services.[75] It might be appropriate to consider making this category of CSPs subject only to the minimum requirements currently in place for DNFBPs. However, it follows that jurisdictions might then need to have some means of determining whether this class of CSP goes outside this narrow scope of business; and of ensuring that, if they do begin to provide a wider range of services, the more rigorous controls are applied to them.

v. Consideration could be given to imposing a requirement, specific to TCSPs, in respect of the establishment of policies and procedures relative to the segregation of clients' assets and liabilities from the assets and liabilities of the TCSP; as well as the safe custody of clients' assets. These policies and procedures may address at least a description of the control of and the full physical separation between the assets of every client, every third party and the TCSP.

vi. Jurisdictions that elect to implement central registry systems should consider the inclusion of effective mechanisms to ensure that beneficial ownership information is kept up to date, and at the point of incorporation/registration, that appropriate CDD is carried out. It could also be important that the onus of these key and ongoing responsibilities be made clear to the responsible person(s); and that adequate and dissuasive sanctions be available and applied to persons who fail to carry out these requirements. However, if this enforcement function is carried out by the Registry itself rather than by another appropriate body, this would move the Registry's mandate more towards that of a supervisory authority, rather than the repository function of most central registries.

vii. As part of the on-going FATF work to look at the AML/CFT standards , the FATF may wish to consider whether Intermediaries/TCSPs should be required to maintain within the jurisdiction current information on beneficial ownership/control pertaining to all legal persons and legal arrangements established or administered by them, except as allowed for under Recommendation 9. It follows that any requirement of this nature would need to be supported by compulsory or punitive measures available to competent authorities to ensure compliance.

6.2 Areas for Further Work

154. In addition to the policy considerations outlined above, the following describe other important areas for possible further research or deliberation.

i. Assessing the national and international cooperation issues ensuring and/or enhancing access to and exchange of information on beneficial owners, was included as a key issue to be addressed within the scope of this report. However, there was insufficient information gathered to form the basis of any substantive analysis of this issue. Nevertheless, this is a matter on which the FATF is now focussing its attention.

ii. A further definition of beneficial owner as it relates to legal entities, such as foundations, and legal arrangements such as trusts, may need to be contemplated. It is recognised that this is one of the issues that the FATF is currently examining through its work in reviewing Recommendations 5, 33 and 34.

---

[75] This is where no value-added services are provided over and above the incorporation service.

iii. Consideration and appropriate research in determining the value of assets administered by and flowing through TCSPs (similar to the statistical data that is maintained for banks, mutual funds, and insurance brokers of the assets managed, premiums underwritten, etc.) may provide a basis upon which to review the level of risk and incentive for fraud, ML and TF being conducted through corporate vehicles.

iv. It may be useful to evaluate the efficacy of extending FATF Recommendation 22, on branches and subsidiaries, to the TCSP sector.

v. Consideration may be given to the development of further guidance in the FATF Methodology on legal professional privilege vis-à-vis the filing of SARs. A study by the FATF on the conflict between legal professional privilege in both common law and civil law jurisdictions may lend clarity to this area and facilitate the development of guidance in this area.

vi. There is a need for a more detailed consideration on whether or not it may be useful to have an international body to provide oversight for the TCSP sector. If this is considered appropriate, then a determination of the scope of the remit of such a body would be necessary to bring uniformity to both the operation of the sector and the supervision of the sector for prudential and AML/CFT purposes.

vii. Consideration could be given, under the anti-corruption framework, to the issue of the abuse of corporate vehicles and legal arrangements in concealing the proceeds of corruption. This is another area included within the current work agenda of the FATF.

viii. The FATF has developed specific requirements regarding the administration of trust services and cooperation between competent authorities that are applicable to all jurisdictions including those countries that do not have any trust laws. It is therefore important that all jurisdictions, including those that do not have any trust laws, effectively implement these requirements. Consideration might be given to whether there is a need for the development of a mechanism to enable or require jurisdictions to determine whether trust services are in fact being provided by persons or entities within their jurisdiction.

ix. Consideration should be given to what more needs to be done to enhance the effectiveness of company registers and other publicly available information sources such as the Stock Exchange. Consideration should be given to determining whether such bodies should be given additional responsibilities in relation to verification of the information provided to them. This is another area included in the current work of the FATF.

x. Consideration should be given to determining whether there is any practical action that needs to be or can be taken to enhance the information that is publicly available in respect of legal arrangements. Again, this is an area included in the current work of the FATF.

xi. Consideration should be given to determining whether guidance in other forms should be produced, for example, risk assessment checklists, to help the competent authorities focus their risk-based approaches in relation to the different types of misuse of legal persons and legal arrangements. In the interim, countries are encouraged to consider the guidance documents issued by the FATF in 2008

and 2009 on the risk-based approach for legal professionals;[76] accountants;[77] and TCSPs.[78] Additionally, it should be noted that the FATF is in the process of developing further guidance to assist jurisdictions in conducting national ML/TF assessments, which is expected to include additional guidance on national risk assessment of certain types of financial institutions or activities. It is also looking at this issue from the point of view of the risk-based approach.

[76] FATF (2008a)

[77] *FATF* (2008b)

[78] FATF (2008c)

REFERENCES

APG/FATF (2007), *Anti-Corruption/AML/CFT Research Paper*, September 2007 (prepared for the FATF/APG Project Group on Corruption and Money Laundering by Dr. David Chaikin and Dr. Jason Sharman (7 September 2007) presented to the FATF and APG plenaries in 2007 and 2008 respectively), www.apgml.org/issues/docs/17/APG-FATF_Report_on_Anti-Corruption_AML.pdf

BakerPlatt (2008), *Anti-Money Laundering/Countering the Financing of Terrorism: Typologies from a Jersey Perspective*, October 2008 (Report prepared on behalf of the Law Officers, Joint Financial Crimes Unit and the Jersey Financial Services Commission) www.jerseyfsc.org/pdf/AMLCFT_Typologies_from_a_Jersey_Perspective_28_Oct_08.pdf

Basil Committee on Banking Supervision (2001), *Customer due diligence for banks*, www.bis.org/publ/bcbs85.htm

FATF (2006), *The Misuse of Corporate Vehicles, including Trust and Company Service Providers*, FATF Paris, www.fatf-gafi.org/dataoecd/30/46/37627377.pdf

FATF (2008a), *RBA Guidance for Legal Professionals*, FATF, Paris, www.fatf-gafi.org/dataoecd/5/58/41584211.pdf

FATF (2008b), *RBA Guidance for Accountants*, FATF, Paris, www.fatf-gafi.org/dataoecd/19/40/41091859.pdf

FATF (2008c); FATF, *RBA Guidance for Trusts, Companies and Service Providers*, FATF, Paris www.fatf-gafi.org/dataoecd/19/44/41092947.pdf

OECD (2001), *Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes*, OECD, Paris, www.oecd.org/document/19/0,3343,en_2649_34795_43731027_1_1_1_1,00.html

OGBS (2002), *Trust and Company Service Providers – Statement of Best Practices*, 2002, Offshore Group on Banking Supervisors Trust and Company Service Providers Working Group, www.ogbs.net/attachments/037_Trust%20and%20Company%20Service%20Providers%20-%20Statement%20of%20Best%20Practice%20.pdf

OGBS (2004), *Securing Effective Exchange of Information and Supervision in respect of Trust and Company Service Providers*, Offshore Group on Banking Supervisors Trust and Company Service Providers Working Group, www.ogbs.net/attachments/036_ogbstrustandcos.pdf

Permanent Subcommittee on Investigations of the Committee on Governmental Affairs – US Senate, *"Role of US Correspondent Banking in International Money Laundering"*, (Hearings March 1, 2, and 6) 2001 – [Containing: *"Correspondent Banking: A Gateway for Money Laundering – A Report by Minority Staff of the Permanent Subcommittee on Investigations"*, February 2001] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_senate_hearings&docid=f:71166.pdf

Sharman, Dr. Jason C. (2008), *Shopping for Anonymous Shell Companies: An Audit Study of Anonymity and Crime in the International Financial System*, Journal of Economic Perspectives, 24(4): 127–40, www.aeaweb.org/articles.php?doi=10.1257/jep.24.4.127

The Egmont Group (2006), *FIU's in Action – 100 cases from the Egmont Group*, www.egmontgroup.org/library/download/21

JURISDICTIONS THAT RESPONDED TO THE QUESTIONNAIRE

CFATF Members	FATF Members	Other Jurisdictions
• Anguilla	• Austria	• Bulgaria
• Bahamas	• Australia	• Estonia
• Bermuda	• Belgium	• Guernsey
• British Virgin Islands	• Canada	• Jersey
• Cayman Islands	• China	• Liechtenstein
• Dominican Republic	• Denmark	• Latvia
• Guatemala	• Hong Kong	• Macau
• Honduras	• Italy	• Nepal
• Netherlands Antilles**	• Japan	• Panama
• St. Lucia	• Netherlands	• Uruguay
• St. Vincent and the Grenadines	• Mexico	
• Turks and Caicos Islands	• Switzerland	
• Venezuela	• United Kingdom	
	• United States of America	

ALPHABETICAL LISTING OF COUNTRY ABBREVIATIONS

AI	Anguilla	**IM**	Isle of Man
AN	Netherlands Antilles**	**IT**	Italy
AT	Austria	**JE**	Jersey
AU	Australia	**JP**	Japan
BE	Belgium	**KY**	Cayman Islands
BG	Bulgaria	**LC**	St. Lucia
BM	Bermuda	**LI**	Liechtenstein
BS	the Bahamas	**LV**	Latvia
CA	Canada	**MO**	Macau
CH	Switzerland	**MX**	Mexico
CN	China	**NL**	the Netherlands
DK	Denmark	**NP**	Nepal
DO	Dominican Republic	**PA**	Panama
EE	Estonia	**TC**	Turks and Caicos Islands
ES	Spain	**US**	United States of America
GB	United Kingdom	**UY**	Uruguay
GG	Guernsey	**VE**	Venezuela
GT	Guatemala	**VC**	St. Vincent and the Grenadines
HK	Hong Kong	**VG**	British Virgin Islands
HN	Honduras		

** As of October 10, 2010 the Netherlands Antilles (comprising of Curaçao, Bonaire, St. Martin, St. Eustatius and Saba) has been dismantled and has therefore ceased to exist. This entails that besides the Netherlands and Aruba, Curaçao and the Dutch part of St. Martin have now become autonomous countries within the Dutch Kingdom, while Bonaire, St Eustatius and Saba have been integrated into the Netherlands as special municipalities. All five islands remain non-sovereign by mutual consent.

AN NEX I - TABLES

Table 1 – Services Provided by TCSPs in Respondent Jurisdictions

Type	Yes	Estimated total based in jurisdiction				No Estimates Provided
Acting as a formation agent of legal persons;	15 Jurisdictions	64 Anguilla 221 Bahamas 56 Bermuda 127 British Virgin Islands 278 Cayman Islands	100 Guernsey 19 St. Lucia 41 Turks and Caicos 209 United Kingdom[a] 995 United Kingdom 5000 United States			Canada Jersey St. Vincent and Grenadines Switzerland
Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;	16 Jurisdictions	64 Anguilla 221 Bahamas 56 Bermuda 127 British Virgin Islands 160 Cayman Islands 140 Guernsey 170 Netherlands	146 Netherland Antilles 19 St. Lucia 41 Turks and Caicos 207 United Kingdom[b] 964 United Kingdom			Canada Jersey St. Vincent and Grenadines Switzerland United States
Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements;	16 Jurisdictions	64 Anguilla 221 Bahamas 56 Bermuda 127 British Virgin Islands 278 Cayman Islands 140 Guernsey 170 Netherlands	146 Netherland Antilles 19 St. Lucia 41 Turks and Caicos 483 United Kingdom[c] 1420 United Kingdom			Canada Jersey St. Vincent and Grenadines Switzerland United States
Acting as (or arranging for another person to act as) a trustee of an express trust;	16 Jurisdictions	16 Anguilla 31 Bermuda 212 British Virgin Islands 160 Cayman Islands 33 Guatemala 120 Guernsey	19 St. Lucia 17 Turks and Caicos 140 United Kingdom[d] 336 United Kingdom			Canada Honduras Jersey St. Vincent and Grenadines Switzerland

Type	Yes	Estimated total based in jurisdiction		No Estimates Provided
Acting as (or arranging for another person to act as) a nominee shareholder for another person.	16 Jurisdictions	35 Anguilla 221 Bahamas 127 British Virgin Islands 271 Cayman Islands 140 Guernsey 20 Netherlands	19 St. Lucia 17 Turks and Caicos 207 United Kingdom[e] 964 United Kingdom	Canada Jersey St. Vincent and Grenadines Switzerland United States Bermuda - unknown

Table notes:

a. UK: 209 solely undertaking this (of acting as a formation agent of legal persons) activity as TCSP activity; 995 undertake this in addition to other activity

b. UK: 207 solely undertaking this (of acting as (or arranging for another person to act as) a director or secretary of a *company*, a partner of a partnership, or a similar position in relation to other legal persons) as TCSP activity; 964 undertake this in addition to other activity

c. UK: 483 solely undertaking this (of providing a registered office; business address or accommodation, correspondence or *administrative* address for a company, a partnership or any other legal person or arrangements) as TCSP activity; 1420 undertake this in addition to other activity

d. UK: 140 solely undertaking this (of acting as(or arranging for another person t act as) a trustee of an express trust) as TCSP *activity*; 336 undertake this in addition to other activity

e. UK: 207 solely undertaking this (of acting as (or arranging for another person to act as) a nominee shareholder for another person) as TCSP activity; 964 undertake this in addition to other activity

Table 2 – Jurisdictions requiring licensing for TCSPs

Questions 9 and 15 Table of Responses

Jurisdiction	TCSP required to be licensed	TCSP required to be registered	No. of TCSPs currently licensed	No. of TCSPs currently registered	Ongoing monitoring and supervision of TCSPs	Competent authority responsible for ongoing monitoring and supervision	Nature of ongoing monitoring and supervision
Anguilla	Yes	-	16	-	Yes	Anguilla Financial Services Commission	Prudential and AML/CFT • Onsite • Offsite • Review of annual submissions
Bahamas							
TSPs	Yes	-	283	-	Yes	Central Bank of the Bahamas	Prudential and AML/CFT
CSPs	Yes	-	211	-	Yes	Compliance Commission on behalf of the Inspector of Financial and Corporate Service Providers (FCSPs) (the Securities Commission)	AML/CFT • Onsite • Offsite • Training • Consultations
Bermuda							
TSPs	Yes	No	31	-	Yes	Bermuda Monetary Authority	Prudential and AML/CFT • Onsite • Offsite • Review of annual submissions
CSPs	No	No	N/a	N/a	No	N/a	N/a

Jurisdiction	TCSP required to be licensed	TCSP required to be registered	No. of TCSPs currently licensed	No. of TCSPs currently registered	Ongoing monitoring and supervision of TCSPs	Competent authority responsible for ongoing monitoring and supervision	Nature of ongoing monitoring and supervision
British Virgin Islands	Yes	-	239	-	Yes	Financial Services Committee	Prudential and AML/CFT • Onsite • Offsite Review of half year prudential return and biennial risk based questionnaire
Canada							
TSPs	Yes (Trust Co's)	-	81	-	Yes	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)[a]	Prudential and AML/CFT • Onsite • Offsite Review of compliance questionnaires
CSPs	No	N/a	N/a	N/a	Yes	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)[b]	AML/CFT • Onsite • Offsite Review of compliance questionnaires
Cayman Islands	Yes	-	278	-	Yes	Cayman Islands Monetary Authority	Prudential and AML/CFT • Onsite • Offsite Review of audited financial statements

Jurisdiction	TCSP required to be licensed	TCSP required to be registered	No. of TCSPs currently licensed	No. of TCSPs currently registered	Ongoing monitoring and supervision of TCSPs	Competent authority responsible for ongoing monitoring and supervision	Nature of ongoing monitoring and supervision
Guatemala*	Yes (financial institution – banks and financial companies - that serve as trustees)	-	33 (18 banks and 15 financial entities)	-	Yes	Superintendency of Banks (prudential supervision) Intendancy of Special Verification (AML/CFT supervision) Superintendency of Tax Administration (matters of tax control)	Prudential and AML/CFT
Guernsey	Yes	-	197	-	Yes	Guernsey Financial Services Commission	Prudential and AML/CFT • Onsite • Offsite Review of annual submissions
Honduras*	Yes (banks are the only entities able to act as 'trustees'. Banks require a license to operate)	-	17	-	Yes	National Banking and Insurance Commission	Prudential and AML/CFT • Onsite • Offsite
Jersey	Yes	-	182	-	Yes	Jersey Financial Services Commission	Prudential and AML/CFT • Onsite • Offsite Review of annual submissions

Jurisdiction	TCSP required to be licensed	TCSP required to be registered	No. of TCSPs currently licensed	No. of TCSPs currently registered	Ongoing monitoring and supervision of TCSPs	Competent authority responsible for ongoing monitoring and supervision	Nature of ongoing monitoring and supervision
Netherlands	Yes (only TCSPs who carry on Corporate Service Business are recognised)	-	170	-	Yes	Dutch Central Bank (De Nederlandsche Bank)	AML/CFT • Onsite • Offsite
Netherlands Antilles	Yes	-	146	-	Yes	Central Bank of the Netherlands Antilles (Bank Van de Nederlandse Antillen)	Prudential and AML/CFT • Onsite • Offsite • Review of submissions
Panama*	Yes	-	-	-	Yes	Superintendency of Banks of Panama	Prudential and AML/CFT
St. Lucia	Yes	-	20	-	Yes	Financial Sector Supervision Unit	Prudential and AML/CFT • Onsite • Offsite Review of financial statements
St. Vincent and Grenadines	Yes	-	24	-	Yes	International Financial Services Authority	Prudential and AML/CFT • Onsite • Offsite Review of annual submissions

Jurisdiction	TCSP required to be licensed	TCSP required to be registered	No. of TCSPs currently licensed	No. of TCSPs currently registered	Ongoing monitoring and supervision of TCSPs	Competent authority responsible for ongoing monitoring and supervision	Nature of ongoing monitoring and supervision
Switzerland	Yes	-	Not known	Not known	Yes	FINMA or a SRO (authorized and monitored by FINMA)	Prudential and AML/CFT • Onsite • Offsite • Audits
Turks and Caicos	Yes	-	58	-	Yes	Turks and Caicos Islands Financial Services Commission	Prudential and AML/CFT • Onsite • Offsite Review of statutorily required documents
United Kingdom	No	Yes	-	2197	Yes	HM Revenue and Customs (HMRC), Financial Services Authority or professional bodies (the relevant legal and accountancy bodies) named in Schedule 3 of Money Laundering Regulations 2007	AML/CFT only • Onsite • Offsite
United States							
TSPs[c]	Yes	-	-	-	-	National or Relevant competent authority for each State	Prudential and AML/CFT
CSPs	No	Yes-in two States[d]	-	1176 approx	Yes – in two States	Secretary of State for each State	Conduct of Business only • Onsite • Offsite Audits

Jurisdiction	TCSP required to be licensed	TCSP required to be registered	No. of TCSPs currently licensed	No. of TCSPs currently registered	Ongoing monitoring and supervision of TCSPs	Competent authority responsible for ongoing monitoring and supervision	Nature of ongoing monitoring and supervision
Venezuela*	Yes	-	-	-	Yes	Inspection Management of Superintendency of Banks and Other Financial Institutions	Prudential and AML/CFT Submission of required documents

Table notes:

* These jurisdictions indicate that only banks or financial institutions are permitted to provide trust services within the jurisdiction. Therefore these financial institutions are licensed under general banking laws and not specifically under separate trust legislation.

a. Trust Companies are regulated at both the federal and provincial level. Market conduct is regulated by the provinces, and federally incorporated trust and loan companies are regulated by the Office of the Superintendent of Financial Institutions (OFSI). FINTRAC conducts onsite compliance inspections for TCSPs. OFSI also conducts onsite inspections, as the primary regulator for trust companies, and shares with FINTRAC information related to AML/CFT compliance.

b. FINTRAC conducts AML/CFT ongoing monitoring and supervision for all reporting entities in Canada, including persons or business carrying out CSP functions.

c. Due to the definition of TCSP used in this report and the fact that in the US, trust companies are defined as 'financial institutions' the responses provided by the US do not generally address trust companies. Trust companies, which are licensed to provide a range of fiduciary services, are chartered at either the national of State level, and are included in the definition of "bank" for AML/CFT purposes and are generally subject to the same regulations.

d. Two States, Delaware and Wyoming, require company service providers having a minimum number of customers to register with the Secretary of State in their capacity as commercial registered agents. In addition, nine other states have adopted the Model Registered Agents Act, (MORAA) which provides incentives that encourage commercial agents to register with the State Filing Office / Secretary of State.

Table 3 – SARs filed by TCSPs

- Number of SARs filed for each year between 2006-2009
- Percentage of SARs filed by TCSPs for each year between 2006-2009 in relation to the total number o f SARs filed for the said period.

	Year									
	2009		2008		2007		2006		2006 - 2009	
Jurisdiction	No. of SARs filed	% of total no. of 2009 SARs filed by TCSPs	No. of SARs filed	% of total no. of 2008 SARs filed by TCSPs	No. of SARs filed	% of total no. of 2007 SARs filed by TCSPs	No. of SARs filed	% of total no. of 2006 SARs filed by TCSPs	No. of SARs filed	% of total no. of SARs 2006-2009 filed by TCSPs
Anguilla	6	8%	5	17%	1	17%	1	14%	13	14%
Bermuda	651 (10 filed by TCSPs)	1.5%	256 (27 filed by TCSPs)	10.5%	246 (34 filed by TCSPs)	13.8%	314 (26 filed by TCSPs)	8.2%	1385 (97 filed by TCSPs)	7%
British Virgin Islands	185	71.4%	153	71.9%	104	82.7%	102	84.3%	544	75.7%
Cayman Islands	58	18.1%	49	19.8%	44	20.1%	45	20.4%	196	19.5%
Guernsey	151	24%	112	22%	109	14%	87	16%	459	19%
Jersey	1854 (368 filed by TCSPs)	20%	1404 (328 filed by TCSPs)	23%	1517 (362 filed by TCSPs)	24%	1034 (216 filed by TCSPs)	21%	5809 (1274 filed by TCSPs)	22%
Honduras	506	0%	192	0%	121	0%	94	0%	913	0%
Hong Kong[a]	19 filed by TCSPs		16 filed by TCSPs		9 filed by TCSPs		11 filed by TCSPs		55 filed by TCSPs	
Mexico	52,958	0.14%	36,934	0.2%	38,400	0.2%	56,659	0.2%	184,951	0.2%
Netherlands	N/a	N/a	0	<0.01%	4	<0.01%	1	<0.01%	5	<0.01%
No. of Unusual Suspicious Transaction	N/a	N/a	4		3		5		12	

	Year									
	2009		2008		2007		2006		2006 - 2009	
Jurisdiction	No. of SARs filed	% of total no. of 2009 SARs filed by TCSPs	No. of SARs filed	% of total no. of 2008 SARs filed by TCSPs	No. of SARs filed	% of total no. of 2007 SARs filed by TCSPs	No. of SARs filed	% of total no. of 2006 SARs filed by TCSPs	No. of SARs filed	% of total no. of SARs 2006-2009 filed by TCSPs
Reports[c]										
Netherlands Antilles	55	0.28%	166	0.74%	46	0.29%	5	0.04%	272	-
Switzerland[d]	47	5.2%	47	5.5%	30	3.8%	46	7.5%	170	5.5%
Turks and Caicos	46 (16 filed by TCSPs)	34.8%	37 (23 filed by TCSPs)	61.2%	34 (12 filed by TCSPs)	35.3%	22 (4 filed by TCSPs)	18.2%	139	-
Venezuela	1	0.2%	1	0.08%	1	0.08%	2	0.07%	5	0.1%

Table notes:

a. No aggregate figures were provided by Hong Kong for SARs filed by all sectors for the relevant period.

b. Unusual Suspicious Transactions Reports: STR's in the Netherlands are different from STR's in other countries. Unusual financial transactions are first investigated by the FIU and then upgraded to Suspicious Transactions Reports (STRs).

c. No aggregated statistics exist for SAR covering all categories of financial intermediaries which provide TCS (legal professionals, fiduciaries and banks). In addition, it is not known what proportion of SAR attributed to lawyers/fiduciaries result exclusively from TCS activities as defined by the FATF. Having considered these limitations, the figures are the aggregated figures for the number of SARs attributed to the fiduciaries and legal professionals.

ANNEX II – ADDITIONAL CASES

Case A: Weak regulatory AML/CFT regime and bank secrecy laws

Banks A and B were offshore banks licensed and operating in a small island State. Bank A was part of a group of companies which also consisted of a trust company providing corporate management services. Bank B was owned by two International Business Corporations which in turn were owned by two individuals in the United States. Bank B was created on their behalf by the trust company for the sole purpose of facilitating the receipt of the proceeds from an 'advance fee-for-loan' fraud operated by the ultimate beneficial owners of Bank B. Bank B had a correspondent banking relationship with Bank A and relied on Bank A's correspondent banking relationships in the United States and elsewhere to facilitate the receipt of the fraud proceeds. Bank B was managed by a corporate service provider which was owned and operated by one of the senior officers in Bank A, and this service provider also managed Bank A's correspondent banking accounts, established IBCs and opened accounts for Bank A's clients as well as for the potential victims of the 'advance fee-for-loan' fraud. These victims were required to establish IBCs in that jurisdiction and to open bank accounts at Bank A to which the fraud proceeds would be sent. Bank A on the instructions of the victims' IBCs would then transfer those funds into Bank B's account. From there the funds were transferred into the IBC accounts of Bank B's owners. This entire scheme therefore took place within the Banking system of this Caribbean jurisdiction, which being subject to bank secrecy laws meant that the fraudster's activities were protected from disclosure to US or local authorities. In the approximately three years over which Bank B was in existence, the Bank was never subjected to any form of regulatory oversight by the competent authorities of the island State. Even though Bank A had a longer history of operation and was implicated in a vaster array of questionable activities and schemes, it too escaped scrutiny by banking regulators because during the entire period of its existence the jurisdiction in question had no policy of examinations for licensed offshore banks. During the relevant period only a nominal requirement was in place for the submission of audited financial statements, but the authorities were lax in policing even this minimal obligation. The fraudsters therefore targeted this jurisdiction as a likely receptacle for the funnelling of illicit proceeds and the pivotal point for commencing the laundering of those proceeds.

Source: Extrapolated from: Minority Staff of the Permanent Subcommittee on Investigations (US Senate)

Case B: Weak regulatory AML regime and unrestricted use of bearer shares

To launder the proceeds of a narcotics importing operation, a lawyer who worked on behalf of the organisation, established a web of offshore corporate entities. These entities were incorporated in Country C, where scrutiny of ownership, records, and finances was not strong and where bearer shares were permitted to be used indiscriminately. A local management company in Country D administered these companies, which were used to camouflage the movement of illicit funds, acquisition of assets, and financing criminal activities on behalf of the criminal organisation. The person at the helm of the narcotics importing organisation was the holder of 100% of the bearer share capital of these offshore entities.

*Source: extracted from website of Jersey Financial Services Commission**

* Found on the Jersey FSC website in **"Anti-Money Laundering/Countering the Financing of Terrorism Typologies from a Jersey perspective"** published on October 28, 2008 and produced by BakerPlatt on behalf of the Law Officers, Joint Financial Crimes Unit and the Jersey Financial Services Commission. The purpose of the publication was to raise awareness of typologies that are relevant to Jersey including the risks arising from the nature of the customer base and products associated with Jersey as an international finance centre. Both local and international cases were used. The cases included within this report with the annotation "Extracted from website of Jersey Financial Services Commission" are the international cases referenced in the October 2008 publication. The origins of the international cases within the publication are not noted therein.

Case C: Concealment of beneficial ownership through the use of shell companies

THE WHITE WHALE CASE – H, an employee of a lawyer's office, was the administrator for 300 companies established through the law office on behalf of its clients, many of whom were known to be involved in international criminal organisations. The majority of the companies were shell corporations established in an

American State, though some companies were incorporated in Spain for the purpose of being used in money laundering schemes based on the real estate market. The Spanish companies were usually owned by the shell corporations registered in the American State and these pre-constituted companies, would have been incorporated using the name of an agent, usually a lawyer. The documents of incorporation for such companies would remain inactive in the hands of the agent until the company was bought by a client, and at the moment of purchase the company would become effective. The board of these pre-constituted companies when first registered would comprise the agent and his associates, who would usually have no link with the real owners who subsequently purchased the shell company.

Source: extracted from 2006 FATF Typology Study – Submitted by Spain

Case D: CSP's role in trade based ML and the concealment of beneficial ownership through use of shell companies

In 2003, ICE received a foreign law enforcement request for information about two U.S. companies which were registered in Wyoming. The foreign law enforcement agency suspected that several shipments of canned seafood, allegedly shipped from the U.S. companies, had been imported into their country, and undervalued in order to evade their taxes and duties.

In response to this request, the ICE was asked to determine if the companies existed, and to obtain as much information as possible regarding their corporate officers, business locations, business activities, and corporate registrations documents.

Subsequent investigation by ICE revealed that both companies were "shell" companies, legally incorporated in the State of Wyoming. The addresses provided by both of the suspect companies on their import documents into the requesting foreign country provided only the address of the Wyoming incorporating agent. The Articles of Incorporation for the suspect U.S. companies were obtained and listed that it was managed by a foreign firm with an address on an island in the Far East. The Articles of Incorporation for the foreign firm had been signed by the Wyoming incorporation agent. The investigation located no records for any additional business addresses, phone listings, or officers located in the United States.

Because there is no requirement for the identification of beneficial ownership at the time of incorporation, the ICE investigation was unable to obtain the information that the foreign government had requested.

Source: submitted by the USA

Case E: Concealment of beneficial ownership through use of shell companies

ICE investigated a criminal organisation where the violators utilized shell corporations to defraud a foreign government out of more than $100,000,000. The foreign and domestic shell companies enabled them to engage in a "bid-rigging" scheme and then launder the fraudulently obtained proceeds. In this bid-rigging fraud scheme, the co-conspirators bribed members of the foreign government's new airport bid committee, in order to win a competitive construction bid. The U.S. targets of the investigation operated a construction company and architectural firm, which submitted a competitive bid for work in the construction of the airport. A Government Assessor in the victim foreign country believed the bid was too high and requested that the bid committee obtain a second bid. As a result, the targets of the investigation utilized a shell company to submit a second, much higher valued bid for the work. As a result of this much higher second bid, the contract was awarded to the targets of the investigation.

Once they had been paid by the foreign government, the organisation laundered the proceeds of the fraud by layering them through a series of shell companies in several countries, including the United States. It was only through handwritten notes kept by foreign bankers that ICE investigators were able to identify the true beneficiaries of the funds. Six of eight indicted individuals were found guilty of violating money laundering, and wire fraud statutes. As part of the sentence, the court ordered the payment of approximately $22 million in restitution.

Source: submitted by the USA

Case F: Criminal culpability of TCSPs as facilitator of ML

X was a chartered accountant and the sole principal of a financial services business trading as X & Co. He acquired companies, provided directors, formed trusts and acted as trustee. He was signatory to hundreds of bank accounts. X used these facilities as a tool kit to help foreign clients to cheat their fiscal authorities and

launder the proceeds of crime. The common theme was that he was willing deal with the assets of clients according to their instruction.

X laundered money in a variety of ways. He extracted money from foreign trading companies using false invoices drafted at the behest of clients, holding the sums received anonymously for his clients. He layered millions of pounds through his pooled accounts. He obtained and delivered cash from and to his clients. He lied about the beneficial ownership and purpose of his companies and the origin of property to the Jersey authorities and others.

A key aspect of his business was his trade in bank notes. He obtained cash from clients who wanted to get rid of it, crediting bank accounts held for them with equivalent sums sourced from different money in return. The actual cash was then delivered to other clients who wanted their income secretly returned to them in this fashion – bank notes which he personally delivered to them in the Country A. These dealings were hidden by the operation of a spider's web of bank accounts.

The result of these activities was that it was impossible to ascertain the origin and ownership of property without access to the records of X & Co. Even then the tracing exercise was extremely difficult, requiring years of analysis by investigative lawyers, police, and forensic accountants to unravel.

Source: extracted from website of Jersey Financial Services Commission[*]

* See note * of Case B, above.

Case G: Concealment of beneficial ownership through use of shell companies

The White Whale Case

In the money laundering scheme involved in this case, ultimate beneficial ownership was obscured through the use of pre-constituted shell companies, which had been incorporated using the name of an agent, usually a lawyer. The documents of incorporation for such companies would remain inactive in the hands of the agent until the company was bought by a client, and at the moment of purchase the company would become effective. The board of these pre-constituted companies when first registered would comprise the agent and his associates, who would usually have no link with the real owners who subsequently purchased the shell company. The immediate benefit of this to the new owners of such companies was that their involvement in the companies remained hidden. *(See Case No. 11 in the report for fuller details)*

Case H: Use of professional intermediaries to facilitate money laundering

There are various examples in the UK of gatekeepers (for example Solicitors, Accountants and Notaries, among others) being involved in setting up Trusts for criminals to launder funds. In one example, a drug dealer deposited the proceeds of his crime into an offshore Trust for laundering purposes and then used funds from the Trust to buy property and also take a loan (one of the powers of a Trust is the facility for it to provide a loan). The use of a Trust in this manner demonstrates a way in which funds can be disassociated from criminality. Investigation of this case suggested that a Solicitor was involved in the laundering process and his expertise used to administer the Trust.

Source: submitted by the United Kingdom

Case I: Use of professional intermediary to facilitate money laundering

Mr. A was in control of a corporation's financial affairs and abused this position of trust by defrauding the company. He authorised and instructed staff to make electronic funds transfers from the company to his bookmakers' accounts. He then instructed the bookmakers to direct excess funds and winnings from the account to his personal account or that of third parties. He also instructed bank officers to transfer funds from his accounts internationally. In order to layer and disguise the fraud, Mr. A instructed his lawyer to contact the beneficiary of these international transfers to return the payments via wire transfers into the lawyer's trust account. Approximately $340,000.00 was returned in one international transfer to the lawyer's trust account. The lawyer then transferred $270,000.00 to a church fund in an attempt to further hide the assets and was preparing to transfer the funds to an overseas account. To access these funds, Mr. A undertook structured withdrawals of $7,400.00 each within a nine day period.

Source: extracted from Egmont Case Studies

Case J: Professional intermediary marketing and providing services as ML facilitator

Mr. C was an accountant who started his own accounting and financial services business, company N, in Panama. He advertised his services primarily on the internet and through mass mailings. Company N provided a variety of services including the following:

- Formation of offshore entities to disguise ownership of assets;
- Passports and dual citizenship, mostly using new nominee names;
- Movement of cash and other assets offshore and back onshore using various methods;
- Issuance of debit cards for the purpose of anonymously repatriating and spending offshore funds;
- Use of correspondent bank accounts to skim profits off legitimate businesses and repatriate funds through the purchase of assets and use of debit cards;
- Anonymous trading of securities through accounts with two major brokerage houses;
- False invoicing/re-invoicing schemes to support fraudulent deductions on tax returns; and
- False investments losses, to disguise transfer of funds overseas.

Mr. C was identified pursuant to an Internal Revenue Service investigation of one of his clients for illegal importation and sale of goods. The targets of this investigation were using a re-invoicing scheme devised by Mr. C to illegally import these chemicals into the US for sale. Mr. C assisted the targets in the re-invoicing scheme by preparing the invoices, receiving the proceeds of the scheme and hiding the proceeds in a myriad of Panamanian corporations for later use by the targets.

Source: extracted from 2006 FATF Typology Study – Submitted by the USA

Case K: Use of professional intermediaries to facilitate money laundering

Bank Y-Trust reported that Mr. John Doe, Attorney-at-Law, contacted them requesting information to open a trust account for his client and was subsequently provided with the necessary information. Bank Y-Trust further reported that John Doe and his client, Mr. Z, visited the office of Bank Y-Trust and presented documents which aroused suspicion because the amount stated to commence the relationship was USD $20 billion. Bank Y-Trust was told that this amount was to be placed into two company accounts, namely 'Night' and 'Day'. Also, the funds were purported to be lodged in cheques at a Bank in a foreign country. Mr. Z indicated that his business partner was Mr. AA. Mr. Z promised to complete and return the due diligence documentation to Bank Y-Trust, which never materialised. Research conducted by Bank Y-Trust, via the internet, revealed that the Central Bank in a foreign country had advised of the counterfeiting of government bonds for and in the name of Mr. AA. The matter was reported to the FIU for analysis, which subsequently forwarded the matter to law enforcement authorities for further investigation.

Source: submitted by the Bahamas

Case L: Detection by TCSP of international boiler room scam

This case is concerned with Subjects A and B who tried to incorporate several International Business Companies in Anguilla at a local TCSP, Company Z via a St. Maarten based TCSP, Company Y. During the KYC process for Company Z, they realized that subjects A and B may have submitted a fraudulent document, namely a reference letter. This was reported to the authorities and further analysis and investigation revealed that subject A and B were owners of several companies which were being used to facilitate an international Boiler Room scam. Most of the victims of this scam were foreign based nationals. Intelligence was supplied to various jurisdictions and investigations have commenced in several. Thus far one Mutual Legal Assistance Letter has been received and the process has already been completed. Thus there will be some form of prosecution as it relates to Company Y which is based in another island jurisdiction as it relates to the matter. A Memorandum of Understanding has also been signed between the cooperating FIUs and any forfeiture made will be shared on a fifty-fifty (50/50) basis.

Source: submitted by Anguilla

Case M: Detection of illegal activities through FIU reporting

Company A was managed by Mr. OXO while company B was managed by Mr. RYA. Company A sold a property to Company B for a significant amount of money, the deposit for which and a large portion of the remaining price was paid in cash and the rest by cheque. The Notary who executed the transaction noticed these unusual large cash payments and made a disclosure to the FIU based on Article 10bis of Belgium's anti-money laundering law. Analysis revealed that:

- The notary deed showed that money for the cheque that was paid to the Notary was put on the account of company A by a cash deposit two days prior to the issue of the cheque.
- Information from the bank showed that company A's account as well as Mr. OXO's personal account were credited by substantial cash deposits, which, among other things, were used for reimbursing a mortgage loan and for cash withdrawals.
- Police sources revealed that both Messrs. OXO and RYA were subjects of a judicial inquiry into money laundering with regard to trafficking in narcotics. They were suspected of having invested their money for purchasing several properties in Belgium through their companies.

These factors together showed that the cash used for purchasing the property probably originated from trafficking in narcotics for which they were on record.

Source: submitted by Belgium

Case N: Investigation of suspicious activities and reporting to FIU

'ABC' was a company established for the provision of accounting, fiduciary and bank signatory services to others. In a regular review of its customers, 'ABC' found the bank accounts of two of its customers, who were the beneficial owners of a number of connected companies, having frequent large-amount deposits and transfers. Open source research was conducted by the TCSP that unveiled that the clients might be related to money laundering activities in three overseas jurisdictions. A report was subsequently filed with the Joint Financial Intelligence Unit and the matter was pursued both in Hong Kong and the concerned overseas jurisdictions.

Source: submitted by Hong Kong

Case O: Reporting of suspicious activities to the FIU and international cooperation between FIUs

Two individuals, A and B, visited a country in Europe where they used a company formation agent to establish a registered company to receive profits from their ownership of 300 fairgrounds sites around the world. The Agent, who also provided a company and account management service, was suspicious of the underlying story and made a disclosure to the national FIU. Huge sums of money were received into the account in a brief period and A and B gave instructions to the Agent for a large sum to be invested in a Unit trust. The account continued to receive large US transfers over 2 years and a large amount was transferred into the account of a Mrs. X., who had earlier that year visited the formation agent with an introduction from A and B.

Mrs. X's story was that she would be receiving this money for a large amount of soya beans which she would be supplying to A and B's fairgrounds and as such needed the agent's help to set up an account to receive these funds. The agent assisted her and then made a further disclosure to the FIU detailing the full transaction. When the large transfer to Mrs. X's account was made, a further disclosure to the FIU was again submitted by the agent.

As a result, the FIU's enquiries to their home country revealed that A and B were convicted drug traffickers and that Mrs. X was the wife of another convicted drug trafficker. Mrs. X later requested the Agent to transfer a huge sum to her personal account in her home country. When notified of this development by the Agent, law enforcement agents in both countries agreed that the transaction should be done to gain further intelligence. However when the money arrived in her account, the Customs agency in Mrs. X's country restrained the funds. These funds were ultimately confiscated after a judicial determination was made that they were drug proceeds. Efforts by Mrs. X to liquidate her remaining funds held by the Agent was also notified to law enforcement and prevented from taking place.

Source: extracted from Egmont Case Studies

Case P: Detection of fraud scheme and international cooperation

Bermuda Police received two suspicious activity reports, one from a bank and the other from a Corporate Service Provider, both in relation to a Country A individual, who was attempting to urgently establish a local business and open bank accounts. Unhappy with the results of due diligence, both the bank and the service provider simultaneously made the reports, indicating that the individual was trying to wire in excess of $1,000,000 into accounts in Bermuda the following day. Upon investigating, Bermuda Police discovered that fraudulent documents had been used to open the accounts and to start the business and therefore quickly arrested the individual. Search warrants conducted the following day in the individual's hotel room revealed evidence of serious fraud, which had been perpetrated in Country A and Country B; as well as documents that showed the route through Countries A, B and C of the laundered proceeds of that fraud. The end result was that the individual was charged and convicted in Bermuda for minor fraud offences and was repatriated to Country A to face criminal charges. The Bermuda Police provided significant evidence for the ensuing market manipulation trials in Country A that saw two persons convicted on numerous counts for a multi-million stock market dollar fraud scheme. They also provided significant evidence relating to the assets of the main perpetrators for later recovery.

Source: submitted by Bermuda

ANNEX III – QUESTIONNAIRE

LONG FORM QUESTIONNAIRE

FATF / CFATF TYPLOGIES PROJECT ON MONEY LAUNDERING AND FINANCING OF TERRORISM USING TRUST AND COMPANY SERVICE PROVIDERS (TCSP)

Dear Colleague

We are writing to seek your assistance in obtaining information for a typologies project on money laundering and financing of terrorism using trust and company service providers (TCSP; see note 1). As you are aware, this and related matters have been the subject of many discussions and debates at the highest levels in our countries and many jurisdictions are currently grappling with how best to address the challenges being faced in this regard.

This questionnaire has been compiled by a Working Group of FATF and CFATF members and the information will be used to create greater awareness and understanding of this important area and potentially assist in policy formulation regarding money laundering and terrorist financing issues that relate to TCSPs[79]. It is intended that a report on Money Laundering and Financing of Terrorism using Trust and Company Service Providers will be completed by the end of 2010.

Please complete all of the following questions as comprehensively as possible. However with regard to information on legislation, a summary of the relevant provisions and/or copies of appropriate sections is acceptable. In order to assist us in meeting key external deadlines we would urgently request that the information be provided to us on or before January 15, 2010.

Industry Feedback on the questions posed in Part G may also be solicited but we would request that such feedback be specifically identified.

Confidentiality: Please be assured that your submissions will remain confidential as the following conditions will be strictly adhered to:

a) The completed questionnaires will not be published; and

b) Jurisdiction specific information will only be included in the report if the permission of the relevant person in the jurisdiction is first obtained.

We certainly appreciate your contribution to this important work.

79 Please note that this is a typologies research project and not a standard setting project.

Part A: BACKGROUND INFORMATION

1. Jurisdiction

2. Contact Name and title (please give two names, if the first contact is regularly away from the office for long periods of time)

3. Contact details

E-mail address	
Telephone Number	
Fax Number	

Part B: DESCRIPTION OF TCSPs

4. Please provide the definition, if any, of TCSPs provided for under the legislation of your jurisdiction.

5. What is the estimated total number of TCSPs in your jurisdiction?

6. i) Of the total number of TCSPs in your jurisdiction, please indicate which of the following types of TCSPs are present. Please also rank each type of TCSP in terms of which is the most and least common type of TCSP present in your jurisdiction (with 1 being the most common and 6 being the least common).

	Type of TCSP	**Present (Yes/No)**	**Rank (1 = most common 6 = least common)**
1	TCSP which carries on Trust business only		
2	TCSP which carries on Corporate Services Business[80] only		

[80] Company Management Business

3	TCSP which carries on both Trust and Corporate Services Business		
4	TCSP businesses which are licensed as a financial institution (other than as a TCSP) or are subsidiaries or branches of financial institutions licensed either locally or in another jurisdiction (E.g. TCSP owned or controlled by banks, attorneys, investment, fund manager or insurance companies)		
5	TCSP businesses which are banks, subsidiaries or branches of TCSP businesses based in another jurisdiction (E.g. Country X TCSP which is a subsidiary of Country Y fiduciary)		
6	Other (please specify)		

ii) Which of the following TCSP services are conducted in your jurisdiction? Where applicable, please state the corresponding legislation (if any) and the estimated number of such TCSP services in the jurisdiction.

Type	**Yes/ No**	**Name of Applicable Legislation**	**Estimated total based in jurisdiction**
Acting as a formation agent of legal persons;			
Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;			
Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements;			
Acting as (or arranging for another person to act as) a trustee of an express trust;			
Acting as (or arranging for another person to act as) a nominee shareholder for another person.			

iii) What restrictions, if any, apply in your jurisdiction on persons carrying on TCSP business? Please provide further information.

Who can act in capacity of: **(Yes/No)**	**Corporations**	**Accountants**	**Lawyers**	**Others (please specify)**
TCSP: incorporating a company				
TCSP: providing company administration/corporate services business				
TCSP: acting as a Trustee				
TCSP: providing trust administration services/trust business				

7. i) Is it a requirement in your jurisdiction that a TCSP be used to incorporate a company or can a company be incorporated through direct central registration? Please provide information on the incorporation process.

ii) Please estimate the approximate proportion of legal persons (see note 2) formed in your jurisdiction by non-residents in relation to residents (the terms 'resident' and 'non-resident' as defined in your jurisdiction).

Is the answer to 7(i) above different for residents and non-residents?

PART C: OVERSIGHT OF TCSPs

Legislation

8. i) Are TCSPs subject to any AML/CFT legislation, or any other related legislation, in your jurisdiction?

If TCSPs are subject to any such legislation, including AML/CFT legislation, please provide information on this legislation. For example, the title of the legislation, the year it came into force and the relevant provisions of the legislation.

ii) Please provide information on the procedure and requirements that TCSPs must comply with pursuant to the relevant provisions of the legislation, including the AML/CFT legislation, in your jurisdiction.

iii) In your view are the activities of TCSPs effectively controlled by the application of AML legislation alone or should they be subject to ongoing regulatory /supervisory measures?

iv) Is there a Self Regulatory Organization involved in the oversight of TCSPs for the purposes of a) AML/CFT compliance or b) Prudential Supervision. If Yes have there been any difficulties with respect to the SRO exercising adequate oversight, monitoring and enforcement?

9. i) Are TCSPs required to be licensed/authorized (as part of a prudential or regulatory regime) in your jurisdiction? If so, how many are currently registered and how many of those registered are active? Please note that this question does not refer to the license that individual lawyers obtain from their respective Bar or Regulatory agency in order to practice.

TCSP License/Registration required?	Total currently registered	Total registrants active

ii) If TCSPs are required to be licensed/authorized please provide information on the relevant legislation.

iii) If TCSPs are required to be licensed/authorized please provide information on the licensing/authorization procedure and requirements.

10. What other risk mitigation measures are in place in your jurisdiction to limit the misuse of TCSPs?

11. i) Are trusts required to be registered in your jurisdiction? If so, how many are currently registered and how many of those registered are active?

Trusts License/Registration required?	Total currently registered	Total registrants active

ii) If trusts are required to be registered please provide the year in which this registration requirement commenced.

iii) If trusts are required to be registered in your jurisdiction, please provide details on the registration requirements.

12. If TCSPs in your jurisdiction are subject to AML/CFT legislation and/or are required to be licensed/authorized what has been the impact, if any, on the operation of TCSPs since these requirements were brought into force.

For example:

- Did the number of TCSPs operating increase or decrease or was there a change in the types of TCSPs operating?
- Have there been any cost and/or efficiency implications for TCSPs?
- Has there been any impact on the efficiency of TCSPs in combating money laundering and terrorist financing? For example:
  a. The number or significance of ML/FT investigations initiated as a result of unsolicited reports from TCSP.
  b. Opinion of law enforcement/prosecution authorities on the information and cooperation received from TCSP during an investigation.
  c. Evidence of criminals being discouraged from using TCSP
- Has there been any increase or decrease in the number of clients using TCSPs?

13. Are TCSPs subject to "fit and proper" requirements (see note 3) in your jurisdiction? If yes, please describe these requirements.

14. Are there any proposed amendments to the legislation affecting TCSPs in your jurisdiction? If yes, please provide further information on these proposed amendments and any ML/FT vulnerabilities that the amendments seek to reduce.

Ongoing Monitoring and Supervision

15. i) Are TCSPs subject to ongoing monitoring and supervision in your jurisdiction? If yes, please provide the name of the monitoring authority responsible for this monitoring and supervision.

ii) Please provide further details on the nature and requirements of the ongoing monitoring and supervision.

16. i) Are onsite inspections carried out in relation to TCSPs in your jurisdiction? If yes, please provide the name of the authority responsible for conducting the inspections.

ii) Please provide further details on the nature and requirements of the onsite inspections.

17. If the answer to question 16 (i) above is yes, how many onsite inspections have been carried out between 2006 - 2009?

Year	**Number of onsite inspections**	**Percentage of providers inspected**	**Percentage of market-share inspected** (in terms of number of companies/trusts covered or otherwise)
2009			
2008			
2007			
2006			

Penalties

18. i) Can any penalties and regulatory or other enforcement action be taken against TCPSs in your jurisdiction? If yes, please provide information on the circumstance that would result in any such penalties and regulatory or other enforcement action.

ii) If the answer to question 18 (i) above is yes, please indicate whether the following type of penalties are available:

Penalties	**Yes or No**	**Any additional comments (including enforcement authority)**
Criminal		
Civil		
Administrative (penalties and fines)		
Others (please specify)		

PART D: INFORMATION REQUIREMENTS FOR TCSPs

Beneficial Ownership

Company and Trust Formation

19. i) Is disclosure of beneficial ownership (see note 4) information required at the time of all company formations in your jurisdiction?

ii) Is disclosure of information on the settlors and beneficiaries (see note 5) of trusts required at the time of all trust formations in your jurisdiction?

iii) If yes, is 'beneficial ownership', 'settlors' and 'beneficiaries' defined in the relevant legislation? Please list the relevant legislation that a) defines beneficial ownership, settlors and beneficiaries, and b) requires the identification and collection of beneficial ownership information and information on settlors and beneficiaries.

iv) If disclosure of beneficial information and information on the settlors and beneficiaries is required at the time of company and trust formation, what (if any) are the requirements for providing the competent authorities with any changes to this information after formation?

General Requirements under AML Legislation

v) Are TCSPs required by AML legislation in your jurisdiction to request beneficial ownership information and information on the settlors and beneficiaries of trusts?

vi) If there is legislation requiring beneficial ownership information and information on the settlors and beneficiaries, has there been any impact on the investigations or prosecutions of the misuse of corporate entities in your jurisdiction since this legislation came into force?

vii) Are TCSPs required to obtain information on any of the following :

Information	Yes/No
Source of funds	
Nature of the business to be undertaken	
If yes to either of the above, are TCSPs required to keep the information up to date?	

viii) If disclosure of beneficial ownership information is required, please provide information on who has access to this information and the conditions of access. Where information is held by a TCSP and requested by a competent authority please indicate in your response:

(a) whether there are established procedures for obtaining this information and whether these procedures are established in legislation or rules or guidance;
(b) whether there are specific timeframes for the release of the information;
(c) whether legal proceedings are required to obtain the information;
(d) any limitations to access by the authority (confidentiality, consent of affected party etc); and
(e) the extent to which TCSPs have been unable to or uncooperative in providing the information.

ix) Are there any challenges or difficulties with access to this beneficial ownership? If yes please provide further details.

x) If disclosure of beneficial ownership information is required, do you think there are any changes that need to be made to the way that beneficial ownership information is kept in your jurisdiction, and why?

Bearer Shares

20. i) Are bearer shares (see note 6) explicitly prohibited or permitted in your jurisdiction, or is the law silent on the issue? If yes, please provide further information on whether bearer shares are known to exist and how bearer shares are dealt with in your jurisdiction.

ii) If bearer shares are permitted, what requirements are in place to address potential AML/CFT risks?

iii) Are there any proposed amendments to the legislation affecting bearer shares in your jurisdiction? If yes, please provide further information on these proposed amendments.

Co-operation/Sharing of Information

21. i) Are there any measures in place in your jurisdiction that provides for domestic and international co-operation regarding the exchange of information on beneficial ownership and control? If yes, please provide details on the relevant legislation and measures in place, for example the procedure for obtaining this information and any restrictions on access to this information.

ii) If the answer to question 21 (i) above is yes, have there been any challenges or difficulties experienced with the exchange of information on beneficial ownership?

PART E: MONEY LAUNDERING/TERRORIST FINANCING AND TCSPs

Suspicious Activity Reports (SARs)

22. i) Are TCSPs required to file SARs in your jurisdiction?

ii) If the answer to question 22 (i) above is yes, please indicate i) the number of SARs filed for each year between 2006-2009 and ii) the percentage of SARs filed by TCSPs for each year between 2006-2009 in relation to the total number of SARs filed for the said period.

Year	**Number of SARs filed**	**As a percentage of the total number of SARs filed**
2009		
2008		
2007		
2006		
Total SARS 2006 – 2009		

23. If SARs are required to be filed, what has been the typical subject area of the SARs filed?

24. (i) If a competent authority carries out investigations in relation to a SAR and/or requests information from a TCSP, what in your experience has been the average response time? If time requirements are specified in the legislation please provide these also.

(ii) If problems have been encountered with obtaining information from TCSPs relating to SARS or investigations please provide a general description of these problems.

Cases

25. Is there evidence in your jurisdiction, and beyond, of the misuse of TCSPs for money laundering and terrorist financing? If yes, please provide recent case studies.

    If there are any other cases involving more generic abuses of TCSPs to carry out other types of offences please also include.

Threats

26. What, in your view are the greatest vulnerabilities, to money laundering and financing of terrorism faced by TCSPs?

PART F: GENERAL ASSESSMENT OF OTHER AML/CFT REQUIREMENTS AND TCSPs

27. i) Please provide an assessment of the adequacy and role that TCSPs play in the detection, prevention and prosecution of money laundering and terrorist financing. Please provide any evidence, including any recent case studies from your jurisdiction, to support your assessment.

    ii) Please provide an assessment of the impact, if any, of AML/CFT legislation on the adequacy and role that TCSPs play in the detection, prevention and prosecution of money laundering and terrorist financing. Please provide any evidence, including any recent case studies from the jurisdiction, to support your assessment.

28. Please provide an assessment of the adequacy and role that the information (See note 7) required from TCSPs, in accordance with the FATF 40 Recommendations, plays in combating money laundering and terrorist financing?

29. i) Are there any difficulties experienced by TCSPs in obtaining the FATF required information from clients? If yes, please provide recent examples of such difficulties.

    ii) If there are difficulties experienced by TCSPs, what action in your view needs to be taken to overcome these difficulties?

30. In your view, do the FATF recommendations and guidance need to more effectively address the role of TCSPs in the efforts to combat money laundering and terrorist financing? If yes, please explain.

International Standards

31. In your view, is there a need for the establishment of an international organization (such as IAIS, IOSCO, Basel etc.) dedicated solely to TCSPs? If yes, please explain.

32. In your view, is there a need for an international standard for TCSPs to address issues such as the "fit and proper" prerequisite and other minimum requirements (E.g. Systems and Controls, Corporate Governance, Authorization criteria, Maintaining and Sharing Information)? If yes, please explain.

33. In your view, what steps would need to be taken to ensure effective implementation of any international requirements (please see question 32 above for details of these requirements)?

TCSP Project

December 2009

NOTES

1. **Trust and company service provider (TCSP):** This has the same meaning as in the glossary attached to the FATF Methodology[81] and refers to any person or business that provides any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

2. **Legal persons**: This has the same meaning as in the glossary of the FATF 40 Recommendations: "Bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property".

[81] FATF Methodology: www.fatf-gafi.org/dataoecd/16/54/40339628.pdf

3. As referred to in the interpretative note of Recommendation 23 of the FATF 40: http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236920_33988956_1_1_1_1,00.html#Interpretative_Note_to_r_23

4. **Beneficial Ownership:** This has the same meaning as in the glossary of the FATF 40 Recommendations: "the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement."

5. **Beneficiary**: This has the same meaning as in the glossary of the FATF 40 Recommendations: "All trusts (other than charitable or statutory permitted non-charitable trusts) must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period."

Settlors: This has the same meaning as in the glossary of the FATF 40 Recommendations: "Settlors are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets."

6. **Bearer Shares**: This has the same meaning as in the glossary of the FATF 40 Recommendations: "Bearer shares refer to negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate."

7. **The relevant provisions of the FATF 40 Recommendations:**

The relevant provisions of the FATF 40 Recommendations applicable to TCSPs are set out below.

Measures to be taken by Financial Institutions and Non-Financial Businesses and Professions (DNFBPs) (See note 8) to prevent Money Laundering and Terrorist Financing

Customer due diligence and record-keeping requirements
Recommendation 12
The customer due diligence and record-keeping requirements set out in Recommendations:

- 5 (CDD measures)
- 6 (Politically Exposed Persons)
- 8 (threats from new technologies and non face to face business)
- 9 (third party reliance)
- 10 (record-keeping)
- 11 (complex, unusual transactions)

apply to designated non-financial businesses and professions in the following situations:

…d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance
Recommendation 16
The requirements set out in Recommendations:

- 13 (report suspicious transactions)
- 14 (protection from any liability for reporting suspicious transactions)
- 15 (develop programmes against money laundering)
- 21 (special measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations)

apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
…c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).
Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Regulation and supervision
Recommendation 24
Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

…b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organization, provided that such an organization can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

8. <u>Designated Non-Financial Businesses and Professions:</u>
a. Casinos (which also includes internet casinos).
b. Real estate agents.

c. Dealers in precious metals.
d. Dealers in precious stones.
e. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person

SHORT FORM QUESTIONNAIRE

FATF / CFATF TYPLOGIES PROJECT ON MONEY LAUNDERING AND FINANCING OF TERRORISM USING TRUST AND COMPANY SERVICE PROVIDERS (TCSPS)

Dear Colleague

We are writing to seek your assistance in obtaining information for a typologies project on money laundering and financing of terrorism using trust and company service providers (TCSP; see note 1). As you are aware, this and related matters have been the subject of many discussions and debates at the highest levels in our countries and many jurisdictions are currently grappling with how best to address the challenges being faced in this regard.

This questionnaire has been compiled by a Working Group of FATF and CFATF members and the information will be used to create greater awareness and understanding of this important area and potentially assist in policy formulation regarding money laundering and terrorist financing issues that relate to TCSPs[82]. It is intended that a report on Money Laundering and Financing of Terrorism using Trust and Company Service Providers will be completed before the end of 2010.

Please complete all of the following questions as comprehensively as possible. In order to assist us in meeting key external deadlines we would urgently request that the information be provided to us on or before January 15, 2010.

Confidentiality: Please be assured that your submissions will remain confidential as the following conditions will be strictly adhered to:

c) The completed questionnaires will not be published; and

d) Specific information will only be included in the report if the permission of the relevant person from the participating organization is first obtained.

Part A: BACKGROUND INFORMATION

34. Jurisdiction/Organization

35. Contact Name and title (please give two names, if the first contact is regularly away from the office for long periods of time)

36. Contact details

E-mail address	
Telephone Number	
Fax Number	

82 Please note that this is a typologies research project and not a standard setting project.

Part B: DESCRIPTION OF TCSPs

37. Please provide the definition, if any, of TCSPs provided for by your jurisdiction/organization.

PART C: GENERAL ASSESSMENT OF OTHER AML/CFT REQUIREMENTS AND TCSPs

38. i) Please provide an assessment of the adequacy and role that TCSPs play in the detection, prevention and prosecution of money laundering and terrorist financing. Please provide any evidence, including any recent case studies from any jurisdiction, to support your assessment.

ii) Please provide an assessment of the impact, if any, of AML/CFT legislation on the adequacy and role that TCSPs play in the detection, prevention and prosecution of money laundering and terrorist financing. Please provide any evidence, including any recent case studies from any jurisdiction, to support your assessment.

39. Please provide an assessment of the adequacy and role that the information (See note 2) required from TCSPs, in accordance with the FATF 40 Recommendations, plays in combating money laundering and terrorist financing?

40. i) In your view, are there any difficulties experienced by TCSPs in obtaining the FATF required information from clients? If yes, please provide recent examples of such difficulties.

ii) If there are difficulties experienced by TCSPs, what action in your view needs to be taken to overcome these difficulties?

41. In your view, do the FATF recommendations and guidance need to more effectively address the role of TCSPs in the efforts to combat money laundering and terrorist financing? If yes, please explain.

International Standards

42. In your view, is there a need for the establishment of an international organization (such as IAIS, IOSCO, Basel etc.) dedicated solely to TCSPs? If yes, please explain.

43. In your view, is there a need for an international standard for TCSPs to address issues such as the "fit and proper" prerequisite and other minimum requirements (E.g. Systems and Controls, Corporate Governance, Authorization criteria, Maintaining and Sharing Information)? If yes, please explain.

44. In your view, what steps would need to be taken to ensure effective implementation of any international requirements (please see question 10 above for details of these requirements)?

TCSP Project

December 2009

NOTES

1. **Trust and company service provider (TCSP):** This has the same meaning as in the glossary attached to the FATF Methodology[83] and refers to any person or business that provides any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

2. **The relevant provisions of the FATF 40 Recommendations:**

The relevant provisions of the FATF 40 Recommendations[84] applicable to TCSPs are set out below.

Measures to be taken by Financial Institutions and Non-Financial Businesses and Professions (DNFBPs) (See note 3) to prevent Money Laundering and Terrorist Financing

Customer due diligence and record-keeping requirements
Recommendation 12
The customer due diligence and record-keeping requirements set out in Recommendations:

- 5 (CDD measures)
- 6 (Politically Exposed Persons)
- 8 (threats from new technologies and non face to face business)
- 9 (third party reliance)

---

83 FATF Methodology: www.fatf-gafi.org/dataoecd/16/54/40339628.pdf

84 FATF 40 Recommendations www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

- 10 (record-keeping)
- 11 (complex, unusual transactions)

apply to designated non-financial businesses and professions in the following situations:

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance

Recommendation 16
The requirements set out in Recommendations:

- 13 (report suspicious transactions)
- 14 (protection from any liability for reporting suspicious transactions)
- 15 (develop programmes against money laundering)
- 21 (special measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations)

apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
…c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).
Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Regulation and supervision

Recommendation 24
Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

…b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organization, provided that such an organization can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

3. Designated Non-Financial Businesses and Professions[85]:

a. Casinos (which also includes internet casinos).
b. Real estate agents.
c. Dealers in precious metals.
d. Dealers in precious stones.
e. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person

[85] FATF 40 Recommendations Glossary: www.fatf-gafi.org/glossary/0,3414,en_32250379_32236889_35433764_1_1_1_1,00.html

ANNEX IV – OGBS STATEMENT OF BEST PRACTICE

TRUST AND COMPANY SERVICE PROVIDERS STATEMENT OF BEST PRACTICE

Introduction

This statement of best practice has been prepared by a Trust and Company Service Providers Working Group set up by the Offshore Group of Banking Supervisors on which four G7 countries (France, Italy, Netherlands and United Kingdom) and three international organisations (FATF, IMF and OECD) were also represented. The terms of reference of the Working Group were –

"To produce a recommended statement of minimum standards/guidance for Trust and Company Service Providers; and to consider and make recommendations to the Offshore Group of Banking Supervisors for transmission to all relevant international organisations/authorities on how best to ensure that the recommended minimum standards/guidance are adopted as an international standard and implemented on a global basis".

The Working Group decided that a statement of best practice should be prepared rather than a statement of minimum standards. At the present time many jurisdictions do not regulate trust and company service providers, and in some cases such providers are not presently embraced by anti-money laundering legislation. Accordingly it is considered that a statement of best practice is more appropriate.

This statement of best practice is intended for use by jurisdictions generally in reviewing the position of their trust and company service providers. It is also intended for use by international organisations such as the IMF when they are engaged in an assessment of individual jurisdictions in respect of their policy/procedures/practices from a financial regulatory/anti-money laundering standpoint.

Trust and company service providers are important for financial regulation, anti-money laundering and combating the financing of terrorism as intermediaries both as introducers of business to other institutions and as entities responsible for handling and/or managing funds/assets. Their importance is recognised in the Financial Stability Forum's report on Offshore Financial Centres and the Financial Action Task Force consultation paper on the review of the forty recommendations.

This statement of best practice is intended to fill the gap that exists at the present time where trust and company service providers generally are not subject to standards set by bodies such as the Basel Committee on Banking Supervision and IOSCO. However, in those cases where such standards do apply nothing in this statement of best practice alters the existing obligations to comply with those standards.

There is a wide range of different types of business or professionals that act as professional service providers for the creation and administration of companies, trusts, foundations and other legal entities or arrangements, and offer related management and advisory services. What are known generically as trust and company service providers ("Service Providers" for the purpose of this statement) refer to those who carry on a business that involves the provision of company administration services or trustee or fiduciary services and in the course of doing so provide one or more of the following services:-

- acting as a company or partnership formation agent;
- acting as (or arranging for another person to act as) a director or secretary of a company or a partner of a partnership;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, partnership or for any other person;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.
- arranging the establishment of, or providing services in relation to, any legal entities not covered by the foregoing (e.g. a foundation or anstalt).

In the following statement, Section A addresses the requirements for Service Providers responsible for handling and managing client funds; Section B considers some broader structural issues; and Section C gives recognition to the possible need for a lighter touch where a Service Provider does not handle client funds.

A. <u>All countries/jurisdictions should require that where a Service Provider is responsible for handling/managing funds/assets</u> –

1. Those individuals holding key positions providing the service should be persons of integrity and should exhibit evidence of meeting the following requirements –

i) having no relevant adverse business/professional/personal history:

relevant considerations would include –

- professional or administrative reprimands;
- regulatory directions/public statements;
- disciplinary findings;
- civil fines;
- criminal convictions;
- declaration of bankruptcy;
- adverse personal credit rating

and would extend to a person's involvement as a director or senior manager/officer within a company that has been the subject of such considerations.

ii) having relevant and appropriate level of competence/capability:

relevant considerations would include –

- professional or other relevant qualifications;
- knowledge and/or experience relevant to the business concerned and appropriate to the employment status/role of the individuals concerned.

2. Those providing the service should exhibit evidence that their business will be or is being conducted in accordance with the following requirements under the headings of corporate governance, customer due diligence, conduct of client business, financial soundness, and systems and controls –

Corporate Governance

The Service Provider should be able to demonstrate that they are in –

i) compliance with recognised general standards of corporate governance in respect of both the business itself and each company, partnership, trust and other legal entity ("the client(s)");

ii) compliance with national regulations with respect to money laundering and the financing of terrorism;

iii) compliance with all relevant and applicable financial regulatory standards;

iv) compliance with all relevant and applicable domestic statutory requirements/obligations (e.g. companies law);

v) compliance with recognised standards in respect of directors/trustees responsibilities;

Customer Due Diligence

The Service Provider should be able to demonstrate that they are engaged in –

vi) effective customer due diligence - to satisfy the standards set out in the Basel Committee's Customer Due Diligence Paper, published in October, 2001, to the extent that the recommendations in that paper are relevant to non-banks.

This should include proper procedures for –

- customer identification;
- verification of identity of customer;
- risk profiling of customers (e.g. politically exposed persons);
- establishing the source of wealth;
- establishing the source of funds;
- ongoing monitoring of a customer's activities.
- adequate documentation to meet KYC requirements.

Specific issues on which attention should focus relate to information on the ultimate beneficial owner and/or controller of companies, partnerships and other legal entities, and the settlor/protector/beneficiaries of trusts, which should be known to the Service Provider and be adequately documented.

Conduct of Client Business

The Service Provider should be able to demonstrate that client business is being properly conducted through the –

vii) Identification and segregation of clients' assets and liabilities from the assets and liabilities of the Service Provider;

viii) effective handling of clients' assets covering –

- safe custody of assets;
- proper management of assets;

ix) maintaining adequate and orderly accounting records of clients affairs;

x) maintaining adequate client documentation (e.g. trust deeds);

xi) ensuring that all transactions/decisions entered into, taken by or on behalf of clients are appropriately authorised/handled by persons with an appropriate level of knowledge, experience and status properly to effect such transactions or make the proper decisions according to the nature and status of the transactions/decisions involved; for example –

- where discretion is exercised for or in relation to clients, all reasonable steps should be taken to obtain sufficient information in order to exercise that discretion or other powers in a proper manner and such discretion should only be exercised for a proper purpose;
- any actual or perceived conflict of interest should be avoided or appropriately disclosed; and where conflicts arise and cannot be resolved by disclosure and, internal rules of confidentiality, or rules on when or when not to act, the Service Provider should withdraw its services in an orderly manner;
- all business (including the establishing, transferring or closing of business relationships with its customers) should be transacted in an expeditious manner.

xii) ensuring that, where appropriate, there is a full understanding of the duties arising under the laws relevant to the administration and affairs of clients for which they are acting in the jurisdictions in which they are carrying on business and in which the assets being handled/managed are held.

Financial Soundness

The Service Provider should be able to demonstrate that it is financially sound by –

xiii) maintaining adequate and orderly accounting records of –

- the business of the Service Provider itself;
- the affairs of the clients.

xiv) maintaining adequate financial resources including –

- paid up capital; and/or
- liquid capital;

to enable the business to continue as a going concern and for the affairs of each client to be managed properly for an appropriate period in the event of a trading difficulty being experienced

xv) providing evidence of compliance with any relevant financial regulatory standards;

xvi) providing evidence of compliance with international accounting standards;

xvii) maintaining adequate professional indemnity insurance cover.

Systems and Procedures

The Service Provider should be able to demonstrate that the following systems, procedures and controls are adequately addressed –

xviii) effective compliance functions – where appropriate a skilled and experienced person should be designated as a compliance officer;

xix) effective reporting procedures and effective systems to submit timely and accurate information to the appropriate authorities – where appropriate a skilled and experienced person should be designated as a money laundering reporting officer;

xx) an effective complaints handling system including maintaining a record of complaints and the actions taken to resolve them;

xxi) maintaining at an appropriate location in the jurisdiction adequate, orderly and up to date records of all business transactions of the Service Provider and instructions received from clients,, including–

- the accounting records of the business;
- the accounting records of each client;
- records of the internal organisation and risk management systems;
- client documentation (e.g. client requirements, customer due diligence requirements);
- document retention policies appropriate to the business of the provider and in compliance with relevant legal obligations;

xxii) maintaining a manual of appropriate policies and procedures for the operation of the Service Provider's business and the provision of services to each client; including business acceptance procedures, and documented systems and procedures intended to safeguard the business and

the clients' and their assets and ensure that all authorised and proper transactions are undertaken;

xxiii) maintaining an adequate span of control with a sufficient number of appropriately skilled and experienced persons able to exercise independent judgement in relation to the running of the Service Provider's business;

xxiv) ensuring that those engaged in the business have appropriate relevant experience and qualifications;

[Note: exceptions to xxiii, xxiv may apply in respect of sole practitioners where, for example, an individual trustee function is controlled by the Court];

xxv) ensuring that continuous professional development requirements are satisfactorily met;

xxvi) maintaining effective procedures to ensure that no false or misleading information is provided (including advertisements).

3. There should be proper provision for holding, having access to and sharing of information, including ensuring that –

i) information on the ultimate beneficial owner and/or controllers of companies, partnerships and other legal entities, and the trustees, settlor, protector/beneficiaries of trusts is known to the service provider and is properly recorded;

ii) any change of client control/ownership is promptly monitored (e.g. in particular where a service provider is administering a corporate vehicle in the form of a "shelf" company or where bearer shares or nominee share holdings are involved);

iii) there is an adequate, effective and appropriate mechanism in place for information to be made available to all the relevant authorities (i.e. law enforcement authorities, regulatory bodies, FIU's);

iv) there should be no barrier to the appropriate flow of information to the authorities referred to in 3 (iii) above;

v) KYC and transactions information regarding the clients of the Service Provider is maintained in the jurisdiction in which the Service Provider is located;

vi) there should be no legal or administrative barrier to the flow of information/documentation necessary for the recipient of business from a Service Provider who is an acceptable introducer to satisfy itself that adequate customer due diligence has been undertaken in accordance with the arrangements set out in the Basel Customer Due Diligence paper;

B. All countries/jurisdictions should make proper provision to ensure that –

– the interests of customer/clients can be adequately safeguarded when the Service Provider is no longer able to carry on the business for any reason;

– external auditors with relevant experience and appropriate qualifications and track record are appointed to carry out a full audit of the Service Provider's business in accordance with international standards;

– external auditors have the statutory authority/protection to report to the competent authorities any breaches of relevant legislation or other material concerns;

– adequate provisions are in place to ensure that regular independent reviews are conducted of all Service Providers who carry on business in or from the country/jurisdiction to assess compliance with the statement of best practice; and that action can be taken where there is evidence of non-compliance;

– for the purposes of compliance with A.2.(ii) above, Service Providers are embraced by national anti-money laundering legislation;

C. Conclusions–

Service Providers in all countries/jurisdictions should be expected to comply with the statement of best practice. However it is recognised that where the Service Provider is not responsible for handling/managing funds/assets and carries on business which might be perceived as lower risk, a lighter touch may be applied, according to the nature and scope of the business activity.

Examples of "lower risk" business might include business which consists solely of one of the following –

- formation of companies, partnerships, and other legal entities;
- providing a registered office or business address for a company or partnership;
- providing for the formation/administration of local trading companies only and where the provider does not act as –
  - · a director or secretary;
  - · a trustee;
  - · a nominee shareholder

In the case of such business the lighter touch could be in respect of –

- the span of control covering the number of persons engaged in the business;
- the level of qualifications/experience of the persons engaged in the business;
- the capital/professional indemnity insurance requirements;

- the audit requirements.

With the exception of the foregoing such service providers, and any other service provider not covered by the above provisions, would be expected to comply with all the requirements set out in Section A.

6th September, 2002

FATF/OECD
December 2010

www.fatf-gafi.org

Appendix W:

FATF, *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* (Paris: FATF, 2006)

Financial Action Task Force

Groupe d'action financière

THE MISUSE OF CORPORATE VEHICLES, INCLUDING TRUST AND COMPANY SERVICE PROVIDERS

13 OCTOBER 2006

Executive Summary

Despite the important and legitimate roles corporate entities, including corporations, trusts, foundations and partnerships with limited liability, play in the global economy, they may, under certain conditions, be used for illicit purposes.

The present study's prime aim has been to seek to identify in respect of corporate vehicles areas of vulnerability for money laundering and terrorist financing, along with evidence of their misuse. Faced with the vast scope of a general project on corporate vehicle misuse the study focuses on what is considered to be the most significant feature of their misuse – the hiding of the true beneficial owner.

The study examined a series of cases as examples of the misuse of corporate vehicles from which certain key elements and patterns for this misuse are identified. The study also analyses the results of a survey conducted to obtain a better picture of the international diversity in the formation and administration of corporate vehicles.

Drawing on the typologies, as well as prior studies, a number of frequently occurring risk factors associated with corporate vehicle misuse are identified, which could be useful to countries in helping identify such misuse.

The information and typologies examined suggest a number of areas that may call for further and separate consideration in preventing corporate vehicles and their activities from misuse by criminals.

Table of Contents

Page

1. Introduction

Corporate entities, including corporations, trusts, foundations and partnerships with limited liability characteristics, conduct a wide variety of commercial activities and are the basis for a broad range of entrepreneurial activities in market-based economies. However, despite the important and legitimate roles these entities play in the global economy, they may, under certain conditions, be used for illicit purposes, including money laundering, bribery and corruption, improper insider dealings, tax fraud, financing of terrorist activities and other forms of illegal activities[1]. Criminals have responded to the money laundering defences put in place by banks and other financial institutions by misusing corporate vehicles, and those who provide trust and company services, to disguise and convert their proceeds of crime before it enters the traditional financial system.

Organised crime groups or individual criminals tend to seek out the services of professionals to benefit from their expertise in setting up schemes that the criminals then use for illicit purposes. Criminals may seek advice from trust and company service providers (TCSPs) as to the best corporate vehicles or jurisdictions to use to support their schemes, with the TCSPs having varying degrees of awareness of or involvement in the illicit purposes underlying their client's activities.

General concerns about the misuse of corporate vehicles by criminals to disguise and convert the proceeds of their illegal activities, as well as concerns about the use of trust and company services to help facilitate this misuse, are reflected in the extension of the scope of the FATF Forty Recommendations to lawyers, accountants and TCSPs, and, in particular, in the wording of Recommendations 5, 33 and 34. They are concerns that have also been specifically referred to by the G7 Financial Stability Forum, the European Commission, the International Organisation of Securities Commissions (IOSCO) and the Organisation for Economic Co-operation and Development (OECD).

Of particular concern is the ease with which corporate vehicles can be created and dissolved in some jurisdictions, which allows these vehicles to be used not only for legitimate purposes (such as business finance, mergers and acquisitions, or estate and tax planning) but also to be misused by those involved in financial crime to conceal the sources of funds and their ownership of the corporate vehicles. Shell companies can be set up in onshore as well as offshore locations and their ownership structures can take several forms. Shares can be issued to a natural or legal person or in registered or bearer form. Some companies can be created for a single purpose or to hold a single asset. Others can be established as multipurpose entities. Trusts are pervasive throughout common law jurisdictions.

When in February 2000 the FATF reviewed the rules and practices that impair the effectiveness of money laundering prevention and detection systems as part of its non-cooperative countries and territories initiative, it found in particular that:

> *Shell corporations and nominees are widely used mechanisms to launder the proceeds from crime, particularly bribery (e.g. to build up slush funds). The ability for competent authorities to obtain and share information regarding the identification of companies and their beneficial owner(s) is therefore essential for all the relevant authorities responsible for preventing and punishing money laundering.*

The aims/objectives of the project:[2] This typologies project's prime aim has been to seek to identify in respect of corporate vehicles areas of vulnerability for money laundering and terrorist financing, along with evidence of their misuse. It has also sought to identify differences among jurisdictions for establishing and using corporate

[1] Organisation for Economic Corporation and Development (OECD), Options for Obtaining Beneficial Ownership and Control Information: A Template (OECD Template) p.7

[2] This report is the product of research carried out by a project team operating under the umbrella of the FATF typologies initiative.

vehicles, how these may be exploited and what steps have been or are being taken by jurisdictions to address this threat[3].

While this typologies project is concerned with the misuse of corporate vehicles for money laundering and terrorist financing, the findings and the issues for further consideration can be expected to have similar application to other types of criminal activity. In addition to their use in facilitating money laundering, corporate vehicles are frequently mis-used to help commit tax fraud, facilitate bribery/corruption, shield assets from creditors, facilitate fraud generally or circumvent disclosure requirements.

The concerns arising from the misuse of corporate vehicles by criminals have been well documented by a number of other authorities.[4] However, it is hoped that from this typologies project will come a clearer picture of the misuse involved. This in turn should help focus and prioritise efforts made in the anti-money laundering (AML) and combating the financing of terrorism (CFT) areas to meet those concerns.

Corporate vehicles play a complex, varied and essential role in modern economies. The scope and scale of a typologies project that looks at the misuse of corporate vehicles is therefore potentially enormous. Extensive literature already exists on the subject, and the considerable jurisdictional variation in the nature, scale and oversight of corporate vehicles means that there are also many differing viewpoints on the subject to be taken into account. Similarly, many specific issues arise regarding the creation, administration and operation of corporate vehicles.

In examining the potential misuse that corporate vehicles may be subject to, it is important to bear in mind that, of the millions of companies that exist, the vast majority engage in legitimate business, and only a small minority are misused. Likewise among the trusts that are set up, the majority serve legitimate purposes, and only a small minority are misused.[5] In considering the misuse of corporate vehicles, it will be essential therefore to distinguish between those vehicles that pose a high risk and those that pose a low risk in relation to money laundering and terrorist financing.

The initial step for this project was to establish a team of experts which included persons drawn from FATF jurisdictions, observer organisations and FATF-style regional bodies (FSRBs) with skills/experience in the process of corporate vehicle formation and administration, and in particular the formation and administration of shell companies, and in regulatory action and law enforcement in this field. The experts came from a range of countries including common law and civil law jurisdictions, countries from outside the FATF and also countries with a substantial TCSP and/or non-resident business activity sectors.

The first step taken by the team of experts was to conduct a survey (by means of a questionnaire)[6] as a way of obtaining a fuller picture of the international diversity in the formation and administration of corporate vehicles, and of providing both FATF and FSRB members with an opportunity to contribute to the exercise.

Faced with the vast scope of a general project on corporate vehicle misuse mentioned above, it was clear to the team of experts that the most effective way to deal with the subject was to focus first on what they and prior studies considered to be the most significant feature of the misuse of corporate vehicles – the hiding of the true beneficial ownership. It is therefore with this aspect in mind that this report is primarily concerned. This is not to deny that there are other aspects that are worthy of attention, and that more detailed work on other areas could be done later.

---

[3] Some jurisdictions, such as the US, do not have a national or nationally uniform system of incorporation or registration of corporations, trusts and other business entities but instead have a dual Federal State or multi-regional systems. References in this report to the laws and principles in such jurisdictions are necessarily generalisations regarding the majority of states or regions, or the most common elements of the specific law or principle referenced.

[4] See the bibliography and Annex 5.

[5] Annex 2 refers to the many legitimate uses for trusts as well as the potential for their misuse.

[6] A copy of the questionnaire used is attached at Annex 7.

The terminology used in the context of corporate vehicles is also quite varied and complex, and it often differs from one study to another. Therefore, a glossary of terms used in this report is included in Annex 1. At the start of this report, it is useful however to highlight two key terms as they will be used for this study:

- *Corporate vehicle*: This term has the same meaning as that used by the OECD[7] and thus includes corporations, trusts, partnerships with limited liability characteristics, foundations, etc.

- *Trust and company service provider (TCSP)*: This term has the same meaning as used by the FATF[8] and thus includes those persons and entities that, on a professional basis, participate in the creation, administration and management of corporate vehicles.

2. Typologies

As a starting point for this study, the team of experts first examined a series of case examples of misuse of corporate vehicles[9]. By examining such material, certain key elements and patterns for this misuse were identified. The following typologies then derive from case examples that were submitted as part of the response to the survey as well as from several databases.

This section uses a selection of the submitted cases[10] to focus on examples in which one of the main objectives of the misuse was to hide the ultimate beneficial owner. The case studies indicate how difficult it can be to determine who actually benefits from the structure. The different ways to maintain anonymity and to hide identity are described in the following case examples. Often these structures are used to perform two functions simultaneously: the execution of a criminal scheme and the diversion of money flows as part of a money laundering scheme.

All submitted case studies show several common features. For illustrative purposes, four typologies were selected, each of which focuses on a specific method or element of a corporate vehicle structure that is commonly used to hide identity. As indicated above, the selection of cases was made so as to highlight the key characteristic involved. The remaining case examples are included in Annex 4, which classifies the examples according to individual typologies and main characteristics that can be useful for money laundering activities.

Typology 1 – Multi-jurisdictional structures of corporate entities and trusts[11]

In many instances, a structure consisting of a series of corporate entities and trusts — created in different jurisdictions — is used to hide identity and carry out a fraud scheme[12]. The complex structure can give the appearance of a legitimate purpose, which can then be used to easily attract investment from third parties. For the third parties that are victims of such schemes, it is almost impossible to see behind the structure of the various corporate entities to find out who is liable for their loss. By setting up such a complex multi-jurisdictional structure, the seemingly logical money flow between these entities is used to move and launder criminal money. These structures can also be convenient for diverting the money flow or hiding payments. The cases belonging to this typology are described briefly in the next few paragraphs, with more detailed descriptions set out in the boxes below.

---

[7] See the OECD report *Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes (Behind the Corporate Veil), 2001*.

[8] See the glossary to the FATF Forty Recommendations.

[9] A detailed description of all characteristics of these case studies is included in Annex 4 which was compiled with the considerable assistance of the Netherlands authorities.

[10] A detailed description of all characteristics of these case studies is included in Annex 4.

[11] This relates to cases 1, 2, 3, 12, 16, 17, 24, 25, 26, 27, 28, 29, 31, 32, 33 and 34.

[12] The scheme mostly involves types of financial fraud and Ponzi schemes.

In Case 1, third parties were persuaded to invest savings and retirements accounts in a series of trusts. The investors were led to believe that the trusts would ultimately provide investment income. In fact, however, the trusts, which were tied to offshore bank accounts, served as conduits for channelling funds to the perpetrators of the fraud scheme.

In Case 2 a multi jurisdictional structure was set up to purchase insurance companies and again divert the assets to the creators of the structure.

Case 3 concerns an investment fraud scheme. To realise the scheme, offshore corporations from Antigua, Isle of Man and Belize were used. The structure was also used to divert the money and hide the profits from fiscal authorities.

Case 1
Mr. [A] was a trust service provider operating a trust company [L]. Using a series of domestic trusts that he established, he wired large sums of money to 51 different US and offshore bank accounts. In total it is estimated the scheme defrauded over 500 investors of approximately $56 million.
The thrust of the scheme was that A and associates convinced their clients to form ["Pure Trust Organizations" (PTO)] and to place their life savings, including their retirement accounts, into these trusts created by [L]. Clients were advised that the [PTO] provided asset protection providing concealment of their assets from the government and other creditors. The [L] package promised the formation of a [PTO] and off- shore bank accounts. The clients were told that when the funds were placed in these off-shore bank accounts the funds was beyond the reach of the US government and any creditor.
Once the clients had placed their assets into the trusts, [A] used another corporation to provide investments for the assets in the trusts. In reality there were no real investments, and [A] and his associates defrauded the trust owners.

Case 2
Mr. [B] set up an international structure with on- and offshore companies as well as trusts to purchase insurance companies. The insurance companies were actually bought through a trust to hide the personal involvement of [B]. The assets of these companies were subsequently drained and used for personal benefits. The draining of these assets was concealed by transferring the money into accounts in and out of the US via wire transfers. Immediately after the acquisition, [B] would transfer million of dollars of reserve assets to a corporation he set up in the US. The funds were transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, [B] used them to pay for his personal expenses. In this way [B] laundered about USD 225 million over a period of 9 years.

Case 3
This case example shows a pyramid investment scheme. It caused more than USD 8.4 million in losses to almost 8,000 investors in the US. The investigation focused on an association [M]. [M] was a pyramid business enterprise that sold various products to its members including investment plans. It was alleged that [M] leaders were promoting the sale of an investment, identified as [Private Placement Offers (PPO)]. The investment promised a 30 to 1 return within a year. To be able to benefit f the investment members were encouraged to establish offshore corporations and bank accounts in Antigua, Isle of Man and Belize. They were advised that financial transactions relating to these investments should be transferred through their offshore accounts. The funds of all the investments were deposited into bank accounts in the US. Instead of using these monies as purported, [M's] leaders diverted the funds to their personal use and used the funds to promote the carrying on of the illegal enterprise. Potential investors were fraudulently lulled into believing that the investment was guaranteed by a bank and the principal insured by a major insurance company. The new investor funds collected and not yet turned over to the US Corporation were used to issue checks to investors within the group who were expecting their first returns from investment. The appearance that the program was working caused a windfall of new investor money to begin pouring in for the [PPO].

Case 4
The identity of the beneficial owner remained unknown in the management of several investment funds.
Fund E was established in the British Virgin Islands. This fund had over EUR 93 million in assets in Bank A. The fund was managed by Company F in Dublin.
One of the shareholders of Fund E was Bank G in Switzerland. Another shareholder was Fund H (Bahamas), managed by Company I (Bahamas). Fund H was 100% controlled by Bank J, another Swiss bank.
However, for Fund E, Bank A was not able to compare the subscriptions with the total amount of capital issued by the fund. Moreover it appeared from business correspondence found during the on-site mission led by the French Banking Commission that Mr K was directly involved in the management of Fund E. It was likely that Mr K's family was the beneficial owner of the fund, but the bank had no evidence thereof.

Typology 2: – Specialised financial intermediaries / professionals

The cases related to this typology highlight the fact that, when there is evidence of the misuse of corporate vehicles, a specialised financial intermediary or professional has often been involved, to a greater or lesser extent, in facilitating the formation of an entity and exploiting the opportunities presented by foreign jurisdictions to employ various arrangements that can be used for legitimate purposes but also can be used to help conceal true beneficial ownership, such as corporate shareholders, corporate directors and bearer shares. The degree of complicity of these financial intermediaries and professionals varies widely, with some unknowingly facilitating illicit activities and others having greater knowledge of their clients' illicit purposes.

Case 5
A company initially established in an offshore centre had moved its registered office to become a limited company under Belgian law. It had consulted a lawyer for this transition. Shortly afterwards the company was dissolved and several other companies were established taking over the first company's activities. The whole operation was executed with the assistance of accounting and tax advisors. The first investment company had opened an account in Belgium that received an important flow of funds from foreign companies. The funds were later transferred to accounts opened with the same bank for new companies. These accounts also directly received funds from the same foreign companies. Part of it was invested on a long term basis and the remainder was transferred to various individuals abroad, including the former shareholders of the investment company. These funds were also transferred to the new companies. The whole structure was set up by tax accountants.

Case 6
Mr. [C] was an accountant who started his own accounting and financial services business [N] in Panama. He advertised his services primarily on the internet and through mass mailings. [N] provided a variety of services including the following:

- *Formation of offshore entities to disguise ownership of assets;*
- *Passports and dual citizenship, mostly using new nominee names;*
- *Movement of cash and other assets offshore and back onshore using various methods;*
- *Issuance of debit cards for the purpose of anonymously repatriating and spending offshore funds;*
- *Use of correspondent bank accounts to skim profits of legitimate businesses and repatriate funds through the purchase of assets and use of debit cards;*
- *Anonymous trading of securities through accounts with two major brokerage houses;*
- *False invoicing/re-invoicing schemes to support fraudulent deductions on tax returns;*
- *False investment losses, to disguise transfer of funds overseas.*

[C] was identified pursuant to an Internal Revenue Service investigation of one of his clients for illegal importation and sale of goods. The targets of this investigation were using a re-invoicing scheme devised by [C] to illegally import these chemicals into the US for sale. [C] assisted the targets in the re-invoicing scheme by preparing the invoices, receiving the proceeds of the scheme and hiding the proceeds in a myriad of Panamanian corporations for later use by the targets.

As a result of this investigation, [C] became a subject of investigation for the formation of illegal trusts to facilitate money laundering and other crimes. The investigation disclosed that [N] had about 300-400 active clients/investors. The investigation also disclosed that it created between 5,000-10,000 entities for these clients, including the layering of foreign trusts, foundations and underlying business corporations, which were formed in offshore countries. The primary package purchased by the client was referred to as the Basic Offshore Structure that includes a foreign corporation, a foreign trust and a foundation. In 2003, [C] was found guilty of money laundering and other criminal violations. He was sentenced to 204 months' imprisonment and fined USD 20,324,560 and ordered to pay restitution to the Internal Revenue Service in the amount of USD 6,588,949.

Typology 3: – Nominees

The next series of cases provides examples of the extent to which the use of nominees may be used to hide the identity of the beneficial owners. Within this typology, the use of nominees may be grouped into the following categories: nominee bank account, nominee shareholders and nominee directors.

Case 7
Mr [B] and his associate bought insurance companies. The assets of these companies were drained and used for personal benefits. The draining of the assets was concealed by transferring them into accounts in and out the US via wire transfers. The first step in the scheme was establishing a trust in the US. [B] concealed his involvement and the control of the trust through the use of nominees as grantors and trustee. [B] then used the trust to purchase the insurance companies. Immediately after the acquisition, [B] would transfer millions of dollars of reserve assets to a corporation he set up in the US. The funds were then wire-transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, [B] used them to pay for his personal expenses.

Case 8
Beginning in 1997, Mr. [D] assisted his clients with various schemes to hide income and assets from the IRS, including a method by which an individual used ' common used trusts' to conceal ownership and control of assets and income and the use of offshore trusts with related bank accounts in which the assets would be repatriated through the use of a debit card. [D] also set up international business corporations (IBC) that had no economic reality and did not represent actual ongoing business concerns, on behalf of his clients, to conceal the clients' assets and income from the IRS. Concerning his own liabilities, [D] opened and maintained nominee bank accounts both in the US and abroad to conceal his income from the IRS.

Case 9
Mr. E, a CEO of a local telecommunication company received corrupt money of RM 300.000 as an inducement to award supply and work worth RM 5 million to a company P which belonged to Mr. F. Mr. F paid the corrupt money as a payment by company P to company Q for services rendered. Company Q also belonged to Mr. F but was merely a dormant and shell company with RM 2.000 paid up capital. The money was later withdrawn from company P and placed in a stock broking firm under the name of Mr. G., a nominee of Mr. E, who opened an account with the same stock broking company using his son's name. The money in G's account was used to purchase shares in the open market and later sold to Mr. E's son using numerous married deal transactions whereby the shares were later sold by Mr. E's son in the open market at a higher price. Capital gains subsequently were used to open fixed deposits, sign up for a insurance policy (under the name of Mr. E) as well as purchase assets in the name of Mr. E's relatives.

Typology 4: Shell companies.

The use of shell companies to facilitate money laundering is a well-documented typology. The complex case included here provides a "textbook" typology as an example of misuse of corporate vehicles. The scheme established here was intended to launder criminal proceeds through real estate investment. A complex structure was set up by legal professionals to hide the origin of the beneficial owners as well as the origin of the money.

THE WHITE WHALE CASE

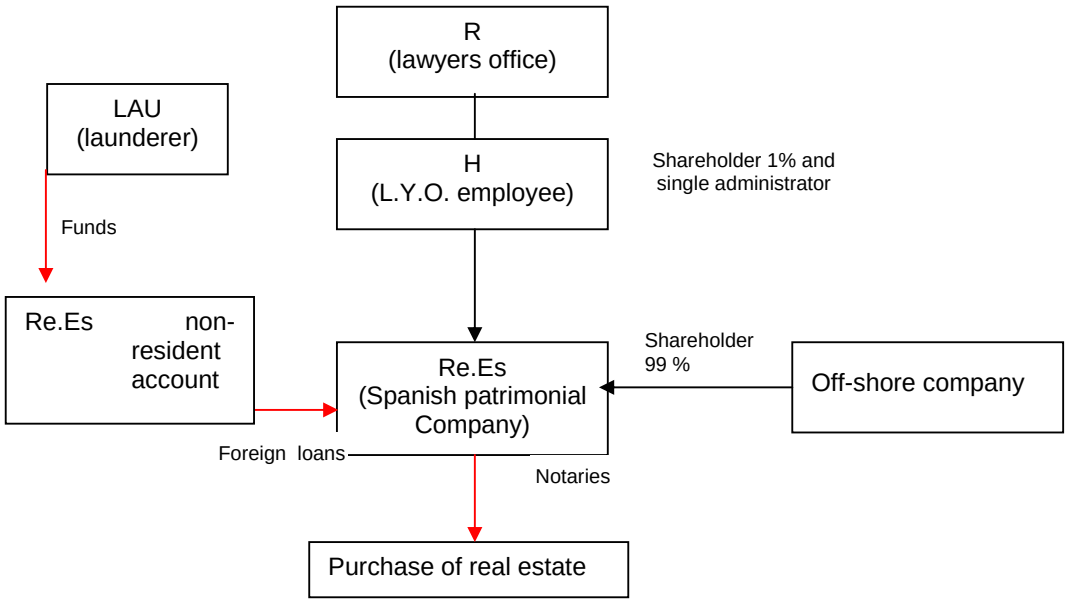
The investigations started in September 2003 by cross referencing data from an investigation on drug trafficking, with information coming from another investigation on assets owned by Eastern European citizens living in the Costa del Sol (Malaga).

In such cross referencing of information it arose that [H] appeared as administrator of more than 300 companies established through [R], a lawyer's office in Marbella (Malaga).

All of the companies had similarities: companies established off-shore, except one held by [H] who was the single administrator of the companies and, at the same time, an employee of [R]. Giving support to clients of H by establishing companies was one of the activities of [R], which also offered the management of client's bank accounts and real estate buying and selling. The investigators knew that several clients of [R] were allegedly connected with international organized crime groups and/or with people involved in serious crimes in Spain and abroad.

The board of [R] was aware of the likely criminal activities of some of H's clients, because they had been the subject of media and press reports as possible criminals, and because the board knew that some clients were in prison in Spain or in other countries since documents had been sent to them there. In other cases, members of the board were called to testify as witnesses in judicial proceedings against those clients.
Additionally, the board deliberately ignored the activities of their clients. In their advertisements they even advertised that the office conducted company´ "engineering", that they guaranteed anonymity and that they did not ask any questions or respond to requests for information.

Diagram of the money laundering scheme



The Spanish companies were established for use as an instrument for money laundering schemes based on the real estate market. They were companies created exclusively for the management and administration of real estate properties. Re.Es. was one of these companies.

The off-shore companies which participated in the Spanish companies were "shell companies" established in an American State whose laws allow a special tax regime for these companies and for their transactions. The companies were pre-constituted in the name of an agent (usually a lawyer) before the incorporation of the company. In other words, the document of incorporation of the company would remain inactive in the hands of the agent until the company was bought by a client, and at that moment the company would be effective.

Therefore, the board of the companies when first registered was made up of the agent and his associate, without any link with the real owners of the company who subsequently purchased the shell. Consequently, the ultimate beneficiaries of the off-shore companies and, consequently, of the Spanish companies, remained hidden.

The launderer (LAU) transferred funds from a foreign country to a non-resident account owned by Spanish company Re.Es. The use of non-resident accounts provided other advantages, including the advantage of being subject to less control by the tax authorities. The funds described above were gathered in the account of Re.Es under the guise of foreign loans received. The destination of the funds received was the purchase of real estate properties in the name of Re.Es., in the last stage of the money laundering process, taking advantage of the hidden situation of the launderer and of the beneficial owners.

Three public notaries documented all the transactions, from the incorporation of the companies to the purchase of real estate. The suspicion of money laundering was clear: incorporation of several companies by the same persons in a short period of time, concurrence of the same partners in several companies, several real estate purchases in a short period of time, etc. Despite this, and even though the public notaries were obliged to report under the Spanish anti-money laundering law, such transactions were not disclosed to the Spanish FIU

Analysis of the Typologies

From the typologies presented here, the methods for concealing the identity of the beneficial owner and/or his customer may be broken down into the following groupings based on the types of corporate vehicles used in the structure of the money laundering scheme.

Figure 1

Use of (various types of) companies	7 cases
Use of banks or investment funds	2 cases
Use of one of more trusts	5 cases
Use of companies and trusts	4 cases
Use of nominees	6 cases
Use of TCSPs	5 cases

More details on the findings for the individual case studies used are described in Annex 4.

Traditionally the money laundering process is broken down into three phases — placement, layering and integration. Since corporate vehicles may be used for multiple purposes in the different phases of the money laundering process, a slightly modified version of this template might be considered to better describe the role

that such entities can play in money laundering[13]. For the analysis of the case studies four phases of money laundering were distinguished.

In the "placement" phase, dirty money is inserted into the financial system. In the second or "layering" phase, the money is moved through various bank accounts, mostly belonging to several different corporate vehicles in multiple jurisdictions. The third phase, known traditionally as the "integration" phase consists of two sub phases: "justification" and "investment". In the "justification" phase, the proceeds are re-integrated into regular business activities, for instance by way of a loan structure. In the "investment" phase, the now laundered money is invested for personal gain, such as purchasing real estate.

Looking at the cases sampled for this study, the following breakdown may be made of the particular phases in which the corporate vehicles appeared to play a preponderant role in the money laundering process.

Figure 2

Money laundering phase	Number of case studies
Placement	22
Layering	5
Justification	2
Investment	4
Unknown (more specific details are needed for classification)	2
No money laundering process identified	4
Combination of money laundering phases	6

As can be seen from this overview, it was found that the majority of the cases presented involved misuse of corporate vehicles in the first phase of money laundering. In a number of cases, corporate vehicles are used to lure third parties in fraudulent investment schemes or committing other types of fraud. It is clear that this finding is based on the information available and that the case studies from which information has been obtained involve crimes other than money laundering. However, the techniques observed – the use of corporate vehicles, the use of specialised intermediaries, and the use of foreign jurisdictions – are all common to the techniques used for money laundering and therefore can be considered to be of equal relevance.

In analysing the submitted case studies, certain common elements were found. These elements are sometimes combined with the typologies (e.g. the involvement of financial or legal experts) and sometimes with an additional element to help achieve the goal (e.g. concealing identity, diverting money flow). The most common elements are the following:

- Multi-jurisdictional and/or complex structure of corporate entities and/or trusts (cases 1, 2, 3, 4 and White Whale);
- (Foreign) payments without a clear connection to the actual activities of the corporate entity (cases 5, 11,and White Whale);
- Use of offshore bank accounts without clear economic necessity (cases 1, 4, 3, 6, 17, 21, 27, 28 , , 30, 31, 32, 34, and White Whale);

[13] It should be noted that the case studies showed that, unlike most other methods used to launder money, legal entities are used not only to launder money, but also to generate it, e.g. from earnings of a criminal offence (money with illegal origin) or as windfalls (earnings) of tax evasion (money with legal origin).

- Use of nominees[14] (cases 2 7, 8, , 27, 28, 35, and White Whale);
- Use of shell companies (White Whale);
- Tax, financial and legal advisors were generally involved in developing and establishing the structure. In some case studies a TCSP or lawyer was involved and specialised in illicit services for their clients (cases 1, 5,6,7 and White Whale).

When hiding or disguising the identity, often a combination of the above mentioned elements and various layers with a foreign element is established to maintain as much anonymity as possible. These elements can be considered as indicators or "red flags" for such activity. The more of these elements observed, the greater the likelihood (and the risk) that the identity may be able to remain unknown. It is therefore essential for authorities to be able to determine the ultimate beneficial owners of a company and the trustees, settlors, beneficiaries involved with a trust.

3. Analysis of the Questionnaires

The following is an analysis of the responses of 32 jurisdictions to the survey conducted by the FATF as part of this study[15]. The assumption underlying the survey is that one of the main purposes of the misuse of corporate vehicles is to hide the identity of the natural person(s) benefiting from and/or controlling the money laundering, that is, the beneficial owner (BO). Thus the primary aim of the survey was to ascertain how criminals might use corporate vehicles to hide their identities and how, in practice, this may have occurred. The survey sought to achieve this aim by eliciting information on (1) the types of corporate vehicles in a particular country, (2) the types of BO relationships, (3) the sources of BO information and methods of obtaining such information, and (4) examples of the misuse of corporate vehicles in that jurisdiction. Beneficial ownership, the sources of information and the regulation thereof are addressed below. The case examples provided earlier demonstrate how the weaknesses identified are exploited in practice. The analysis is based solely on the information obtained through the survey; no verification of the information provided by respondent jurisdictions was undertaken.

The types of corporate vehicles are described in Annex 6[16]. Although many different types of corporate vehicle can be abused, the submitted case studies show that the legal entity most commonly misused is a private limited company with shared capital combined with activities in a jurisdiction other than the jurisdiction where the entity was created.

Section 1: Beneficial Owners

The FATF Methodology Glossary defines a beneficial owner (BO) as the natural person "who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement."[17] Accordingly, the issues of ownership, control, and, for trusts, beneficiary identification must be addressed.[18]

---

[14] Other legal structures that could lead to same result are the use of bearer shares and corporate directors.

[15] The participating jurisdictions are listed in Annex 3, along with the abbreviations used hereafter. The analysis was undertaken with the considerable assistance of the World Bank.

[16] In the case studies, varying types of corporate vehicles are referenced, such as *offshore corporate vehicles* (case 3), , *limited companies* (case 17), *UK limited companies* (case 19), *limited liability companies* (case 18,19), *corporate vehicles* (case 20), , *shell companies* (case 21), *Nevada corporations* (case 22), *trusts* (case 33 and 34). Both formal terms (e.g. *limited liability company*) and informal or "popular" terms (e.g. *shell companies*) were used interchangeably.]

[17] FATF Methodology, www.fatf-gafi.org/glossary.

[18] In view of the lack of universally accepted definitions or principles regarding control, beneficial ownership and related concepts, this report does not attempt to provide a detailed analysis of these concepts.

A. Ownership

The potential for anonymity is a critical factor in facilitating the misuse of corporate vehicles.[19] In particular, the fact that ownership of a corporate vehicle may be through corporate shareholders, nominee shareholders and bearer shares presents a special challenge to determining beneficial ownership of a corporate vehicle.[20] Each of these types of ownership is considered in Figure 2.1. It should be noted however that the ownership and control structures described below have many legitimate purposes.

Figure 3

PRACTICE: Ownership through…	Defining Characteristics	Associated Problems/ Risks	Where permitted among reporting jurisdictions
Corporate shareholders[21]	Shares are owned by a legal entity.	Creates an extra layer between BO and entity.	Not addressed in questionnaire
Nominee shareholders][22]	Shares are registered in the name of another (such as a stockbroker)	Reduces usefulness of shareholder register	Not addressed in questionnaire
Bearer shares[23]	Negotiable instruments according ownership of a corporation to the person who possesses the bearer share certificate.	Can be easily transferred without leaving a paper trail	NL,[24] UK,[25] TR, LB, LV, NZ, QA, HK, MH, DE, SK, CH, US, DK Permitted but dematerialised[26] in: VI, BE, LT, MO, FR

B. Control[27]

Corporations serving as directors and nominee directors can be used to conceal the identity of the natural persons who manage and control a corporate vehicle.[28] Corporate directors and nominee directors are described in Figure 4.

---

[19] OECD *Behind the Corporate Veil*, 2001, pp. 21.

[20] Id pp. 29-32.

[21] This type of ownership was not addressed in the survey, but the layering of different corporate entities on top of each other is a common characteristic in many cases of misuse of corporate vehicles, and hence it is included here. Of course this is not so much a "practice", but rather a logical characteristic of corporate law; anyone can hold shares, be it a natural person or a legal entity.

[22] This type of ownership was also not addressed in the survey. It is included here because two jurisdictions mentioned this issue (GI and IM). Of course ownership through nominee shareholders being simply a contractual relationship, it is possible in any jurisdiction that does not explicitly prohibit it, and this type of ownership is necessary for any broker trading on a stock exchange where shares are held on behalf of a client.

[23] A majority of bearer shares are book entries and are "dematerialised". Shares are dematerialised when they are registered. Dematerialisation is achieved by requiring registration upon transfer or requiring registration in order to vote the shares or collect their dividends. While physical transfer of bearer shares is possible it is believed to be rare.

[24] A majority of the bearer shares are *book entries* and are dematerialised. While physical transfer of bearer shares is possible it is believed to be rare.

[25] Some of the bearer debt in the United Kingdom is dematerialised, while another part of it is immobilised in International Central Securities Depositories (ICSD). The records of the ICSDs cannot be inspected.

[26] Shares are dematerialised when they are registered. Dematerialisation is achieved by requiring registration upon transfer or requiring registration in order to vote the shares or collect their dividends.

[27] Of course ownership will in many cases entail (a degree of) control. This paragraph deals only with those relationships of control that do not derive from ownership.

[28] OECD. Behind the Corporate Veil 2001 pp. 31.

Figure 4

PRACTICE: Control through...	Defining Characteristics	Associated Risks	Where permitted among reporting jurisdictions
Corporate directors	Corporation is selected to serve as a director. Management functions performed by representative of the selected corporation.[29]	Creates an extra layer in establishing identity of natural person who controls. May facilitate abuse of CVs if legal system cannot timely assign responsibility to physical persons.	NL, MY, US, GI, LV, MA, GG, QA, UK,[30] HK, MH, DE, PW, TR, LB, VI[31], BE, BA
Nominee directors [[32]]	Director nominates another entity or person to act as the director in its place.	Increased difficulty in identifying those who exercises de facto control.	Not addressed in questionnaire

Nineteen of the 32 jurisdictions responding to the survey indicated that corporations are permitted to serve as directors, whereas corporate directors are prohibited in eight. Five jurisdictions failed to provide an answer to this item on the questionnaire.[33] None of the responding jurisdictions that permit corporate directors indicated that foreign corporate directors were prohibited. One jurisdiction stated that "a fit and proper test applies to corporate directors, however executing these tests on foreign directors tend to be difficult due to lack of information."[34]

Although the survey did not specifically address the use of nominee directors, at least one respondent indicated that this practice is one of the greatest contributors to a corporate vehicle's vulnerability to misuse.[35] Typically, a nominee director appears as a director on all company documents and in any official registries, but passes the requisite duties of the directorship on to the beneficial owner.[36]

One jurisdiction allows TCSPs to act as nominee directors if certified to do so.[37] In this jurisdiction, TCSPs can face significant liability for failure to practice customer due diligence (CDD) and generally cannot be released from liability as nominees.[38] This jurisdiction further indicated that TCSPs are required to obtain indemnity insurance before acting as nominee directors.

[29] In some jurisdictions this representative can be liable for civil and criminal penalties. It is unclear from the questionnaires which jurisdictions in fact enforce these penalties.

[30] Legislation requiring that at least one natural person serve on the board is pending in the UK.

[31] VI has passed legislation requiring that at least one natural person serve on the board.

[32] Jurisdictions may have nominee directors, but this was not addressed in the survey.

[33] The item on the questionnaire reads "Are corporate directors possible?"

[34] NL, noting risk mitigation factors that effectiveness is limited to domestic corporate directors.

[35] GI, noting that the concept of nominee directors "does not exist in law". IM and TR also indicated permission of nominee directors.

[36] OECD *Behind the Corporate Veil*, 2001, pp. 31.

[37] IM.

[38] IM.

C. Beneficiaries

A beneficiary is someone for whose benefit property is held in trust, especially one designated to benefit from a disposition or assignment or to receive something as a result of a legal arrangement or other instrument. Traditionally, trusts have been treated like contractual agreements between private persons and subjected to less regulation and oversight and to fewer disclosure requirements, thus making them susceptible to abuse.[39] Trusts can legally be established in seventeen of the jurisdictions surveyed.[40]

Section 3: Information Sources

Information about corporate vehicles may be obtained from a variety of sources such as the corporate vehicles themselves, from a company registry, from public sources such as government or regulatory authorities, exchange operators, via intermediaries such as TCSPs or lawyers, notaries or accountants, or from other sources through the use of compulsory or investigatory measures.[41]

A. Corporate Vehicles

Corporate vehicles often keep shareholder registers. Fifteen jurisdictions indicated that corporate vehicles are obliged to keep shareholders lists that are then available to competent authorities.[42] One jurisdiction indicated that international business companies (IBCs) are required to maintain a register of shareholders at its registered office.[43] To be clear, the shareholder registers may contain accurate information on legal ownership, but not necessarily on beneficial ownership.[44]

B. Company Registries

All jurisdictions responding to the survey indicated that company registries with information on legal ownership are required. Twenty jurisdictions include foundations in these registries[45], twenty-five jurisdictions include limited liability partnerships[46], and three jurisdictions include trusts.[47] Eighteen jurisdictions indicated that it is mandatory for the registry to be regularly updated.[48] One jurisdiction requires that any change in the beneficial ownership of shares be reported to the public registry.[49] These registries are accessible to the public in all but three jurisdictions.[50] One jurisdiction indicated that it is optional for companies to be recorded in the company registries.[51] Five jurisdictions require that a corporate vehicle be approved before it can be included in the company registry.[52]

---

[39] OECD Behind the Corporate Veil, 2001 pp. 25-26.

[40] GG,IM,MH,HK,UK,QA,MY,GI,NO,PW,MA,NZ,JE,VI,JP,BA,US. Other countries may recognize trusts pursuant to the Hague Convention on the Law applicable to Trusts and on their Recognition.

[41] OECD *Behind the Corporate Veil,* 2001, pp. 41-42.

[42] GI, MY, CH, US, LT, SK, MA, QA, HK, FR, TR, LB, BE, VI, NL.

[43] BA, noting how it obtains information on ownership of companies.

[44] MY, GI, SK, MO, GG, BH, LB and JE require upfront disclosure with respect to beneficial ownership prior to start up. However, for GG, BH and LB, this information is not required to be updated. Only JE reported an explicit requirement that information on beneficial ownership be updated.

[45] NL,GI,MY,CH,US,SK,NZ,MO,ES,QA,DE,DK,PW,TR,LB,FR,JP,AU,BE,BA.

[46] NL,GI,MY,US,SK,NZ,MO,BH,ES,IM,QA,UK,HK,MH,DE,DK,PW,LB,FR,JE,VI,AU,BE,BA.

[47] For GI,MY and HK it is unclear whether registration is required.

[48] GI,MY,SK,NZ,MO,MA,BH,IM,UK,HK,DK,TR,LB,FR,JE,BE,BA,CH.

[49] JE, noting how it obtains information on the beneficial owner.

[50] BH,TR and JP did not report that the registries were open for public inspection, although they indicated that the registries could be accessed through investigatory means.

[51] VI

[52] NL, MY,LV,BH,GG

C. Intermediaries

Intermediaries, such as TCSPs, lawyers, notaries and accountants, commonly play a role in the formation and management of corporate vehicles.[53] In the cases submitted as part of the survey, intermediaries played a role in many instances. Twelve jurisdictions require TCSPs to carry out customer due diligence procedures that are predicated upon a verified identification of the beneficial owner[54], and nine jurisdictions mandate that TCSPs apply for a license before engaging in the business of the formation or management of corporate vehicles[55]. About half of the jurisdictions use TCSPs for the formation and management of corporate vehicles.[56] Within these jurisdictions, TCSPs face sanctions for deficiencies in exercising due diligence. These sanctions can include making public statements, the imposition of conditions on continued licensure, requiring specific actions, and license revocation.[57]

Twenty-nine jurisdictions allow lawyers, notaries, and accountants to participate in the formation and management of corporate vehicles.[58] However, only seven jurisdictions specifically reported that their governments enforce AML regulations with respect to intermediaries.[59] Of those six, three jurisdictions defined penalties for failure to follow AML regulations.[60] Those penalties included letters of disapproval, automatic governmental access to books and accounts, and loss of license. Ten jurisdictions rely on private regulation of intermediaries for the civil enforcement of AML.[61]

One jurisdiction stated that it places significant reliance on financial institutions to obtain information on the beneficial owner. It noted the importance of CDD and KYC practices for the success of their reliance on financial institutions.[62]

D. Other Sources

Other sources of information can be utilised through a jurisdiction's investigatory powers, including both the ability to gather information from public records as well as the authority to compel corporate vehicles to release information. Thirteen jurisdictions rely exclusively on investigatory powers to obtain information on beneficial ownership.[63]

Typical means employed by jurisdictions relying on investigatory powers include examining the tax returns of corporations through the local internal revenue office,[64] retrieval of information from online databases,[65] and acquiring information from a jurisdiction's securities exchange commission. According to one jurisdiction, the inability to use evidence gathered by investigation at trial presents a problem with this method.[66] Another

---

[53] *Behind the Corporate Veil*, 2001 pp. 50 (company formation agents, trust companies, lawyers, notaries, trustees, and other professionals).

[54] NL,GI,MY,CH,MA,GG,IM,UK,HK,JE,VI,BA

[55] NL,GI,NO,CH,MA,GG,IM,JE,BA

[56] NL,GI,NO,MY,CH,MA,GG,IM,UK,HK,DE,QA,LT,JE,VI,AU,BA

[57] JE, noting penalties regulatory bodies may impose on TCSPs

[58] GI, NO, MY, CH, US, LT, MO, LV, MA, BH, GG, IM, QA, UK, HK, MH, FR, DE, DK, PW, TR, LB, AU, NL, JP, VI, BE, BA, JE. Out of these, LT, GG, VI, NL and JP do not allow accountants to participate in these functions.

[59] MY, LT, HK, FR, AU, BE. BA noted that AML applies to all its citizens in compulsion for information but did not state any specific facts regarding lawyers, accountants, and notaries.

[60] MY, HK, BE

[61] MY, MO, LV, UK, HK, TR, LB, FR, JP, BE

[62] BA, noting the importance of financial institutions gaining BO information

[63] NO, US, SK, LV, QA, MH, DE, DK, PW, TR, LB, JP, AU, BE

[64] US,NL,UK,PW,SK,NL all noted the information on beneficial ownership could be obtained through tax returns.

[65] US noted availability of information from Dunn & Bradstreet, Lexis/Nexis, and Choicepoint.

[66] NO, noting its difficulties in using acquired intelligence information.

jurisdiction indicated that it uses its governmental powers to "undertake monthly updates of records of selected companies."[67]

The obstacles to obtaining information are compounded by the fact that in almost all cases of the misuse of corporate vehicles, there is one or more cross border relationship, as was evidenced by the cases submitted for the survey. In these examples, the cross-border structures had different corporate vehicles "stacked" on top of each other, with each vehicle holding (all or some) shares in the vehicle below it, they had non-resident management (directors)[68], or else the corporate vehicle had been incorporated in jurisdiction other than the one in which the related activity took place:

Figure 5

Jurisdiction or state of incorporation is *not* the same as jurisdiction or state where the actual activities take place	23 cases
Jurisdiction or state of incorporation is the same as jurisdiction or state where the actual activities take place	2 cases
Unknown (lacking information)	8 cases
Total number of analysed cases	33 cases

Indeed, the lack of economic and/or logistic benefits when using a multi-jurisdictional structure for corporate entities or the related money flow would appear to be an important indicator of possible abuse.

Furthermore, foreign (offshore) bank accounts were used in 13 of the 33 analysed cases. In 11 out of the 13 cases, a combination of multi-jurisdictional structure and foreign bank accounts was identified.

Section 4: Overview of survey responses

The responses to the survey highlighted the main areas of risk with respect to corporate vehicles, indicated frequent problems in obtaining information on beneficial ownership, and suggested areas for further investigation.

A. Areas of Risk

Several jurisdictions continue to have practices that make use of corporate vehicles which are relatively more vulnerable to exploitation for illicit purposes, such as ownership through nominee shareholding and bearer shares, and control through nominee and corporate directors.

Where information on a corporate vehicle must be disclosed upfront, there is a potential problem with ensuring that this information remains current and accurate over time. Dealing with this issue will require learning more about how jurisdictions with upfront disclosure systems for corporate vehicles enforce and update their company registers.

TCSPs, lawyers and accountants are required in most jurisdictions to practice CDD. Based on responses to the questionnaire this normally results in the information on beneficial owners being obtained by persons subject to AML requirements, but it does not necessarily mean this information is then directly accessible by the authorities.[69] Also, in jurisdictions with strong confidentiality rights, information held by the TCSPs may be treated in the same way as information held by legal professionals, thus making it harder for competent authorities to gain access to the records.[70]

[67] MO.

[68] See cases 4, 10, 11, 17, 19 .

[69] For example, MY, noting that TCSPs are not required to give information to investigators unless a warrant is obtained.

[70] Id.

Although bearer shares can serve legitimate purposes, they can also be used to mask the true ownership and control of a company and thus may be used for money laundering, self-dealing and/or insider trading. Sixteen of the thirty-two jurisdictions permit the use of bearer shares, and in two jurisdictions bearer shares can also be used by private companies.[71] Five jurisdictions indicated that they have dematerialized or immobilized bearer shares in an effort to verify the identities of their owners.[72]

B. Prevalent Problems in Obtaining Information[73]

Twenty-nine of the jurisdictions surveyed stated that they are willing to exchange information on beneficial ownership with foreign jurisdictions[74], although nine expressed concern about bureaucratic delays associated with obtaining information from foreign authorities[75]. Also, seven noted that the inability to gather necessary information from analogous regulatory bodies in other jurisdictions was due to insufficient disclosure from corporate vehicles and TCSPs, not from lack of co-operation.[76]

In summary: the survey appears to show that in the reporting jurisdictions–

- There is a wide variety of types of "corporate vehicles";
- "Beneficial owners" are involved with corporate vehicles in a number of different ways –through direct shareholding and through indirect shareholding (corporate shareholders, nominee shareholders, bearer shares, trusts);
- There are a large number of different competent authorities with oversight of corporate vehicles;
- Information on "corporate vehicles" can be found in a number of different places, such as company registries, financial institutions, and TCSPs;
- The degree of regulation applied to the creation and administration of corporate vehicles varies significantly from jurisdiction to jurisdiction – for example, a few jurisdictions regulate trust and company service providers, but the majority still do not;
- Many countries permit bearer shares to be issued and also permit the appointment of corporate and nominee directors;
- In some countries, the corporate vehicle itself is obliged to furnish/maintain certain information, and it is sometimes subject to criminal liability;
- In all countries covered by the survey, a company registry exists, but the extent of the information available from the registry varied significantly from jurisdiction to jurisdiction. Some require full shareholder information, others only partial information. Some provide information from the time of creation and have no update obligation; others include an obligation to register changes in shareholding. In nearly all cases, the information in the company registry relates to legal ownership – and not necessarily the beneficial ownership – of the corporate vehicle;

[71] TR,LB.

[72] LV,MO,FR,VI,BE.

[73] Note: there are a number of current international initiatives to improve the ability of regulatory authorities to share information (e.g. IOSCO).

[74] NL,GU,NO,MY,CH,LT,SK,MO,LV,MA,BH,GG,IM,QA,UK,HK,MH,DE,PW,TR,LB,FR,JE,JP,AU,BE, VI,BA, US

[75] GI,NO,MY,MA,IM,HK,PW,LB,JP

[76] NL,GI,LV,MA,GG,HK,LB

- Lawyers and accountants that are involved in establishing corporate vehicles are subject to AML regulation in the majority of countries surveyed.

4. Overall findings and conclusions

From the foregoing analysis of the typologies and the survey, it seems clear that prevention of corporate vehicle misuse for ML purposes could be improved by knowing or being in a position to determine in a timely fashion who are the ultimate beneficial owners of a company and who are the trustees, settlors, beneficiaries involved with a trust. It would also be important to find out for what purpose the corporate vehicle was formed, why foreign jurisdictions are being used for creation/administration of the entity, and why complex structures are being built.

The level of misuse of corporate vehicles could be significantly reduced if the information regarding the ultimate beneficial owner, knowledge of the source of assets and the business objective of the company or a trust within a structure were readily available to the authorities that might need it, especially in situations containing many or all of the "risk indicators" cited on pages 13/14. Since many of the structures are set up and / or managed by trust and company service providers it might be advisable that TCSPs be obliged to gather and maintain the above mentioned information. Some of this is already part of the present FATF-recommendations (at least the identification of the beneficial owner, as well as suspicious transaction reporting).

Another conclusion that may be drawn is that, in theory, it matters less who maintains the required information on corporate vehicles, namely:

- the corporate vehicle itself;
- the trust and company service provider;
- the registrar of companies; or
- another authority;

provided that the information on beneficial ownership exists, that it is complete and up-to-date and that it is available to competent authorities. It is thus an essential corollary that competent authorities – especially across jurisdictional lines – need to know where relevant corporate vehicle information is held and how it can be obtained. Both the OECD and IOSCO have emphasised that it is important for competent authorities to be able to co-operate with other competent authorities within and without their own jurisdiction to share relevant information on beneficial ownership.[77]

Company registers are an important source of information on legal ownership, although they may not always contain the most current information on the corporate vehicle. Nevertheless, as is indicated by the results of the survey, checking company registries is an important first step in obtaining information about the structure of corporate vehicles that are of concern. It is thus important that such registries be as comprehensive and as up-to-date as possible. Similarly, legal ownership information held by other public entities such as filings with financial regulatory authorities or stock exchanges should also be accurate and current.

Individuals and corporate vehicles have legitimate expectations of privacy and business confidentiality in their affairs and, from the information obtained through the survey, it is evident that jurisdictions adopt different approaches to protect legitimate privacy interests.[78] Certain of the arrangements and practices however, including the absence of appropriate regulation/supervision, would appear to contribute to the potential for

[77] OECD, Options for Obtaining Beneficial Ownership and Control Information: A Template (OECD Template) Annex 1, p33; IOSCO, Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information (IOSCO Multilateral MOU); and IOSCO, Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation, Principles 11-13.

[78] OECD Template 2002, Annex 2, p34.

corporate vehicle misuse by making it very difficult, and perhaps even impossible, for the authorities to identify beneficial owners and controllers.

As with all regulation – and as confirmed by the survey – it appears that there is a need to strike a balance between the need for robust regulation and/or supervision to prevent corporate vehicle misuse and the need to avoid unnecessary restrictions on legitimate business. In developing further guidance for this area, it will be important to consider the potential impact on overall economic performance, market integrity, market efficiency, market transparency and incentives.

The analysis of the typologies submitted as part of the survey, as well as prior studies relating to this topic,[79] points toward a number of frequently occurring risk factors associated with the corporate vehicle misuse (see Section 2 above). From this can be concluded that the further development of these common risk factors could be useful for countries in determining their own factors that help to identify such misuse and could be used in conjunction with other, existing, diagnostic tools, such as the OECD Template and the IOSCO Multilateral MOU. Examples of these factors are included in Figure 6.

Figure 6

Examples of Risk Assessment Factors

1. *What are the corporate vehicle formation requirements in the source jurisdiction?*
   - *Is information concerning the beneficial ownership and control of a company required to be recorded, maintained and kept up-to-date?*
   - *Do similar requirements apply concerning information on the settlor or founder, trustee and beneficiaries of a trust or foundation, and the partners of a partnership?*
   - *Are regularly updated list of the shareholders, directors and principal officers of all companies required to be maintained?*
2. *Are there adequate regulatory and/or AML standards or investigative capacities in the jurisdictions where the corporate vehicle has been incorporated /formed/administered (e.g. particularly in the application to lawyers, accountants and trust and company service providers engaged in the formation and administration of corporate vehicles)?*
3. *How might information on the beneficial owners be made available, or be obtained, in the jurisdiction of incorporation and/or the country in which the company and trust administration services are provided?*
   - *Is all or some of the information required to be maintained:*
     (a) *On a public register (and how easy it is to obtain the information)? *[80]*
     (b) *On a private register available to financial institutions;**
     (c) *On a private register available to regulators/law enforcement agencies (and under what circumstances can they share information available to them with other domestic/foreign regulatory authorities or law enforcement agencies)?*
     (d) *By licensed/regulated trust and company service providers (and under what circumstances and to whom are they permitted or required to make information available)?*
     (e) *By unregulated trust and company service providers (and under what circumstances and to whom are they permitted or required to make information available)?*
     (f) *By the entities themselves (and under what circumstances and to whom are they permitted or required to make information available)?*

[79] Id.

[80] Items marked by an asterisk should also be of particular interest to financial institutions when undertaking CDD in respect of corporate vehicles seeking to use their services.

- *Is there a register (public or otherwise) of the corporations, trusts, foundations and partnerships that are created, incorporated, registered or administered in the jurisdiction?**
- *Is the information referred to in the preceding bullet point required to be maintained in –*
  - *(a) The country of creation/incorporation?*
  - *(b) The country(ies) of administration or operation (if different to (a))?*
  - *(c) Both (a) and (b)?*

4. *What is known about the beneficial owner?**
5. *Is the corporate vehicle a regulated or unregulated entity?**
6. *What is the purpose of the corporate vehicle? Does it have 'real' activities (e.g. manufacturing, trading) or is it solely involved with holding/administrating the assets of the beneficial owner?**
7. *If applicable, why has the corporate vehicle been established in a foreign jurisdiction?**
8. *If applicable, why has an individual given up control over his assets to trustees, through the formation of a trust?**
9. *What is the purpose behind naming corporate shareholders, nominee shareholders, corporate directors or bearer shares* –*

   - *Are bearer or nominee shares permitted, and if so, is there an effective mechanism that will allow the ultimate beneficial owner of the shares to be ascertained? Who can use this mechanism and with whom can the information be shared?*
   - *Are corporate or nominee directors permitted, and if so, is there an effective mechanism that will allow the person with ultimate control of the company to be ascertained? Again, who can use this mechanism and with whom can the information be shared?*
   - *Is there a requirement that at least one director of the company/trustee of a trust/administrator of a foundation/partner in a partnership must be a natural person resident in the jurisdiction of creation/ incorporation/administration?*

10. *Can shell or shelf companies be formed in the jurisdiction of incorporation?*
11. *What is known about the source of funds?**
12. *What is known about the scale of the business/funds?**
13. *Are the business activities unusual, particularly with regard to the nature of the beneficial owners?**
14. *Are there any other unusual features about the structure/business activities of the corporate vehicles?**
15. *Are corporate vehicles administered by lawyers, accountants, trust company service providers or other individuals, and are intermediaries identified as the legal owner?*
16. *Is there a lack of oversight of those engaged in the formation and administration of corporate vehicles (e.g. is there a fit and proper test for those able to form and administer corporate vehicles; is there adequate control over the opening of bank accounts in the name of the corporate vehicles in the jurisdiction where the vehicle is formed)?*
17. *Do secrecy laws prevent or unduly restrict access to beneficial ownership information?*
18. *Are financial institutions and intermediaries obliged to obtain beneficial ownership information, and perform customer due diligence at the commencement, and during the course of, a business relationship, in particular when opening an account for a customer?*
19. *Have competent authorities been designated to oversee and monitor compliance with the requirements referred to in the preceding bullet point, including imposing sanctions for non-compliance where appropriate?*
20. *Can law enforcement agencies, and financial regulatory authorities, obtain or access beneficial ownership*

information, and is there evidence of information being obtained on a timely basis:

(a) For their own investigative or regulatory purposes?

(b) Based upon a legitimate request from another domestic or similar foreign authority, and share that information on a timely basis, and without unduly restrictive conditions?

21. Is there evidence of a lack of effective international cooperation exhibited by the authorities in the jurisdictions where the corporate vehicle is formed and/or administered?

22. What are the penalties or other consequences for non-compliance with international standards in the jurisdiction where the vehicle is formed and/or administered?

As suggested by the typologies examined as part of this research, there appear to be two essential factors that further protect against the misuse of corporate vehicles: (1) the quality of available information and (2) the quality of the "gateway" through which that information can be obtained. There is little value in having good gateways if no information on beneficial owners can be obtained. Likewise there is little value in knowing that there is good quality information available when investigators are unable to get access to it.

The conclusions drawn from the typologies are further reinforced by findings made in other sources that were consulted as part of this research project (extracts from these sources are included in Annex 5).

4. Issues for consideration

As stated at the beginning of this paper, the focus of research for this FATF typologies project has been on the beneficial ownership issues that are directly tied to the misuse of corporate vehicles for money laundering purposes. Despite this limited focus, however, the information and typologies examined through the project survey suggest a number of areas that may call for further and separate consideration – by the FATF and/or other relevant international organisations[81] – in preventing corporate vehicles and their activities from misuse by criminals. Some of the most important questions are as follows:

- Are the existing AML/CFT standards as a whole adequate to discourage the misuse of corporate vehicles?
- Are the specific FATF Recommendations 12, 16 and 24 sufficient as a basis for dealing with the issue of corporate vehicle misuse?
- What more can be done to ensure that adequate, accurate and timely information on the beneficial ownership and control of legal persons/legal arrangements may be obtained or accessed in a timely fashion by competent authorities?
- What can be done to ensure that those engaged in the formation and administration of corporate vehicles are "fit and proper"? Is there a need for an international standard for TCSPs or professionals engaged in providing trust and company services?
- What steps can and should be taken to ensure that the actions of those engaged in the formation and administration of corporate vehicles are properly monitored or subject to investigation as necessary?
- Should TCSPs be regulated or should there be enhanced regulation of such service providers, including lawyers and accountants where they offer similar services?

[81] For example, the OECD, who have already conducted extensive work in this area

- Should existing corporate governance standards (such as the OECD Principles) be extended to include factors relating to the role of TCSPs, lawyers and accountants in relation to the potential misuse of corporate vehicles?

- Should guidance in other forms be produced – for example risk assessment check lists – to help the competent authorities focus their risk-based approaches in relation to the different types of misuse of legal persons and legal arrangements?

- Where should beneficial ownership information be held?

- What more needs to be done to enhance the effectiveness of company registers, and other publicly available information?

- Is there any practical action that needs to be or can be taken to enhance the information publicly available in respect of legal arrangements?[82]

This typologies report should be seen as an initial report. It has addressed what is seen as the key issue in limiting the misuse of corporate vehicles – namely who is the beneficial owner and what is the purpose behind the corporate vehicles being used. There are however many matters deserving of further consideration which are further evidence of the scale and complexity of the issues involved in preventing the misuse of corporate vehicles.

[82] See Annex 2 for information on the South African system for registering the information on trusts.

BIBLIOGRAPHY

The following is a list of the source material/documentation accessed by the team of experts

- Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes; a report by the OECD (2001);
- Options for Obtaining Beneficial Ownership and Control Information – a template prepared by the OECD (September 2002);
- Trust and Company Service Providers: Statement of Best Practices – a report by the Offshore Group of Banking Supervisors (OGBS) (September 2002);
- Securing Effective Exchange of Information and Supervision in Respect of Trust and Company Service Providers – a report by OGBS (December 2004);
- A review commissioned by the International Trade and Investment Organisation and the Society for Trust and Estate Practitioners on "Regulating Corporate Vehicles and Cross-Border Transactions" (2002);
- FATF Report on Money Laundering Typologies 2000-2001 – February 2002;
- "Euroshore". Final report prepared for the European Commission, Falcone Progamme 1998, (January 2000) on Protecting the EU Financial System from the Exploitation of Financial Centres and Offshore Facilities by Organised Crime;
- Transparency and Money Laundering. A report produced for the European Commission by the Research Centre on Transnational Crime – University of Trento ("the Savona Report") (October 2001) on Study of the Regulation and its Implementation in the EU Member States that Obstruct Anti-money Laundering International Co-operation;
- Report of the United States Government Accountability Office (October 2000) on Possible Money Laundering by US Corporations Formed for Russian Entities;
- US Money Laundering Threat Assessment (December 2005) – report of an inter-agency working group composed of experts from the spectrum of the US government agencies, bureaux and offices that study and combat money laundering;
- Options papers prepared for the FATF working groups engaged on the review of the Forty Recommendations on beneficial ownership and control of corporate vehicles; enhancing the transparency of trusts; and trust and company service providers (March 2002);
- US Government Accountability Office (April 2006) – Report to the Permanent Sub-Committee on Investigations, Committee on Homeland Security and Governmental Affairs, US Senate on Company Formations – minimal ownership information is collected and available.

Annex 1 GLOSSARY

The following are terms used in this report, and elsewhere in the study of the misuse of corporate vehicles:-

Corporate vehicles: The term "corporate vehicle" when used has the same meaning as in the OECD report "Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes", and embraces corporations, trusts, partnerships with limited liability characteristics, foundations etc.

Legal persons/arrangements: The FATF Recommendations use two separate terms which together have the same scope as the OECD term "corporate vehicle" –

- legal persons - this refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property;

- legal arrangements - this refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include *fiducie*, *Treuhand* and *fideicomiso*.

  Particular difficulties are often experienced in understanding what is meant by a "trust". The Hague Convention on the Law Applicable to Trusts and their Recognition (1985) provides as follows in Article II –

  "For the purposes of this Convention, the term "trust" refers to legal relationships created ... by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose".

  There are many different types of trusts, many of which are most unlikely to be used by criminals (e.g. a will trust, an employee share/options trust, a pension fund trust). For an explanatory note on trusts, see Annex 2, which for the most part is taken from an OECD report produced by the Global Forum Joint Ad Hoc Group on Accounts entitled "Enabling Effective Exchange of Information: Availability and Reliability Standard".

Bearer shares: These are negotiable instruments that accord ownership of a corporation to the person who possesses the bearer share certificate.

Beneficial owner: This refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also encompasses those persons who exercise ultimate effective control over a legal person or arrangement.

Beneficiary: A person who is designated to receive something as a result of a trust arrangement. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust's perpetuity period, which is usually referred to in the trust deed as the trust period.

Corporate Director: A corporation appointed as a director with "management" functions being performed by a representative of the selected corporation.

Corporate Shareholder: a legal person who holds shares.

Corporate Trustee: A trust company appointed as a trustee and who has all the responsibilities/obligations of an individual trustee.

Nominee: The person, corporation, or beneficiary who has been appointed or designated to act for another (e.g. a Nominee Director is a director nominated by another director to act in his or her place).

Settlors: Persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.

Shelf company: A corporation that has had no activity. It has been created and put on the "shelf". This corporation is then later usually sold to someone who would prefer to have an existing corporation than a new one.

Shell company/corporation: A company that is incorporated that at the time has no significant assets or operations.

Trustee: A trustee, who may be a paid professional or company or unpaid person, holds the assets in trust fund separate from their own assets. The trustee invests and disposes of the trust assets in accordance with the settlor's trust deed, taking account any letter of wishes. There may also be a protector, who may have power to veto the trustee's proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

Trust and company service provider (TCSP): This has the same meaning as in the Glossary attached to the FATF Forty Recommendations and refers to any person or business that provides any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

In many jurisdictions the existence of TCSPs is not recognised. However, trust and company services may well be provided by lawyers and other professionals. For example, in most, if not all, jurisdictions lawyers will be engaged in the formation of foreign companies for clients to hold assets outside of that client's jurisdiction (e.g. a yacht, a residential or commercial property etc). Some TCSPs are required to afford confidentiality privileges to a client which can conflict with AML reporting requirements.

Even where jurisdictions do not recognise trusts, they may well have lawyers or other professionals within the jurisdiction engaged in the administration of trusts. For example, there may be no barrier in such jurisdictions to a resident professional acting as a trustee for a trust established under the law of a jurisdiction that does recognise trusts.

Annex 2 Explanatory Note: Trust

1. Definitions of a trust are to be found in the domestic trust law of those jurisdictions where such laws exist. Alternatively, the definition can be taken from the Hague Convention on the Recognition of Trusts.

2. As an example of a definition incorporated in a trust law, the following is taken from the Trusts (Guernsey) Law, 1989, which mirrors the definition in the Jersey (Trusts) Law, 1984:

   "A trust exists if a person (a "trustee") holds or has vested in him, or is deemed to hold or have vested in him, property which does not form, or which has ceased to form, part of his own estate –

   (a) for the benefit of another person (a "beneficiary"), whether or not yet ascertained or in existence;

   (b) for any purpose which is not for the benefit only of the trustee.

3. The Hague Convention on the Law Applicable to Trusts and their Recognition (1985) provides as follows in Article II –

   "For the purposes of this Convention, the term "trust" refers to legal relationships created .... by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose".

4. The definition of a trust, whether included in domestic law or in the Hague Convention, normally embraces a wide range of types of trust.

5. It is important to remember that a trust is not a legal entity, it is a relationship between juridical persons – settlor, trustee, beneficiary.

Express Trusts

6. These are trusts created voluntarily and intentionally, either orally or in writing –

   - inter-vivos by the settlor executing an act or instrument of settlement made between the settlor and the trustees under which the settlor transfers assets to the trustee to hold subject to the terms of the trusts set out therein;

   - inter-vivos by the settlor transferring assets to the trustees and the trustees executing a declaration of trust (to which the settlor is not a party) whereby the trustees acknowledge that they hold the assets subject to the terms of the trusts set out in the instrument; or

   - on death by the Will of testator taking effect, whereby the testator's executors are directed to transfer all or part of the testator's estate to trustees (who may be the executors) to hold subject to the trusts set out in the Will.

7. The following are forms of express trusts. Within any trust, different elements of the following may be found.

   (a) <u>Bare/Simple Trust</u>

   A bare trust is one in which each beneficiary has an immediate and absolute right to both capital and income.

   (b) <u>Discretionary Trust</u>

This is a form of trust where the interests of the beneficiaries are not fixed but depend upon the exercise by the trustee of some discretionary powers in their favour. As such, it is the most flexible of all trusts.

(c) Interest in Possession Trust

This is a trust where a particular beneficiary (the "life tenant") has a right to receive all the income arising from the trust fund during his life time. The trustee will usually also have the power to apply capital to the life tenant. Often there are successive life interests in favour of an individual and his spouse. On the death of the life tenant, the remainder of the trust fund is often held on discretionary trusts for the other beneficiaries.

(d) Fixed Trust

A trust where the interests of beneficiaries are fixed. The trustee will have control over the management of the assets, but the interests of the beneficiaries are defined in and by the trust instrument. Typically such a trust may provide an income which is paid, say, to the wife of the settlor and capital to the children on her death.

(e) Accumulation and Maintenance Trust

This form of trust is usually created for the children or grand-children of the settlor, where the trustees have powers during the minority of each beneficiary to pay income in a way beneficial for the upbringing or education of the beneficiary, and to accumulate income not so applied. On attaining a certain age each beneficiary will become entitled to a particular share of the trust fund.

(f) Protective Trust

A trust where the interest of a beneficiary may be reduced or terminated, for example on the happening of events (a common scenario may be if the beneficiary attempts to alienate or dispose of his interest in income or capital).

(g) Employee Share/Options Trust

Trusts established by institutions in favour of their employees.

(h) Pension Fund Trusts

Trusts established to provide pensions for employees and their dependants.

(i) Charitable Trust

A trust established purely for charitable purposes. In this case there needs to be an enforcer.

(j) Purpose Trust

A trust established for one or more specific purposes. There are no named or ascertainable beneficiaries and there is commonly an enforcer to enforce the terms of the purpose trust.

(k) Commercial Trusts

The major applications include –

- unit trusts;
- debenture trusts for bond holders;

- securitisation trusts for balance sheet reconstructions;

client account trusts for lawyers and other providers of professional services, separate from the provider's own assets;

- retention fund trusts, pending completion of contracted work.

Implied Trusts

8. A trust can also arise from an oral declaration or by conduct and may be deemed by the Court to have been created in certain circumstances. On account of their very nature there are no formal requirements for those trusts. Usually the existence of such trusts is only recognised as a result of legal action.

Resulting Trusts

9. Both express and implied trusts require an intention for their creation. A resulting trust arises where the intention is absent and yet the legal title to property is transferred from one person to another. By way of example, where X transfers £100 to Y at the same time as executing an Express trust in respect of £80, only the balance of £20 is held on a Resulting Trust to be retransferred back to X. In this situation, in the absence of intention, the beneficial ownership remains with the transferor.

Constructive Trusts

10. Constructive trusts are those trusts that arise in circumstances in which it would be unconscionable or inequitable for a person holding the property to keep it for his own use and benefit absolutely. A constructive trust can arise in a number of differing scenarios covering a broad spectrum of activity. The proceeds of criminal activity can be traced into the hands of the recipient's bankers who, once alerted, would hold them as constructive trustee on behalf of those to whom they actually belong.

11. Trusts may also be classified according to why they are created and may include –

- private trusts – made for the benefit of specific private individuals, or a class thereof;
- public trusts – made for the benefit of the public at large, or a section of the public – for example a charitable trust established to relieve poverty, to advance education or to promote religion;
- purpose trusts (see above).

12. This brief, and limited, description of trusts shows that the concept encompasses a wide variety of arrangements. Essential to them all is that legal ownership and control is passed from the settlor to the trustee.

Potential for misuse

13. Aspects of some trusts that can give rise to a lack of transparency and enable their misuse, which are also to be found in the misuse of companies, limited partnerships and other legal entities, can be itemised as follows –

(a) Trusts can exist without any written record.

These conditions where they exist can create difficulties for law enforcement or regulatory authorities (either administrative or judiciary) to gather rapidly information or evidence regarding the very existence of the trust and collect the names of their settlor or beneficiary(ies). In such circumstances, it can also be very difficult, if not impossible, for a financial institution to know and verify the name of a beneficiary of a financial transaction conducted through such a trust.

(b) A trust deed can exist which does not identify the settlor and/or the beneficiary.

Together with the situation in (a) above, this can create an important obstacle for the law enforcement authorities to identify rapidly the beneficiary(ies) of the trust, and can hamper a financial institution in fulfilling properly its know your customer requirements.

(c) Some form of trusts, such as the discretionary trust, can make it possible to give the trustee discretionary power to name the beneficiary within a class of beneficiaries and distribute accordingly the assets held in trust.

The beneficiary can be named or changed at any time, which can make it possible to keep the beneficiary's identity secret up until the time the ownership of the assets held in trust is transferred to them. As in (a) this can also make it difficult, if not impossible, for a financial institution to know and verify the name of a beneficiary of a financial transaction conducted through such trusts.

(d) The laws of certain jurisdictions have encouraged the development of so called asset protection trusts which can protect the settlor from the freezing, seizure, or confiscation of the assets, even though the settlor is able to keep control over their management, either by giving the trustee instructions or by naming a protector. In some jurisdictions, the settlor can be made a beneficiary of the trust without anyone being able to find out.

(e) Decisions about the management of trusts may not be recorded and they may not be disclosed in writing to anyone. If such decisions are not recorded at least by the trustee the law enforcement authorities cannot have access to them.

(f) Trusts can be set up for the purpose of managing shares in a company, which can make it even more difficult to determine who the true beneficiaries of assets managed by trusts are (cascade arrangements). These kinds of arrangements often have the purpose of hiding the identity of the ultimate beneficiary(ies) or real owner of an asset.

(g) Flee clauses can constitute an obstacle to an effective anti-money laundering framework, in particular in terms of international legal assistance. These clauses permit the automatic change of the law of the trust in case of certain events. With such clauses it is possible to protect trust assets against legal action.

(h) In some countries the use of trusts can be a way to escape from judicial decisions that freeze, seize or confiscate the assets located in trusts. Some legislation can explicitly prohibit freezing, seizure or confiscation of the assets located in trusts.

Register of Trusts

14. Most countries in which trusts are set up do not consider it practical to require trusts to be registered in the same way that a company is registered. However, in South Africa the Trust Property Control Act, 57 of 1988, Section 4, provides that the trustee must, before he or she assumes control of the trust property, lodge with the Master of the High Court the trust instrument in terms of which the trust property is to be administered. In other words, in respect of a trust inter vivos, the deed in terms of which the trust agreement is recorded must be lodged with the Master of the High Court before a trustee is allowed to take charge of the trust property.

The contents of the trust deed and the appointment of the trustees are therefore matters of public record. The master must on written request and payment of the prescribed fee furnish a certified copy of any document under the Master's control relating to trust property to a trustee, his or her surety or representative or any other person who in the opinion of the Master has sufficient interest in the document.

The value of the register depends on what information is contained in the trust deed. Insofar as a trust is a discretionary trust reference may be made in the trust deed simply to a class of beneficiary.

Annex 3 Jurisdictions Completing the Questionnaire

FATF Members	Members of FSRBs
Austria (AT)	Bahamas (BA)
Belgium (BE)	Bahrain (BH)
Denmark (DK)	British Virgin Islands (VI)
France (FR)	Gibraltar (GI)
Germany (DE)	Guernsey (GG)
Hong Kong, China (HK)	Isle of Man (IM)
Japan (JP)	Jersey (JE)
Netherlands (NL)	Latvia (LV)
Netherlands Antilles (NA)	Lithuania (LT)
New Zealand (NZ)	Macao, China (MO)
Norway (NO)	Malaysia (MY)
Spain (ES)	Marshall Islands (MH)
Switzerland (CH)	Mauritius (MA)
Turkey (TR)	Palau (PW)
United Kingdom (UK)	Qatar (QA)
United States of America (US)	Slovakia (SK)
(16)	(16)

Annex 4 Cases

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
1	Mr. A was a Trust Service Provider operating a Trust Company [L]. Using a series of domestic trusts that he established, he wired large sums of money to 51 different U.S. and offshore bank accounts that originated from a investment/securities fraud. The thrust of the scheme was that A and associates convinced their clients to form 'Pure Trust Organisations' (PTO) and to place their life savings, including their retirements accounts, into these Trusts created by L. Clients were taught the PTO provided asset protection providing concealment of their assets from the government and other creditors. The L-package promised the formation of a PTO and offshore bank accounts. The clients were told when the funds were placed in these offshore bank accounts it was beyond the reach of the U.S. government and any creditor. Once the clients placed their assets into the Trusts, A used another corporation to provide investments for the assets in the Trusts. In reality there were no investments, and A and his associates defrauded the Trust Owners.	Unknown	TSP	1) trusts in the U.S. (unknown is the type of Trust and the state in the U.S. in which the Trusts were established) 2) Pure Trust Organisation (PTO) (unknown is the type of corporation and the jurisdiction in which the corporation was established) 3) another corporation (unknown is the type of corporation and the jurisdiction in which the corporation was established)	The activities of this Trust Service Provider took place in the U.S. (unknown is the state in which this Trust Service Provider is seated and active)	1) use of trusts and corporations to realize scheme 2) use of trusts to divert the money flow 3) use of trusts and corporations to conceal identity of clients	IRS	1) Investment fraud 2) securities fraud 3) mail fraud 4) wire fraud 6) conspiracy Mr. A pleaded guilty and was sentenced to 220 months in federal prison.	1 Placement	In total it is estimated the scheme defrauded over 500 investors of approximately USD 56 million.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
2	Mr. B and his associate bought insurance companies. The assets of these companies were drained and used for personal benefits. The draining of the assets was concealed by transferring them into accounts in and out of the U.S. via wire transfers. The first step in the scheme was establishing a Trust in the U.S. B concealed his involvement and control of the Trust through the use of nominees as the grantors and trustee. B used the Trust to purchase the insurance companies. Immediately after the acquisition, B would transfer million of dollars of reserve assets to a corporation he set up in the U.S. The funds were then wire transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, B used them to pay for his personal expenses.	Unknown during 9 years	Feasible but not specifically described	1) trust in the U.S. (unknown is the type of Trust and the jurisdiction or state in which the Trust was established) 2) corporation in the U.S. (unknown is the type of corporation and the jurisdiction in which the corporation was established) 3) another corporation with an offshore bank account (which type of corporation and in which jurisdiction the corporation was established)	Mr. B used a U.S. trust to purchase insurance companies (unknown in which jurisdiction) and subsequently transferred millions of dollars of reserve assets to a corporation in the U.S.	1) use of structure, trust and shell companies to realize scheme 2) use of structure to conceal identity 3) use of nominees to conceal identity	IRS	1) wire fraud 2) money laundering 3) racketeering influenced corrupt organisation (RICO) 4) RICO conspiracy 5) securities fraud	1 Placement	Total restitution ordered by the court was approximately USD 400 million.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
3	Mr C and his associates perpetrated of a pyramid investment scheme caused more than USD 8,4 million in losses to almost 8,000 investors in the U.S. The investigation focused on an association [M]. M was a pyramid business enterprise that sold various products to its members including investment plans. The chairman of M was Mr. C. It was alleged that M's leaders were promoting the sale of an investment, identified as Private Placement Offers (PPO). The investment promised a 30 to 1 return within a year C promoted the PPO investments to M members and encouraged them to establish offshore corporations and bank accounts in Antigua, Isle of Man and Belize. He advised them to conduct their financial transactions relating to the PPO investments through their offshore accounts. It was proven that all the participants conspired to defraud and obtain money and property from individuals by means of false and fraudulent representations. From 4 years, C and his associates caused members of the M to invest in the PPO offered by a U.S. corporation. The result was the receipt of more than USD 8 million from investors for participation in the PPO. These funds were deposited into bank accounts in the U.S. Instead of using these monies as purported, they were diverted to the personal use and benefit of C and his associates and used to promote the carrying on of the illegal enterprise.	Unknown	Feasible but not specifically described	1) offshore corporations in Antigua, Isle of Man and Belize (unknown is the type of companies that were established)	An association known as Sovereign Business System (SBS) , a pyramid business enterprise was established in the U.S. and used to promote PPO´s. The investors subsequently transferred money into offshore organisations and trusts that were established in Antigua, Isle of Man and Belize.	1) use of multi jurisdictional structure realize scheme 2) use of offshore corporations divert money flow 3) use of offshore bank accounts	IRS	1) money laundering 2) mail fraud 3) wire fraud 4) other criminal charges	1 Placement	More than USD 8,4 million in losses to almost 8,000 investors in the U.S. Due to the seizure of assets, restitution of approximately USD 5,8 million was paid to the victims of this fraud.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
4	Fund E (BVI) had over EUR 93 million in assets in Bank A and was managed by company F in Dublin. One of the shareholders of Fund E was Bank G in Switzerland. Another shareholder was Fund H (Bahamas) managed by company I (Bahamas). Fund H was 100% controlled by Bank J, another Swiss bank. However, for Fund E, Bank A was not able to compare the subscriptions with the total amount of capital issued by the fund. Moreover it appeared from business correspondence found during the on-site mission led by the French Commission that Mr. K. was directly involved in the management of Fund E. It was likely that Mr. K´s family was the beneficial owner of the fund, but the bank had no evidence thereof.	Unknown	Feasible but not specifically described	1) British Virgin Islands (BVI) (unknown which type of fund was established) 2) Bahamas (unknown which type of fund was established) 3) Ireland (unknown which type of company was established) 4) Bahamas (unknown which type of company was established)	Fund E was managed by Company F in Ireland. Fund E used apparently French bank accounts Investments in Fund E were made by two Swiss banks, one of the Swiss banks invested in Fund E via Fund H established on Bahamas. Out of 51 companies for which bank A. did not identify the beneficial owner, 14 were established in BVI, 12 in Panama, 2 in Luxembourg, 1 in the Bahamas.	1) conceal identity of the beneficial owner through multi jurisdictional structure where companies, management, bank accounts and shareholders are all situated in different jurisdictions	French banking commission fined a bank for breach of the obligation to identify the beneficial owner (on-site visit)	Breach of French law	no ML	Banking commission fined Bank A with EUR 100.000
5	Company established in an offshore centre and moved its registered office to become a limited company under Belgian law. Limited company was dissolved and several other companies were established taking over the activities. The investment company (in Belgium) had opened a bank account and received an important flow of funds from foreign companies Funds were later transferred to accounts opened with the same bank for the new Belgium companies	Unknown	Yes judicial financial fiscal experts	1) Offshore centre (unknown is the type of company that is established and the jurisdiction in which the companies are set up)	Money flow from various foreign companies to Belgium companies Subsequently money flow from Belgium to various individuals abroad including the original shareholder.	1) multi jurisdictional structure 2) dissolvement after creating new companies 3) money flows without clear connection to activities of company	Disclosure by bank to FIU. There was no economic justification for transactions	1) Tax fraud 2) Money laundering	1, 2 Placement and layering	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
6	Mr C was an accountant that started his own accounting and financial services, N in Panama. He advertised his services primarily on the internet and through mass mailings. N provided a variety of services including the following: formation of offshore entities shelf corporations (trust, foundations and corporations to disguise ownership of assets; passports and dual citizenship, mostly using new nominee names; movement of cash and other assets offshore and back onshore using various methods; issuance of debit cards for the purpose of anonymously repatriating and spending offshore funds; use of correspondent bank accounts to skim profits of legitimate businesses and repatriate funds through the purchase of assets and use of debit cards; anonymous trading of securities through accounts with two major brokerage houses; false invoicing-re-invoicing schemes to support fraudulent deductions on tax returns; false investment losses, to disguise transfer of funds overseas. C was identified pursuant to an IRS-CI investigation of one of his clients for illegal importation and sale of goods. The targets of this investigation were using a re-invoicing scheme devised by C to illegally import these chemicals into the U.S. for sale. C assisted the targets in the re-invoicing scheme by preparing the invoices, receiving the proceeds of the scheme and hiding the proceeds in a myriad of Panamanian Corporations for later use by the targets. As a result of this investigation, C became a subject investigation for the formation of illegal trusts to facilitate money laundering and other crimes. The investigation disclosed that L had about 300-400 active clients/investors. The investigation also disclosed that it created between	2000-2003?	C was an accountant	1) foreign trusts (unknown is the type of Trust and the jurisdiction in which the Trusts were established 2) Panamanian corporations (unknown is the type of corporation) 3) foundations (unknown is the jurisdiction in which the foundations were established)	N was seated in Panama and advertised its services primarily via the internet and through mass mailings.					

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
	5.000-10.000 entities for these clients, including the layering of foreign trusts, foundations and underlying business corporations, which were formed in offshore countries.									

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
7	Mr. B and his associate bought insurance companies. The assets of these companies were drained and used for personal benefits. The draining of the assets was concealed by transferring them into accounts in and out of the U.S. via wire transfers. The first step in the scheme was establishing a Trust in the U.S. B concealed his involvement and control of the Trust through the use of nominees as the grantors and trustee .B used the Trust to purchase the insurance companies. Immediately after the acquisition, B would transfer million of dollars of reserve assets to a corporation he set up in the U.S. The funds were then wire transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, B used them to pay for his personal expenses.	Unknown during 9 years	Feasible but not specifically described	1) trust in the U.S.(unknown is the type of Trust and the jurisdiction or state in which the Trust was established) 2) corporation in the U.S.(unknown is the type of corporation and the jurisdiction in which the corporation was established) 3) another corporation with an offshore bank account (which type of corporation and in which jurisdiction the corporation	Mr. B used a U.S. trust to purchase insurance companies (unknown in which jurisdiction) and subsequently transferred millions of dollars of reserve assets to a corporation in the U.S.	1) use of structure, trust and shell companies to realize scheme 2) use of structure to conceal identity 3) use of nominees to conceal identity	IRS	1) wire fraud 2) money laundering 3) racketeering influenced corrupt organisation (RICO) 4) RICO conspiracy 5) securities fraud	1 Placement	Total restitution ordered by the court was approximately USD 400 million
8	Beginning in 1997, Mr D assisted his clients with various schemes to hide income and assets from the IRS, including a method by which an individual used 'common used trusts' to conceal ownership and control of assets and income and the use of offshore trusts with related bank accounts in which the assets would be repatriated through the use of a debit card. D also set up international business corporations (IBC) that had no independent economic reality and did not represent actual ongoing business concerns, on behalf of his clients, to conceal the clients´ assets and income from the IRS. Concerning his own liabilities, D opened and maintained nominee bank accounts	1997-2001	Tax advisor	1) trusts 2) international business corporations (IBC) (unknown in which jurisdiction the IBC was established) 3) offshore trusts (unknown is the type of Trust and the jurisdiction in which the Trusts were established	The actual activities took place in the U.S.	1) use of trusts and corporations to conceal identity 2) use of nominee bank accounts to conceal identity	IRS	1) criminal tax fraud 2) wire fraud	1 Placement	D admitted that between 1998 and 201, he was paid USD 281.890 in income and then directed those payment

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
	both in the U.S. and abroad to conceal his income from the IRS.									s to nominee bank accounts primarily set up in foreign countries .
9	Mr. E a CEO of a local telecommunication company received corrupt money of RM 300.000 as an inducement to award supply and work worth RM 5.0 million to company P, which belongs to Mr. F. Mr. F paid the corrupt money as a payment by company P to company Q for services rendered. Company Q also belongs to Mr. F, but was merely a dormant and shell company with RM 2.00 paid up capital. The money was later withdrawn from company Q and placed in a stock-broking firm under the name of Mr. G., a nominee of Mr. E, who opened an account with the same stock broking company using his son´s name. The money in G.´s account was used to purchase shares in the open market and later sold to Mr. E´s son using numerous married deal transactions whereby the shares were later sold by Mr. E´s son in the open market at a higher price. Capital gains subsequently were used to open fixed deposits. Sign up for a insurance policy (under the name of Mr. E) as well as purchase assets in the name of Mr. E´s relatives.	Unknown	Feasible but not specifically described.	1) Company P and Q. (unknown which type of company and in which jurisdiction these companies were established)	The activities of the companies took place in Malaysia. The purchase of shares in the open market took place via a stock broking firm seated in Malaysia	1) use of corporate structure for hiding of payments 2) conceal of identity by nominees (Mr. E´s son and Mr. G.)	Unknown	1) corruption	4 Investment	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
10	Individual B, a foreigner without an address in Belgium set up a company X for buying and selling real estate. The company was set up by Notary A. The sole manager and shareholder of this company was a family member of B, who also resided abroad. Shortly after its creation the company bought property in Belgium. The property was paid on the account of notary A by means of several transfers, not from company X, but form another foreign company about B B did not provide any details.	Unknown	Yes Notary	1) Belgium (unknown is the type of company that was established) 2) foreign (unknown in which jurisdiction the company was established)	Shortly after incorporation company X bought a property in Belgium. The property was paid by means of several transfers not by company X, but by another foreign company The sole manager and shareholder of this company was a family member of B, who also resided abroad B. was known by Police for financial fraud	1) multi jurisdictional structure 2) payment by foreign company without clear connection to company X nor clear connection between the two companies involved 3) incorporation of a company by a non-resident with no links nor activities in jurisdiction where the company is established 4) the company´s sole manager and shareholder	Notary in Belgium filed STR	1) financial fraud 2) money laundering	4 Investment (possibly phase3, if payment was made by way of a loan)	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
11	Individual A, a foreign national without an address in Belgium, but manager of company X established in Belgium was active in the sector of household appliances. A held several bank accounts in the Middle East. A had substantial cash deposits in various foreign currencies. One of the accounts was credited by a transfer from a tax haven by order of individual B. Immediately afterwards, A. requested to transfer funds to an account of company X meant for the creation of new capital. The CTIF-CFI in Belgium received a request for information from a FIU in the Middle East.	Unknown	Unknown	1) Belgium (unknown is the type of company that was established)	Several substantial deposits in various foreign currencies were made and one of the bank accounts in the Middle East was credited by a transfer from a tax haven by order of B Subsequently the money was transferred to an account of company X in Belgium.	1) multi jurisdictional structure 2) incorporation of a company by a foreign national without an address in land of incorporation of the company 3) international money flows without clear connection to the activities of company 4) cash deposits in foreign currencies without link to company X (household appliances)	CTIF/CFI received request for information from FIU in Middle East	Suspicion that company X laundered the assets of international trade in cigarettes	1.2 Placement and layering	Unknown
12	A foreign citizen residing in Belgium opened a bank account. Immediately afterwards the account was credited by a very substantial transfer from a lawyer´s office in North America. This amount was the result of the closing of the account in the name of a trust. The individual requested to withdraw this amount in cash.	Unknown	Yes lawyer in US (unknown which state)	1) US trust (unknown which type of trust and in which state the trust was established)	Bank account in Belgium was credited by a very substantial amount from the U.S. (unknown from which state). This amount was the result of the closing the account in the name of a trust Individual wanted to withdraw the amount	1) conceal identity of the beneficial owner by using a foreign trust.	Bank in Belgium filed the STR and opposed to the withdrawal.	Money laundering suspicion	1 Placement	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
13	Companies B1 en B2 were registered in the BVI. Both companies had opened several accounts at Bank A in France. The balance on the bank accounts amounted to approximately EUR 3 million. Half of these amounts were used to secure a loan. Companies B1 and B2 were managed by a foreign registered Trustee C. licensed by the Guernsey FSC. The French banking commission fined Bank A for breach of the obligation to identify the beneficial owner.	Unknown	Yes Trustees C licensed by the Guernsey FSC.	1) British Virgin Islands (BVI) (unknown which type of companies were established)	Bank accounts in France totalled approximately EUR 3 million, half of which was secured by a loan. The French banking commission considered that Bank A had not gathered convincing documents to verify the identity of the ultimate beneficial owner(s) of companies and legal arrangements in BVI, Bahamas	1) conceal identity of the beneficial owner through structure of corporate entities and trusts and international money flow	French banking commission fined a bank for breach of the obligation to identify the beneficial owner (on-site visit)	Breach of French law	no ML	Unknown
14	Company L registered in Liberia, borrowed funds from Bank B for the purchase of a ship. Company L acquired the ship financed and gave it in guarantee of the loan. The register of Lloyd´s insurances mentioned the name of company L under the name of company M without any other details, implying that company M manages company L. During investigations, it was established that the interlocutor of the bank was Mr. J. who was supposed to be the beneficial owner of company M, but the bank did not have any document attesting this information. The shares of company O were held 50% by company P and 50% by company Q. Mr. J. was allegedly the beneficial owner of company Q and one of his associates was supposed to be the beneficial owner of company P. Mr. J. negotiated the terms of the loan.	Unknown	Lawyers and legal advisors	1) Three companies were established in Liberia (unknown which type of companies were established) 2) Companies M, P and Q (unknown which type of companies and in which jurisdiction these companies were established)	Company L seated in Liberia was used to purchase a ship by obtaining a loan from Bank B, seated in France and gave it in guarantee of a loan.	1) conceal identity of the beneficial owner through structure of foreign companies(with possibility to issue bearer shares, articles of associations or financial statements in which the shareholders or capital owners are not mentioned)	Investigation of French banking commission.	Breach of French law	no ML	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
15	Bank B gathered the 'Certificate of Incorporation' of its Delaware customer company N and later obtained information about the 100% shareholder Delaware Corporation O. The incorporation documents did not give details about the real beneficiaries. There was no other document related to the capital structure and the shareholders. Bank B provided a loan to Single purpose company N in Liberia to facilitate a plane lease construction in which the single purpose company N holds the head lease and trust holds the sublease. The airline companies paid rentals for the sub lease to the trustee. U.S. Holding holds 100% of the shares in the airline leasing companies and another special purpose company (owner at the reimbursement term).	Unknown	Feasible but not specifically described.	1) Two Delaware companies (unknown which type of companies were established)2) US holding company (unknown which type of company and in which state the company was established) 3) Trust(ee)(unknown which type of trust and in which jurisdiction the trust was established and who acts as trustee in this case) 4) Airline leasing companies (unknown which type of companies and in which jurisdiction these companies were established)	The loan was provided by a bank in France. Airline leasing companies paid rentals for sub lease the Trustee. The Trustee paid Single purpose company N in Delaware for the head lease. It seems that company N paid the interest and/or repayments on the French bank loan.	1) conceal identity of the beneficial owner through structure of a trust and foreign companies	Investigation of French banking commission	Breach of French law (AML law)	Unknown	EUR 1.000.000
16	Between the years 2000-2002, a gang of robbers carried out robberies at private and public premises. The robbers' main targets were the jeweler and pawnshops throughout Malaysia. During this period, the total haulage of ill-gotten proceeds was laundered by acquiring various types of businesses such as seafood restaurants, car accessories, and electrical shops. The bulk of the laundered proceeds were invested in jeweler	2000-2002	Unknown	1) Various Malaysian businesses were purchased (type of company, if any, is unknown)	The activities of these businesses took place in Malaysia.	1) use of businesses or one-man businesses to launder money by way of increasing fictitious turnover of these business or one-man	Investigation by the police.	1) robbery 2) breach of AML law	3 Justification	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
	business.					businesses				
17	The case relates to three fraudulent wire transfers from Miami to Mauritius and the funds were thereafter transferred to Sri Lanka, Hong Kong, India, USA and Panama A limited company A operating in the textile sector exports mainly to the USA. Its Board of Directors consists of an Indian national based in Sri Lanka, a Mauritius national, and a sister company B seated in Sri Lanka. A Miami bank received three requests by fax to debit the accounts of Mr. N., a client based in Venezuela and operating in cosmetics through his company C. and credited accounts of A a bank in Mauritius for an amount of USD 1,8 million. The Mauritius bank received three requests from their correspondent bank HSBC in New York for cancellation of the payment orders to A s they were sent in error. Delphis bank requested A to authorise for reversal of the payment order. However the funds were transferred to other bank accounts in Sri Lanka, India, Panama and Hong Kong. It seems that Mr. N. agreed A not to produce the goods. The goods were manufactured by B in Sri Lanka, but since there is exchange control regulation in Sri Lanka and Mauritius has offshore facilities the remittances were made to A in Mauritius. The documents that witnessed the export of textile to Venezuela were forged and improper.	2001-2004	Unknown	1) Mauritius (limited company) 2) Sri Lanka (unknown is type of company) 3) Company C(unknown is type of company and jurisdiction in which this company was established)	The goods were manufactured in Sri Lanka. In order to avoid exchange control regulation, the goods were pretended to be manufactured in Mauritius. The goods were sold to Mr. N in Venezuela, who paid by means of a wire transfer to a company incorporated in Mauritius (not Sri Lanka). The funds were thereafter transferred to Sri Lanka, Hong Kong, India, USA and Panama. Mauritius has offshore facilities.	1) multi jurisdictional structure to evade exchange control and taxes in Sri Lanka 2) false documents also to evade exchange control and taxes in Sri Lanka. 3) management of a company in Mauritius consists of at least one non-resident person.	Investigation by the police	1) forgery	no ML	Each director of A was fined to pay Rs. 1 million plus Rs 500 costs in 2004

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
18	Investment of Russian funds, presumably criminal funds in real estate in Amsterdam. Company C was incorporated in the Netherlands. Its shareholder was Company D, on Curacao A local carpenter acted as director in the Dutch limited liability company C. Another company, E, on Curacao provided a loan to Company D in the Netherlands in several tranches. The loan turned out to be not secured in favour of E and interest was not paid but accrued. The terms of the loan seem not businesslike. A TCSP in the Antilles acted as director in both companies D and E. C invested the money in real estate in Amsterdam. The UBO is only known by the TCSP in the Antilles.	1997-2002	Yes Tax advisor Notary	1) Two Netherlands Antilles N.V.´s 2) Dutch limited liability company (B.V.) purchased real estate via a notary.	Investment of Russian funds, presumably criminal funds in real estate in the Netherlands. A loan was provided by E to the Dutch B.V.	1) conceal identity of the beneficial owner through structure of foreign companies 2) management of a real estate company by a strawman 3) Loan back structure (loan was provided by a foreign allegedly non-related company. However in fact it concerns a company owned and controlled by the same beneficiary) 4) The terms of the loan were not businesslike.	Investigation by fiscal intelligence service-economic control service FIOD/ECD	1) breach of AML law 2) falsification of documents 3) tax fraud	3.4 Justification and investment	Unknown
19	English limited companies used in VAT-schemes. The difference between the legal systems in the Netherlands and England is being used to deduct taxes. According to English law the company is dissolved, whereas in the company lives on for VAT tax-purposes in the Netherlands and can file VAT returns claiming input tax. Since the company is dissolved in England there is no beneficial owner causing legal problems in addressing claims according to Dutch tax and corporate law. Investigation revealed the destination of money,	unknown	unknown	1) English limited liability companies incorporated and then dissolved	In the Netherlands the same English limited liability companies live on en file fraudulent VAT- tax returns.	1) incorporation of an U.K. limited liability company by a foreigner, with no link nor activities in the jurisdiction where the company is established.	Investigation by fiscal intelligence service-economic control service FIOD/ECD.	1) tax fraud 2) falsification of documents	1 Placement	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
	but turned out to be out of reach for the Dutch authorities.									
20	At the end of the 90s, a European telecommunication group X asked a Swiss lawyer Y, to construct a specific payment system. The purpose is to transfer bribes to influential persons in emerging markets abroad. X received important orders to establish the mobile network in these countries. The lawyer Y used a number of corporate vehicles to veil the connection between X and the recipients of the bribes. Y opened bank accounts in the name of every company at several banks in Switzerland and opened bank accounts in their own names which were specifically to be used for bribes to easy the decision-making process for foreign administration officials/lobbyists. X credited the accounts with explanations as market studies, support international trade etc. In may 2002 the frequent large cash withdrawals attracted the attention of one of the banks in the canton of Zurich. STR´s were filed.	End of 90s till June 2003	Mr. Y. is a lawyer	1) Several Swiss companies (unknown is the type of companies that were established)	The activities of a number of corporate vehicles probably took place in Switzerland.	1) use of multi jurisdictional structure to divert the payments	Bank in canton of Zürich filed STR´s	1) bribery	1 Placement	Maybe disciplinary measures against lawyer Y Investigation still open: almost CHF 550 million flowed through corporate vehicles

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
21	Two US citizens formed a LLC, which was an independent venture capital firm but was secretly controlled by the two US citizens in violation of the State´s order. At order of L. direction M. created a number of shell companies and bank accounts in the Caribbean island of Nevis for himself and other defendants. M. used these Nevis companies to funnel money offshore by submitting fraudulent stock subscription agreements and financial statements of the Nevis companies, to make it appear that the LLC had wealthy backers and lines of credit. The LLC fraudently raised USD 12 million from investors. In total securities with a value over USD 90 million were offered and sold.	2001-2002	No	1) LLC (a venture capital firm) in the U.S. 2) Nevis shell companies (unknown are the type of companies which were established)	The LLC in the U.S. fraudently raised millions from U.S. investors.	1) use of multi jurisdictional structure to divert the payments 2) conceal identity by using Nevada and Nevis companies 3) use of offshore bank accounts	IRS	1) conspiracy 2) mail fraud In 2004 M. was sentenced to four years in prison to be followed by 3 years of supervised release with restrictive financial/employment conditions	1 Placement	In total a value of securities worth USD 90 million were offered/sold
22	A US citizen, Mr. H operated two Nevada corporations doing business in Idaho Falls. Approximately 100 clients invested a total of USD 1.7 million on the promise of a good return and minimal risk through day trading. However, H did not do the trading he promised, but diverted much of the money to his own personal use. To keep the investments coming in H prepared monthly statements for each investor, falsely representing that he engaged in day trading on a regular basis.	2004	No	1) Two Nevada corporations (unknown are the type of companies which were established)	The activities took place in Idaho Falls in the U.S	1) use of multi jurisdictional structure to divert the payments (between U.S. states) 2) conceal identity by using Nevada companies	IRS	mail fraud In 2005 H was sentenced to 37 months in prison to be followed by 3 years supervised release	1 Placement	Total loss was for investors more than USD 1.2 million H was sentenced to pay USD 1.2 million in restitution to the victims

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
23	Mr. J, an attorney made false statements in support of a bank loan application in the Springfield area from 1973 until his disbarment in 2000. J induced a number of individuals to invest funds with him through company T by false and fraudulent pretences. J claimed that T was engaged in the business of factoring accounts receivable in the trucking industry and that there was little or no risk of loss of investment. However J did not invest the funds. Instead he used the money to make periodic payments representing return of their investment. J converted more than USD 1 million for his own use.	1973-2000	Mr. J is an attorney	1) Company T was established in the U.S. 2) Bank loan application was filed in the Springfield area in the U.S.	Mr. J defrauded numerous investors through an investment scheme, whereby used part of the invested money for his own use and part of the invested money to make periodic payments representing return on investment.	1) use of multi jurisdictional structure to divert the payments 2) conceal identity 3) use of false 'loan' documents.	IRS	1) money laundering 2) defrauding more than USD 1,6 million from his clients and others through an investment scheme 3) false tax returns 4) false statements in support of a bank loan application.	1 Placement	Total loss admitted by Love amounts to USD 158.152. Love was sentenced to 108 months in prison and ordered to pay USD 2.442.564 in restitution.
24	Mr. K a tax attorney was arrested in Madagascar after fleeing the U.S. K set up/advised a scheme for a client to defeat the assessment of income taxes on the sale of a company by confusing the nature of the capital gain. K conspired with the client to establish a complicated series of transactions involving shell corporations, limited partnerships, trusts and sham corporate executives.	1996-2004	Mr. K is a tax attorney	1) Various shell corporations, limited partnerships, trusts were established. (unknown which type of corporation and trust and in which jurisdiction)	Violations took place in the state of Michigan in the U.S.	1) use of multi jurisdictional structure to divert the payments 2) conceal identity (sham executives) 3) falsification of documents (backdating)	IRS	1) mail fraud 2) money laundering 3) tax fraud 4) theft of property violations 5) falsification of documents (backdating)	1 Placement	This sham resulted in the reporting to the IRS the sale of the company to be USD 2,8 million whereas the actual selling

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
										price was USD 9,8 million.
25	Mr. L claimed to have invented a revolutionary new software program that could compress huge amounts of data and transmit the compressed data over standard telephone lines. L sold or licensed the software to three different investment groups, receiving about USD 12,5 million from investors, but never delivered the product to any of the groups.	2001-2005	No	1) Shell corporations in various states in the U.S. L used numerous identities across the U.S.	Activities took place in various states in the U.S. (from Florida to Ohio, to California, to Texas and then to Colorado)	1) use of multi jurisdictional structure to divert the payments 2) use of structure to conceal identity	IRS	1) wire fraud 2) bank fraud 3) money laundering Mr. L was sentenced to 480 months/40 years in prison on April 27, 2005	1 Placement	Damage USD 13,5 million.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
26	On April, 19, 2005, in New York, Mr. M was sentenced to 96 months in prison, was amongst others ordered to pay USD 106 million in restitution to the creditors he defrauded. M was convicted of conspiring to defraud, and defrauding, his creditors and income tax evasion based on his receipt of over USD 25 million he never reported to the IRS. M and his partner N built a series of companies by borrowing hundreds of millions of dollars from and through various financial institutions and personally guaranteed many of the loans. After failing to repay the loans, M and N put into place a restructuring plan pursuant to which they signed deficiency notes making themselves personal liable to their creditors for approximately USD 100 million. Around the same time they were signing deficiency notes, M and N sold Company A to Company B in a deal that allowed M and N to earn shares of B. Pursuant to the agreement M and N with the assistance of others pulled off a massive fraud involving falsely representing to their creditors that they were broke and could not repay the notes and duping the creditors that held the notes, at a steep discount, to purportedly unrelated third parties who were in fact sham entities controlled and funded by M and N. During the scheme the identity of M and N remained unknown.	2002-2004	unknown	1) A series of companies (unknown is the type of companies and the state in which they were established)	unknown	1) use of structure to realize scheme 2) use of structure to conceal identity	IRS	1) bank fraud 2) tax evasion	1 Placement	On April 19, 2005 Hundley was sentenced to 96 months/ 8years in prison, ordered to pay USD 106 million in restitution to the creditors he defrauded and USD 5,4 million in restitution to the IRS The judge also entered a forfeiture order USD 44 million allowing the U.S. to seize assets of M.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
27	O owned eight residential apartment complexes, which contained more than 400 rental units. O along with his wife conspired to hide owner-ship of the rental units, so they could conceal the income from the rental units and avoid paying taxes. O transferred ownership of the apartments to sham entities, which they called Unincorporated Business Organisations (UBO) and opened more than 40 bank accounts with signature authority in their own names or nominees. O and his wife advised their accountant that they had no income from the apartments because, having transferred the rentals to the UBO, they no longer owned the rentals. They then filed false tax returns, failing to report the income.	2002-2004	Feasible but not specifically described	1) sham entities which were called Unincorporated Business Organisations (UBO). (unknown which type of corporation) O was sentenced in Salt Lake City.	The actual activities took place in the U.S. (unknown in which state the activities took place)	1) use structure to realize scheme 2) use of structure to conceal identity 3) use of nominees to conceal identity	IRS	1) conspiracy 2) tax evasion 3) bankruptcy fraud	1 Placement	During the years of the conspiracy O failed to pay more than USD 5 million in federal taxes. On June 22, 2005 O was sentenced to serve 100 months in federal prison to be followed by three years of supervised release. In addition O was ordered to file accurate tax

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
										returns with 18 months of his sentencing
28	Mr P invented a wheel-locking device to be used on four-wheel drive off-road vehicles. After forming a company to market his product, he sold the company for USD 1.008.000,-. P failed to file a tax return that reported any of the funds generated by the sale, nor did he pay any taxes on the income. Instead, he placed the funds into offshore bank accounts, used bank accounts in the names of other persons and entities, and conducted financial transactions using large amounts of cash. The loan fraud conviction was based on the submission of a false employment letter in connection with a loan application to purchase a house.	2002/2004	Feasible but not specifically described	1) company (unknown which type of company and in which jurisdiction the company was established) 2) entities (unknown which type of entities and in which jurisdiction the entities were established)	The activities took place in various states of the U.S.	1) use structure to realize scheme 2) use of structure to conceal identity 3) use of nominees to conceal identity 4) use of offshore bank accounts	IRS	1) tax evasion 2) loan fraud 3) structuring cash transactions to avoid federal reporting requirements	1.4 Placement and investment	P owes USD 264.335 in back taxes. On January 31, 2005 P was sentenced to 33 months in prison. In San Diego county, on January 31, P was sentenced to 33 months in prison.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
29	Between November 1998 and March 1999, at least 13 lenders sent a total of USD 1,760.000 by means of wire transfers to Anguila in the name of Company Q. During 1998 and 1999, Mr. A the founder and the director of two companies, Q in Anguilla, British West Indies and R In the state of Missouri, induced individuals to lend money to the company in Missouri, for a period of one year and one month and promised to pay interest to such lenders at 120 percent per year. A represented to the lenders that all of the money was to be used to purchase U.S. bonds or other comparable obligations and that all of their money would be insured. In addition A told the lenders that the government bonds or other obligations purchased were to be used as collateral to obtain more money to be used to trade financial instruments in order to generate profits to repay the loans and earn interest.	1998-2005	Unknown	1) Company Q was established in Anguila (BWI) 2) Company R was established in the state of Missouri in the U.S.	U.S. Investors invested their money in U.S. bonds with a '120 percent' return per year.	1) use structure to realize scheme 2) use of structure to conceal identity	IRS	1) wire fraud 2) money laundering	1 Placement	On June 17, in St. Louis Mr. A was sentenced to 51 months in prison for wire fraud and money laundering and ordered to pay USD 2.070.000 in restitution.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
30	A was a TCSP that operated from California in the late 1990. In order to help clients commit money laundering and tax evasion, he assisted them in purchasing banks offshore. Two of his clients, D and K, were committing investment (securities) fraud stealing millions of dollars from their clients. A helped them to set up a bank X that maintained a corresponding account at another bank in Liechtenstein for USD 25.000. Shortly after opening this account A set up an account at another bank Y in Liechtenstein. Monies from Bank X were wired to this account. During the period December 1, 1998 - February 5, 1999 approximately 2 months, D and K defrauded clients of approximately USD 8 million, that were deposited in to the account in Bank Y. However, Sexton convinced D and K to give a Power of Attorney to withdraw over USD 2 million and divert to another bank account that he controlled in Liechtenstein. Funds were then removed from this account and transferred to a trust A set up in the U.S. A then used these funds to pay for his personal expenses including purchase of a condominium in Austria, renovating a hotel he owned in California, purchase of a boat, among other items.	1998-1999	TCSP	1) Bank X (unknown in which jurisdiction the bank was incorporated)	The activities took place in the U.S. (unknown in which state)	1) use of trusts to conceal the identity 2) use of trusts to divert the money flow 3) use of offshore bank account (jurisdiction with bank secrecy law)	Liechtenstein bank contacted law enforcement agency	1) mail fraud 2) wire fraud 3) money laundering 4) conspiracy	1.2 Placement and layering	D and K defrauded clients of USD 8 million.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
31	Mr X was a TCSP that co-founded an organisation Z that sold audiotapes, CD´s and tickets to offshore seminars on "wealth building" strategies. This firm and its vendors conducted seminars which promoted bogus trust packages and other schemes advocating fraudulent methods of eliminating a person´s income tax liability. Z allegedly received more than USD 40 million from selling the so-called "wealth building" products and tickets to the offshore seminars. The defendants were charged with concealing income they earned from the sale of Z products, in part by using bogus trusts, nominee entities and offshore bank accounts, into which they deposited portions of their profits. They also allegedly transferred funds from the offshore bank accounts back into the U.S. through wire transfers and the use of debit cards. All of Mr. X´s co-defendants have pleaded guilty to tax crimes in the Western District of Washington. All four defendants face sentencing on April 10, 2006 in Seattle.	1996-2002	TSCP	1) Corporation Z (unknown in which jurisdiction the corporation was established)	The tax crimes took place in the state Washington in the U.S.	1) use of corporation to realize scheme 2) use of trusts, corporations and offshore bank accounts to divert money flow 3) use of trusts, corporations to conceal identity 4) use of offshore bank accounts	IRS	1) charged in a superseding indictment with additional counts of tax evasion; conspiring to defraud the IRS.	2 Layering	If convicted, Mr. X faces a maximum potential sentence of 20 years in jail and USD 1 million in fines.
32	In August 1995, Mr. and Mrs. A sold 20 acres of property for USD 3,1 million. They tried to evade paying federal taxes with the use of sham trusts which were lacking economic substance. One day prior to the sale, Mr and Mrs. A transferred ownership of the property to a trust for "USD 10 and some shares", where they along with one of their sons, were the trustees with complete control of the assets. Mr. and Mrs. A also created another trust, just five days prior to the closing of the sale, along with a bank account, which was used to deposit the sales proceeds of the property. The majority of the money was later transferred into a Barclays bank account located offshore in the Cayman Islands, still under complete control of Mr	1995-2005	Unknown	1) trusts (unknown which type of trust and the jurisdiction in which the trust is established)	The activities took place in the U.S. (unknown in which state or jurisdiction) The majority of the sale proceeds was transferred to a bank account on the Cayman Islands	1) use of trusts to realize scheme 2) use of trusts to conceal identity 3) use of trusts to divert the money flow 4) use of offshore bank accounts	IRS	1) tax fraud	1.2 Placement and layering	Unknown

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
	& Mrs A. Over the years, Mr. and Mrs. A used some of the money for their personal benefit, including the purchase of their own residence for USD 168.000 "ownership" of which was put into another sham trust.									
33	Mr. M and Mr. N marketed trust packages through a Tacoma-based organisation. The defendants advised customers that they could avoid paying taxes if they placed their income and assets in a "pure equity trusts", even though the customers retained control over the use of the income and assets they placed into the trusts. The defendants promoted the scheme through seminars, a website and booklets.	1994-2006	Unknown	1) pure equity trusts (unknown is the type of Trust and the jurisdiction or state in which the Trusts were established) 2) unknown in which state/ jurisdiction this company was established.	Unknown in which jurisdiction/state the business was active. The defendants promoted the scheme through seminars, a website, and a website and booklets.	1) use of trust to realize scheme	IRS	1) tax fraud	1 Placement	The defendants promoted the scheme and received over USD 2 million in revenue from the sales of more than 400 trusts, charging customers approxim

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
										ately USD 5.000 - 7.500 for the trust packages .
34	Mr. P routed his clients' income through bank accounts in the names of trusts located in the U.S. and abroad in order to conceal their income from the IRS. P admitted in his guilty plea that his clients, all medical doctors from Northern California - begin using his tax evasion system to cycle income from their medical practices through domestic and foreign bank accounts in an effort to conceal their funds from the IRS. P charged a fee for running client income through the system of bank accounts and then back to an account controlled by the client. P's clients then filed federal income tax returns without disclosing the income that had been routed through the offshore accounts.	? - 2002	Yes tax advisor	1) trusts in the U.S. (unknown is the type of Trust and the jurisdiction or state in which the Trusts were established)	Use of U.S. trusts and foreign bank accounts to route and conceal funds from the IRS. Unknown in which jurisdiction the bank accounts were opened.	1) use of trust to realize scheme 2) use of foreign bank accounts	IRS	1) tax evasion and fraud	1 Placement	Mr. P was ordered to pay a fine of USD 67.500 and to serve a three-year term of supervised release after prison. P clients have been sentenced for their participation in the scheme.

No	Short description	Time	Experts involved	Jurisdiction of incorporation	Jurisdiction where the actual activities take place	Similar fashion (typology)	Case ID via	Offence(s)	ML phase	Amount (fine/damage)
35	Mr. X, a CEO of a local telecommunication company received corrupt money of RM 300.000 as an inducement to award supply and work worth RM 5.0 million to company A, which belongs to Mr. Y. Mr. Y paid the corrupt money as a payment by company A to company B for services rendered. Company B also belongs to Mr. Y, but was merely a dormant and shell company with RM 2.00 paid up capital. The money was later withdrawn from company B and placed in a stock-broking firm under the name of Mr. W., a nominee of Mr. X, who opened an account with the same stock broking company using his son's name. The money in W.´s account was used to purchase shares in the open market and later sold to Mr. X´s son using numerous married deal. The married deal transactions whereby the shares were later sold by Mr. X´s son in the open market at a higher price. Capital gains subsequently were used to open fixed deposits. Sign up for a insurance policy (under the name of Mr. X) as well as purchase assets in the name of Mr. X´s relatives.	unknown	Feasible but not specifically described.	1) Company A and B. (unknown which type of company and in which jurisdiction these companies were established)	The activities of the companies took place in Malaysia. The purchase of shares in the open market took place via a stock broking firm seated in Malaysia	1) use of corporate structure for hiding of payments 2) conceal of identity by nominees (Mr. X´s son and Mr. W.)	Unknown	1) corruption	4 Investment	Unknown

Annex 5 Findings Drawn from other Source Material

There is extensive source material that reinforces the findings drawn from the typologies. The following extracts are taken from some of the key sources referred to in the Bibliography -

1. Behind the Corporate Veil – OECD Report (2001)

Page 8 - "In essence, any jurisdiction that provides mechanisms enabling individuals to successfully hide their identity behind a corporate vehicle while excessively constraining the capacity of authorities to obtain and share information on beneficial ownership and control for regulatory/supervisory and law enforcement purposes is increasing the vulnerability of its corporate vehicles to misuse. Certain jurisdictions allow corporate vehicles established in their jurisdictions to use instruments that obscure beneficial ownership and control, such as bearer shares, nominee shareholders, nominee directors, "corporate" directors, flee clauses, and letters of wishes, without devising effective mechanisms that enable the authorities to identify the true owners and controllers when illicit activity is suspected or to fulfil their regulatory/supervisory responsibilities. Some of these jurisdictions further protect anonymity by enacting strict bank and corporate secrecy laws that prohibit company registrars, financial institutions, lawyers, accountants, and others, under the threat of civil and criminal sanctions, from disclosing any information regarding beneficial ownership and control to regulatory/supervisory and law enforcement authorities."

Page 8 - "In order to successfully combat and prevent the misuse of corporate vehicles for illicit purposes, it is essential that all jurisdictions establish effective mechanisms that enable their authorities to obtain, on a timely basis, information on the beneficial ownership and control of corporate vehicles established in their own jurisdictions for the purpose of investigating illicit activities, fulfilling their regulatory/supervisory functions, and sharing such information with other authorities domestically and internationally."

Page 41/42 – "A number of factors influence the choice of mechanism for obtaining information on beneficial ownership and control, including the nature of business activity in a jurisdiction, the extent and character of non-resident ownership, corporate regulatory regime, existing anti-money laundering laws, powers and capacity of supervisors and law enforcement authorities to obtain beneficial ownership and control information, functioning of the judicial system, and availability of anonymity instruments. In addition, policy makers must find an appropriate balance between ensuring proper monitoring/regulation of corporate vehicles and protecting legitimate privacy interests. In jurisdictions with a substantial domestic commercial sector and where existing investigative mechanisms function well, policy makers must also take into account the risk that an extensive up-front disclosure system may impose unnecessary costs or burdens on corporate vehicles, particularly smaller enterprises."

2. Transparency and Money Laundering – Savona Report (2001).

Page 76 – the thematic area "incorporation" –

"The incorporation is the initial phase in the "life" of a legal and non-legal structure, in which the structure itself is established through a series of acts aimed at making it operational. The relevance of this thematic area for anti-money laundering international cooperation lies in the fact that lack of checks during the incorporation phase results in greater opacity in company law, which might obstruct the acquisition of information regarding the physical persons participating in its establishment. The less opaque (or the more transparent) the process of incorporation is, the more available should be the information concerning the incorporation of the structures. This facilitates investigation of their activities and of the persons controlling them, both at the national and at the international levels".

Page 79 - The thematic area "company activity" –

"The area of "company activity" refers to the activities of an operative legal and non-legal structure aimed at achieving its economic or patrimonial goal.

This area is relevant for anti-money laundering international cooperation because lack of checks on the activities of the company increases the opacity in company law and makes it difficult to monitor its behaviour and exchange this information with other foreign authorities. The greater the possibility is of gaining information on the management and on the activities of a structure, the more the names of shareholders are accessible to other parties.

The more closely accounts are audited, and the greater the obligation to disclose relevant information, the more information concerning the activities of structures is available to the law enforcement, judiciary and financial authorities to be exchanged, when necessary, with their counterparts for anti-money laundering purposes".

Page 82 – the thematic area "identification of the real beneficial owner" –

"The area "identification of the real beneficial owner" refers to those rules aimed at identifying the person/s who are actually in control of a structure and its activities.

In this thematic area, the opacity created by the impossibility of ascertaining the identity of the shareholders and establishing a connection between a structure and a physical person/s running it, obstructs effective investigation at the national and transnational levels.

Page 125 –

"The results illustrate that the greatest obstacles to anti-money laundering international cooperation are to be found in the thematic area "identification of the real beneficial owner"…. The main obstacle is lack of regulation requiring full information on the real beneficial owner of a public or private limited company, especially when a legal entity is a shareholder or director, or the issuance of bearer shares is permitted".

"The thematic area "incorporation" also presents obstacles to anti-money laundering international cooperation, even though at a lower degree than the former. Lack of regulation in this area makes it more difficult to acquire information of physical persons party to the creation of legal structures and increases the possibility that these might be used for criminal purposes".

"The analysis of regulation covering trusts has shown it has been characterised by great opacity and absent of all those provisions relevant for anti-money laundering international cooperation. Their regulation and the confidentiality of their constitution hinder the gathering of information on the people setting them up and of that management structure. This opacity creates obstacles to anti-money laundering international cooperation because of the lengthy process in getting information."

3. OECD, Template; Options for Obtaining Beneficial Ownership and Control Information (September 2002)

This OECD template, developed by an expert group under the authority of the OECD Steering Group on Corporate Governance, outlines three options for obtaining beneficial ownership and control information and provides a diagnostic tool to assist jurisdictions in assessing these options –

(a) Upfront disclosure system – an upfront disclosure system requires the disclosure of the beneficial ownership and control of corporate entities to the authorities charged with the responsibility at the establishment or incorporation stage and imposes an obligation to update such information on a timely basis when changes occur. The obligation to report beneficial ownership and control information to the authorities may be placed on the corporate entity, the ultimate beneficial owner or the corporate service provider involved in the establishment or management of the corporate entity;

(b) Imposing an obligation on service providers to maintain beneficial ownership and control information. This option requires intermediaries involved in the establishment and management of corporate entities, such as company formation agents, trust companies, registered agents, lawyers, notaries, trustees companies, registered agents, lawyers, notaries, trustees and companies supplying nominee shareholders, directors and officers

("corporate service providers") to obtain, verify and retain records on the beneficial ownership and control of the corporate entities that they establish, administer, or for which they provide fiduciary services;

(c) Primary reliance on an investigative mechanism. Under an investigative system, the authorities seek to obtain (through compulsory powers, Court issued subpoenas, and other measures) beneficial ownership and control information when illicit activity is suspected, when such information is required by authorities to fulfil their regulatory/supervisory functions, or when such information is requested by other authorities domestically and internationally for regulatory/supervisory or law enforcement purposes. The effectiveness of an investigative system depends, to a significant extent, on the likelihood that beneficial ownership and control information relating to the establishment stage is available within the jurisdiction in which the corporate entities were established.

4. US Money Laundering Threat Assessment (2005)

Page 47 - "The use of bearer shares, nominee shareholders and nominee directors function to mask ownership in a corporate entity. While these mechanisms were devised to serve legitimate purposes, they can also be used by money launderers to evade scrutiny.

Trusts separate legal ownership from beneficial ownership and are useful when assets are given to minors or individuals who are incapacitated. The trust creator, or settlor, transfers legal ownership of the assets to a trustee, which can be an individual or a corporation. The trustee fiduciary manages the assets on behalf of the beneficiary based on the terms of the trust deed.

Although trusts have many legitimate applications they can also be misused for illicit purposes. Trusts enjoy a greater degree of privacy and autonomy than other corporate vehicles, as virtually all jurisdictions recognising trusts do not require registration or central registries and there are few authorities charged with overseeing trusts. In most jurisdictions no disclosure of the identity of the beneficiary or the settlor is made to authorities. Accordingly, trusts can conceal the identity of the beneficial owner of assets and ….. can be abused for money laundering purposes, particularly in the layering and integration stages.

Legal entities such as shell companies and trusts are used globally for legitimate business purposes, but because of their ability to hide ownership and mask financial details they have become popular tools for money launderers."

5. US Government Accountability Office Report on Company Formations (2006)

Page 1 – "Companies – business entities that conduct a variety of commercial activities and hold a variety of assets – form the basis of most commercial and entrepreneurial activities in market based economies. Companies in the United States play an essential and legitimate role in the country's economic system. They provide a wide variety of services that range from the provision of necessary utilities and investment services to retail sales of items such as clothing and furniture. Companies can also be set up that act as "shell" companies and conduct either no business or minimal business. Shell companies are used for legitimate purposes; for example, they may be formed to obtain financing prior to starting operations. However, government and international reports indicate that shell companies have become popular tools for facilitating criminal activity in the United States and internationally and can be involved in fraud and corruption or used for illicit purposes such as laundering money, financing terrorism, hiding and shielding assets from creditors, and engaging unquestionable tax practices. Such schemes can conceal money movements that range from a few thousand to many millions of dollars".

Page 6 – "Although law enforcement officials noted that information on owners was useful in some cases, State officials, agents and others we interviewed said that collecting company ownership information could be problematic. For instance, if States or agents collected such information, the cost of filings and the time needed to approve them could increase, potentially slowing down business dealings or even derailing them. A few States and some agents also said they might lose business to other States, countries, or agents that had less stringent requirements, a consequence two foreign jurisdictions experienced after regulating agents and requiring collection of ownership information. Further, State officials and agents pointed out the difficulties of collecting

information when companies are being formed or on periodic reports since ownership can change frequently. In addition, State officials and agents expressed concerns about maintaining privacy when making public information about legitimate businesses that historically has been protected. State officials, agents and other experts in the field suggested internal company records, financial institutions, and the IRS as alternative sources of ownership information for law enforcement investigations. However, collecting information from these sources could present many of the same difficulties."

Annex 6 Corporate Vehicles

I. Corporations

A corporation is a legal entity whose owners consist of shareholders. Control of a corporation is vested in the board of directors elected by the shareholders. Since a corporation is a legal entity, the shareholders are only liable up to the amount of their investment. A corporation can have unlimited duration.

a. Private Companies[83] – A private company is restricted in its number of shareholders and the transferability of its shares. Private companies may not issues shares to the general public. Private companies have less stringent reporting requirements than public companies.

b. Public Companies – A public company can freely trade its shares and there is no limit on the number of shareholders. It may offer its shares to the general public. A public company is generally required to adhere to strict reporting guidelines and is subject to rigorous governmental oversight.

II. Partnerships[84]

A partnership is an association of two or more legal or natural persons created to conduct business. For the most part partnerships do not enjoy limited liability and partners may be jointly and severally liable for the actions of the partnership. Partnerships generally benefit from "flow through" taxation which prevents profits being taxed twice.

a. General Partnership – In a general partnership, partners are jointly and severally liable. Partners in such an arrangement are usually easy to identify and general partnerships are rarely required to register.

b. Limited Partnership – A limited partnership consists of general partners and limited partners. The general partners are liable as under general partnerships. The limited partners will typically have limited control and are only liable up to the amount of their investment. Limited partnerships are required to register in most jurisdictions.

c. Limited Liability Partnerships – Under this arrangement, all partners possess limited liability even if they exercise management control. Limited liability partnerships are required to register in most jurisdictions.

III. Limited Liability Companies (LLC)

The LLC is a hybrid business structure that is designed to provide the limited liability features of a corporation and the tax and operational flexibilities and efficiencies of a partnership. The advantages are:

1. Limited liability of the members;
2. Profits and losses are passed-through for taxation purposes; and
3. In the U.S., for the most part, you do not need to be a U.S. person to own, operate or control an LLC.

LLCs generally have fewer disclosure requirements, both in the formation stages and subsequently. Unlike corporations, LLCs are run by members and do not have a formal structure (i.e. with directors and corporate officers). Generally, there are no annual reporting requirements for LLCs, and there are less

[83] Responses to the questionnaires support the conclusion that Trusts and Private companies are the vehicles that are most susceptible to abuse.

[84] All jurisdictions indicated recognizing Partnerships.

administrative burdens than on corporations. Generally, they are less expensive and easier to form and maintain.

IV. Foundations[85]

A foundation (based on the Roman law *universitas rerum)* is the civil law equivalent to a common law trust in that it may be used for the similar purposes. A foundation traditionally requires property dedicated to a particular purpose. Typically the income derived from the principal assets (as opposed to the assets themselves) is used to fulfill the statutory purpose. A foundation is a legal entity and as such may engage in and conduct business. A foundation is controlled by a board of directors and has no owners. In most jurisdictions a foundation's purpose must be public. However, there are jurisdictions in which foundations may be created for private purposes. Normally, foundations are highly regulated and transparent.

V. Trusts[86]

A trust[87] is a corporate vehicle that separates legal ownership (control) from beneficial ownership. Trusts are important for transferring and managing assets. Trusts usually are restricted in duration. Trusts are not required to register in many jurisdictions and because of this it can be difficult to identify the beneficial owner of a trust. Trusts are common law vehicles, but there are civil law constructions that also separate legal ownership from beneficial ownership.

VI. Associations[88]

Associations (based on the Roman law *universitas personarum*) are membership-based organizations whose members, legal or natural persons, or their elected representatives, constitute the highest governing body of the organization. They can be formed to serve the public benefit or the mutual interest of members. Whether an association is a legal entity or not often depends upon registration. Registered associations may enjoy the same benefits as other legal entities.

[85] LV,TR, LT, ES, LB, QA, FR, MY, US, MO, GI, CH, NL, NO, PW, MA, SK, DE, NZ, JP, AU, BE, BA

[86] NZ, MA,PW, NO, GI, MY, QA, GG, UK, HK, MH, IM, JE, VI, JP, BA

[87] See Annex 2 above .

[88] NL, NO, LT, FR, SK, CH, DE, BE

Annex 7 QUESTIONNAIRE

FATF-XVII WGTYP/50

FATF TYPOLOGIES PROJECT ON MISUSE OF CORPORATE VEHICLES (see note 1) QUESTIONNAIRE

This questionnaire has been compiled by the FATF for use in typologies research – the examination of money laundering and terrorist financing methods and trends. The information from this questionnaire will be used by the FATF as part of its assessment on the misuse of corporate vehicles; the completed questionnaires will not be published. A completed report on the misuse of corporate vehicles will be published on the FATF website in June 2006; no country specific information will be placed in the report without first seeking the permission of the country concerned.

Further information on FATF typologies can be found at: http://www.fatf-gafi.org/document/23/0,2340,en_32250379_32237277_34037591_1_1_1_1,00.html

Please try and complete all of the following questions as comprehensively as possible.

1. Country or Jurisdiction (see note 2)

2. Contact Name (please give two names, if the first contact is regularly away from the office for long periods)

3. Contact details -

E-mail address:	
Telephone number:	
Fax. Number:	

4. What type of corporate vehicles (see note 1) can be formed or (b) can be recognised legally (see note 3) in the jurisdiction? Please give the national name of each type, the closest English translation (or equivalent) and a brief description.

	Can be formed	Can be recognised legally (see note 3)	Are bearer shares possible	Are corporate directors possible
1. Legal persons				
Companies				
Foundations				
Partnerships				

Other (specify)				
2. Legal arrangements			[redacted]	
Trusts				
Other				

If there is a form of corporate vehicle that neither can be formed nor can be recognised legally, how are such vehicles that are formed in other jurisdictions dealt with if they are the subject of investigation/prosecution (e.g. if a trust can neither be formed nor recognised legally how would assets held in the trust be dealt with in the event of an investigation/prosecution).

5. What is the estimated number of corporate vehicles formed, for the most recent year for which data is available? If possible this information should be split between corporate vehicles formed for residents and for non-residents.

	Number formed in ……for residents of the jurisdiction	Number formed in ... ... for non-residents of the jurisdiction	Total number of 'live' companies as at end 2004
Companies			
Trusts			[redacted]
Foundations			
Foundations			
Partnerships			
Others (specify)			

If a register is kept of all 'live' companies incorporated please also provide a total figure as at end 2004 (or the most recent end year available).

6. Which of the following entities in the jurisdiction are engaged in the formation and/or administration of corporate vehicles -

	Yes/No	Estimated Number of Entities	Comments
Lawyers, notaries etc.			
Accountants			
Financial institutions (see note 4)			
Trust and company service providers (see note 5)			
Other entities (please specify)			

7. For those who are engaged in the formation and/or administration of corporate vehicles which of the following are they subject to. In each case, please specify the agency or other body that is responsible for performing the relevant functions. To the extent possible also indicate the main characteristics of each of the categories in your jurisdiction.

	The Agency(ies) Responsible	Brief Description of What is Involved
AML legislation		
Prudential regulation		
Self-regulation		
Registration		
A fit and proper test		
Regulatory oversight (see note 6)		
Regulatory monitoring (see note 6)		
Investigatory powers		

8. How do investigative agencies (or other competent authorities) obtain routine information (see note 7) on legal persons and legal arrangements?

	Comments
1. Legal persons	
Companies	
Foundations	
Partnerships	
2. Legal arrangements	
Trusts	
Other	

9.How do investigative agencies (or other competent authorities) obtain information on the beneficial ownership of companies and other legal persons?

	Comments
Upfront disclosure (see note 8)	
From trust and company service providers when required (please indicate what kind of information they are required to keep) (see note 8)	
Through the use of investigatory powers	

Where relevant please distinguish between domestic and foreign beneficial owners

10. How do investigative agencies (or other competent authorities) obtain information on the beneficiaries and settlors of trusts and other legal arrangements?

	Comments
Upfront disclosure (see note 8)	
From trust and company service providers when required (please indicate what kind of information they are required to keep) (see note 9).	
Through the use of investigatory powers	

Where relevant please distinguish between domestic and foreign beneficiaries

11. Can information obtained on corporate vehicles be exchanged with other jurisdictions?

Yes/No

If not what restrictions are in place?

What is the experience of obtaining information from other jurisdictions? What particular difficulties have been experienced?

12. What information is available on the purposes for which corporate vehicles are established, and have you noted any recent trends in this respect?

13. Where those engaged in the formation and administration of corporate vehicles are covered by AML legislation what number of STRs are being filed by this sector, what proportion of the total number of STRs does this account for, and how many have led to investigations/prosecutions.

(i) Number of STRs filed by those engaged in the formation and administration of corporate vehicles in 2004	
(ii) Total number of STRs filed in 2004	
(iii) The number of STRs filed under (i) that have led to investigations/prosecutions to date	

14. What evidence do you have available, in the form of recent case studies, of the misuse of corporate vehicles to launder the proceeds of crime? Please provide evidence, for example, of situations in which the differences between corporate vehicle establishment/management systems in two jurisdictions have been exploited for ML purposes or to carry out other types of offences.

If you have any cases involving more generic abuse of corporate vehicles to carry out other types of offences – circumventing disclosure requirements, bribery/corruption, committing fraud, hiding assets from creditors - please also submit these as case examples.

15. From experience of the misuse of corporate vehicles what in your view are the greatest money laundering vulnerabilities (e.g. which corporate vehicles are most misused and why in your view are these vehicles most usually selected for misuse).

16. What risk mitigation measures are in place to limit the misuse of corporate vehicles (e.g. where bearer shares and/or corporate directors are permitted).

NOTES

1. The term corporate vehicles is as used in the OECD publication "Beyond the Corporate Veil":

   http://www.oecd.org/document/11/0,2340,en_2649_201185_2672715_1_1_1_1,00.html. It includes both legal persons (companies, foundations, partnerships etc.) and legal arrangements (trusts, some forms of anstalts, etc.) as defined for the purposes of the FATF Recommendations.

2. Where the matters with which the questionnaire is concerned are the responsibility of a regional or State authority within a federal structure please complete a separate questionnaire for the jurisdiction as a whole and the regional/State authorities.

3. The term "recognised legally" means recognised by the Courts of the jurisdiction.

4. The term "financial institutions" is as for the FATF Forty Recommendations: http://www.fatf-gafi.org/glossary/0,2586,en_32250379_32236930_34276935_1_1_1_1,00.html#34289432

5. The term trust and company service providers is as for FATF Recommendation 12: http://www.fatf-gafi.org/document/45/0,2340,en_32250379_32236930_33966509_1_1_1_1,00.html

6. Regulatory oversight is intended to cover those situations where there is an opportunity to exercise regulatory control on an ad hoc basis whereas regulatory monitoring envisages a situation where there is formal, continuous, monitoring of those concerned.

7. Routine information would include name, date of incorporation/registration, place of business, registered office/place of administration, sources of funds, shareholders/ and purpose.

8. Upfront disclosure means disclosure to a public body. In the comment please specify what type of information is required to be filed/registered with a local registry or other authority and whether or not the information is available to the public. Please also indicate if information on beneficial owners/beneficiaries is required to be kept by the legal entity itself.

9. The term trust and company service providers is not necessarily restricted to the formal professional category of TCSP's. If – in your jurisdiction – these services are mainly provided by other regulated entities, such as lawyers (see question 6) , please also indicate to what extent investigators can rely on records that are legally required to be kept by such other professionals when providing TCSP-services.

If you have any questions on the FATF typologies, or how to compete the questionnaire please contact Mark Hammond at the FATF Secretariat at: mark.hammond@fatf-gafi.org or tel: +33 (0)1 45 24 99 50

MCV Project
14 September 2005

Appendix X:

FATF, *Best Practices on Beneficial Ownership for Legal Persons*
(Paris: FATF, 2019)

FATF

BEST PRACTICES ON **BENEFICIAL OWNERSHIP FOR LEGAL PERSONS**

OCTOBER 2019

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2019), *Best Practices on Beneficial Ownership for Legal Persons,* FATF, Paris,
www.fatf-gafi.org/publications/documents/beneficial-ownership-legal-persons.html

Table of Contents

ACRONYMS

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Customer due diligence
DNFBP	Designated non-financial businesses and professions
FATF	Financial Action Task Force
FIU	Financial intelligence unit
FI	Financial Institution
INR.	Interpretive Note to Recommendation
LEA	Law Enforcement Authorities
ML	Money laundering
NRA	National Risk Assessment
R.	Recommendation
RBA	Risk-based approach
SRB	Self-regulatory body
STR	Suspicious transaction report
TCSP	Trust and company service providers
TF	Terrorist financing

Executive Summary

1. The results of FATF Mutual Evaluations indicate that jurisdictions find it challenging to achieve a satisfactory level of transparency regarding the beneficial ownership of legal persons. This best practice paper aims to provide suggested solutions, supported by cases and examples of best practices from delegations, in response to challenges faced by delegations in implementing FATF Recommendation 24.

2. As stated in Interpretative Note to R.24, countries should use one or more of mechanisms (the Registry Approach, the Company Approach and the Existing Information Approach) to ensure that information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or can be otherwise determined in a timely manner by a competent authority[1].

3. Countries' experience shown in the FATF mutual evaluations echoes that jurisdictions using a single approach is less effective in making sure that competent authority can obtain accurate and up-to-date BO information to in a timely manner. Instead, a ***multi-pronged approach*** using several sources of information is often more effective in preventing the misuse of legal persons for criminal purposes and implementing measures that make the beneficial ownership of legal persons sufficiently transparent. The variety and availability of sources increases transparency and access to information, and helps mitigate accuracy problems with particular sources.

4. Under a multi-pronged approach, competent authorities can gain access to information on beneficial ownership through different sources. They can also ensure the accuracy of information by cross-checking. It is also easier for key stakeholders (including companies, directors, shareholders, obliged parties such as FIs and DNFBPs) to identify incorrect beneficial ownership information in their database by looking up different registers or requesting information from different sources. This will then trigger the obliged party to seek clarifications from the companies, and if necessary, report suspicious activities to competent authorities. Therefore, such approach encourages key stakeholders to fulfil their obligations through peer interaction and supervision.

5. This paper then identifies the following suggested key features of an effective system (Section 5): a) Risk assessment; b) Adequacy, accuracy and timeliness of information in beneficial ownership; b(i) Obliged parties to verify or/and monitor the accuracy of the information; b(ii) Supplementary information platform in addition to company registry; b(iii) Ongoing reporting at company level / to the reporting entities or company registry; b(iv)Verification through different means; b(v) Enhanced measures for companies with foreign ownership/directorship; b(vi) Highly effective law enforcement authorities with adequate resources; b(vii) Using technology to facilitate checking and validation; c) Access by competent authorities; d) Forbidding or immobilising bearer shares and nominee arrangements; e) Effective, proportionate and dissuasive sanctions.

[1] Interpretative Note to R.24, para. 7 and 8, FATF (2013a).

6. The case examples covered in the best practice paper should be considered in the context of their national system. For jurisdictions that have undergone mutual evaluations, their case examples have been checked against their respective mutual evaluation reports and take into account the latest development in the jurisdiction as far as practicable. It should also be noted that some cases are provided by countries which have not yet undergone mutual evaluation to date, but they are included based on their relevance. Readers are advised to bear this in mind when drawing reference to these examples.

7. This best practice paper also puts forward suggestions on ensuring authorities can access getting information on beneficial ownership of overseas entities (Section 6).

Section I - Introduction and key concepts

This paper should be read in conjunction with the following, which are available on the FATF website: www.fatf-gafi.org.

a) The FATF Recommendations, especially Recommendations 1, 2, 10, 11, 20, 22, 23, 24, 26, 27, 28, 30, 31, 34, 35, 37, 40 and their Interpretive Notes (INR), and the FATF Glossary

b) FATF Guidance on Transparency and Beneficial Ownership (October 2014)

c) The Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018)

d) The FATF Horizontal Study: Enforcement and Supervision of Beneficial Ownership Obligations

Background and context

8. In 2003, the FATF became the first international body to set international standards on beneficial ownership. In 2012, the FATF strengthened its standards on beneficial ownership, to give more clarity about how countries should ensure information is available, and to deal with vulnerabilities such as bearer shares and nominees. The revised standards also clearly distinguish between basic ownership information (about the immediate legal owners of a company or trust), and beneficial ownership information (about the natural person(s) who ultimately own or control it). They also clarify that having accurate and up-to-date basic information about a legal person or legal arrangement is a fundamental prerequisite for identifying the ultimate beneficial owners, and require countries to provide international co-operation in relation to ownership information.

9. The FATF further published the Guidance on Transparency and Beneficial Ownership in 2014 to explain what the FATF Standards require. This guidance paper gives a step-by-step guide on how to access publicly available information on legal persons and legal arrangements, and establish procedures to facilitate information requests from foreign counterparts.

10. However, effective implementation of these measures is still challenging. At the time of publication, 25 FATF members have been assessed since the FATF Standards were strengthened in 2012.[2] For R.24, only 11 out of 25 were rated as largely compliant, 12 were rated as partially compliant and 2 were rated as non-compliant. For IO.5, only 4 out of 25 countries attained a substantial level of effectiveness in preventing the misuse of legal persons and arrangements, 17 attained a moderate level of effectiveness and 4 attained a low level of effectiveness.

[2] Consolidated assessment ratings, FATF www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf

11. In 2016-17, the FATF undertook a horizontal study on the enforcement and supervision of beneficial ownership obligations. The FATF and Egmont Group also jointly published the Report on Concealment of Beneficial Ownership in July 2018. The results of the analysis pointed to that the root of the problem lies in the weak implementation of the existing standard, rather than in the gaps of the standard itself.

12. There is a need for more practical advice and examples for jurisdictions on the effective measures to ensure that legal persons are prevented from being used for criminal purposes, and information on their beneficial ownership is available to competent authorities without impediments.

13. Based on the reviews conducted in the fourth round of FATF mutual evaluation so far, the FATF has identified some specific obstacles in the following areas to effective implementation (detailed in Section II), including:

a) risk assessment;

b) adequacy, accuracy and timeliness of information on beneficial ownership;

c) access by competent authorities;

d) bearer shares and nominee shareholder arrangements;

e) fines and sanctions; and

f) international co-operation.

14. From countries' experience, there is no single solution to tackle these obstacles that are intertwined with each other. The fourth round of FATF mutual evaluations reveals that systems combining one or more approaches under R.24[3] are often more effective than systems that rely on a single approach.

15. To ensure that the system is effective, it requires concerted efforts from different stakeholders to implement measures that prevent legal persons from being misused, and make available accurate information on the beneficial ownership of legal persons so that competent authorities can access the information in a timely manner.

16. This best practice paper aims to provide suggested solutions, supported by cases and examples of best practices that are correspondent to each challenge. This paper draws on countries' experience concluded from adopted MERs, information provided by the delegations, as well as work carried out by other stakeholders in the field. The paper will also provide cases and examples to other inter-governmental organisation in developing their areas of expertise.

17. Taking into account the flexibility allowed by the FATF Recommendations, this best practice paper suggests different ways jurisdictions can use to ensure

[3] The approaches include:
(a) Registry Approach – requiring company registries to obtain and hold up-to-date information on the companies' beneficial ownership
(b) Company Approach – requiring companies to obtain and hold up-to-date information on the companies' beneficial ownership or requiring companies to take reasonable measures to obtain and hold up-to-date information on the companies' beneficial ownership
(c) Existing Information Approach – using existing information

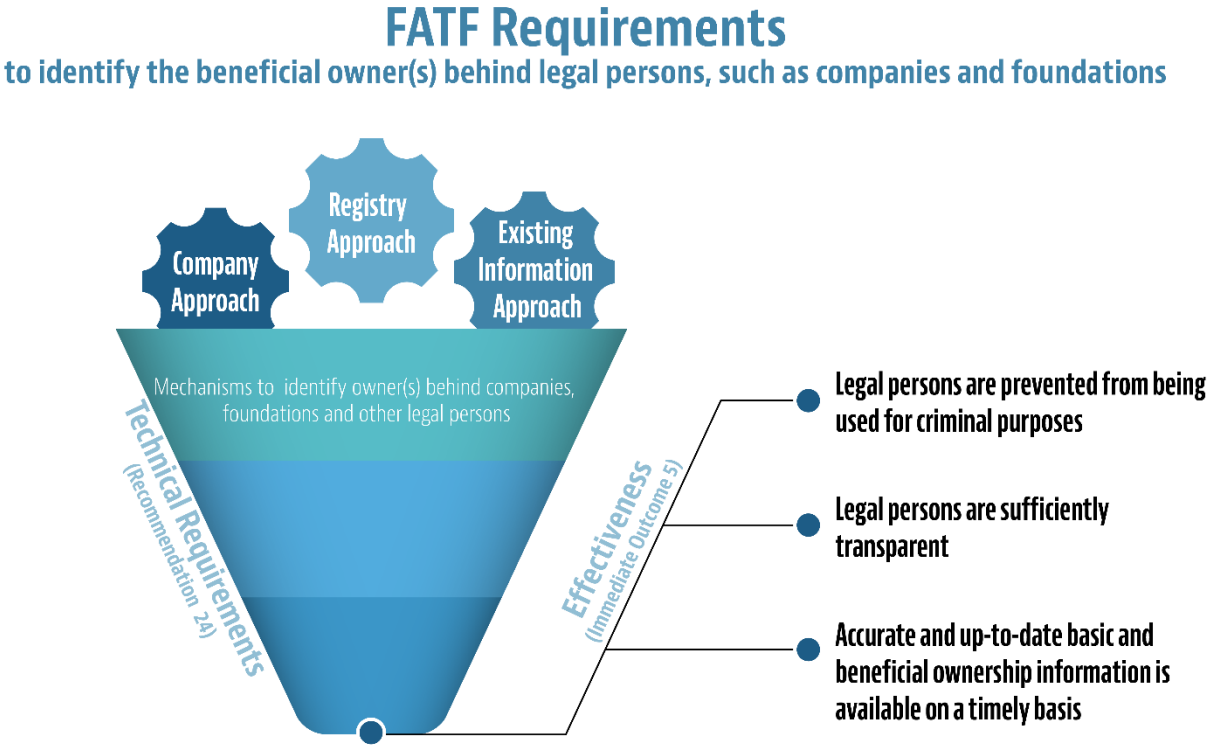
compliance and provides advice on how to implement chosen approaches in the most effective way.

Scope of the paper

18. In order to keep the scope of this project achievable, this paper will focus on beneficial ownership of legal persons (not of legal arrangements such as trusts).

19. The implementation of R.24 and IO.5 also hinges on the effectiveness of other FATF Recommendations (paragraph 44 refers). Although the discussion of the paper will touch on other FATF Recommendations, this paper will only cover examples of best practices that are directly related to approaches associated with transparency of beneficial ownership under R.24 and measures on preventing misuse of legal persons by criminals under IO.5.

Section II - Objectives



FATF requirements

20. Under R.24, countries should take measures to prevent the misuse of legal persons for ML/TF. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for ML/TF. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) undertaking the requirements as set out in R.10 and 22.

21. In relation to beneficial ownership information, countries should ensure that either information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or can be otherwise

determined in a timely manner by a competent authority[4]. In order to meet such requirement, countries should use one or more of the following mechanisms[5] –

a) requiring company registries to obtain and hold up-to-date information on the companies' beneficial ownership (the Registry Approach);

b) requiring companies to obtain and hold up-to-date information on the companies' beneficial ownership or companies to take reasonable measures to obtain and hold up-to-date information on the companies' beneficial ownership (the Company Approach);

c) using existing information (the Existing Information Approach), including:

   i. information obtained by FIs and/or DNFBPs, in accordance with R.10 and 22;

   ii. information held by other competent authorities on the legal and BO of companies;

   iii. information held by the company as required; and

   iv. available information on companies listed on a stock exchange, where disclosure requirements ensure adequate transparency of beneficial ownership.

22. Regardless of which of the above mechanisms is used, R.24 specifically requires countries to establish mechanisms to ensure that companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner. Under the existing R.24, countries have three options for facilitating such co-operation which may be used alone or in combination[6]:

a) Require companies to authorise at least one natural person resident in the country of incorporation to be accountable to the competent authorities for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities as needed.

b) Require companies to authorise a DNFBP in the country to be accountable to the competent authorities for providing such information and assistance.

c) Take other comparable measures which can effectively ensure a company's co-operation.

23. The FATF Guidance on Transparency and Beneficial Ownership[7] states that the FATF Recommendations recognise these different mechanisms and the need to provide flexibility for countries to implement the requirements in a manner that corresponds with their legal, regulatory, economic and cultural characteristics.

4 R.24 applies broadly to "legal persons" meaning any entities, other than natural persons, that can establish a permanent customer relationship with a FI or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities that have legal personality. This can include non-profit organisations (NPOs) that can take a variety of forms which vary between jurisdictions, such as foundations, associations or cooperative societies.

5 Interpretative Note to R.24, para. 7 and 8, FATF (2013a).

6 Interpretive Note to R.24, para. 9, FATF (2013a).

7 Guidance on Transparency and Beneficial Ownership, para. 38, FATF (2014).

Whichever mechanism(s) is used, the fundamental requirement relating to beneficial ownership information remains the same. Countries should ensure that either:

a) information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or

b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority[8].

24. Countries may choose the mechanisms they rely on to achieve the objective of preventing the misuse of legal persons for ML/TF [9]. Countries should consider the feasibility of the possible mechanisms based on their particular circumstances and risk assessment. In determining the appropriate mechanism, countries should seek to strike an appropriate balance between allowing the legitimate operation of corporate vehicles and the need to combat ML/TF[10].

25. R. 24 states that countries should use one or more of the mechanisms (the Registry Approach, the Company Approach and the Existing Information Approach). As stated in the Interpretive Note to R.24, it is also very likely that countries will need to utilise a combination of mechanisms to achieve the objective[11].

Relationship between R.24 and IO.5

26. Compliance with R.24 is intrinsically linked with the effectiveness of the measures assessed in IO.5 to prevent the misuse of legal persons for ML/TF[12]. R.24 requires countries to ensure that competent authorities have timely access to adequate, accurate and up-to-date beneficial ownership information. As a result, measures to implement R.24 is fundamental to implement an effective system.

27. IO.5 states clearly that an effective system should put in place measures to:

a) prevent legal persons and legal arrangements from being used for criminal purposes;

b) make legal persons and legal arrangements sufficiently transparent; and

c) ensure that accurate and up-to-date basic and beneficial ownership information is available on a timely basis.

28. Persons who breach these measures are subject to effective, proportionate and dissuasive sanctions. This results in legal persons being unattractive for criminals to misuse for ML and TF. Prohibitive measures should be imposed to deter criminals from using legal persons to obscure beneficial ownership of illicit assets.

29. Other measures to ensure transparency of beneficial ownership is also essential to AML/CFT regimes so that competent authorities can trace and identify the right target to conduct investigation and prosecution effectively, as well as to provide the high quality of financial intelligence.

---

8 Interpretive Note to R.24 at para. 7 and Immediate Outcome 5 of the FATF Methodology, FATF (2013a).

9 Interpretive Note to R.24, para. 1, FATF (2013a).

10 Guidance on Transparency and Beneficial Ownership, para. 41, FATF (2014)

11 Interpretive Note to R.24, para. 1, FATF (2013a).

12 Guidance on Transparency and Beneficial Ownership, para. 22, FATF (2014)

Section III – Common challenges

Common challenges faced by countries

30. Based on the reviews conducted in the fourth round of FATF mutual evaluation, the FATF has identified the following common challenges faced by countries in implementing measures on beneficial ownership, including:

a) **Risk assessment –** Inadequate risk assessment concerning the possible misuse of legal persons for ML/TF, e.g.

i. Not all types of legal persons were covered in the risk assessment.

ii. Relevant risk assessment was not consistent with the results of national risk assessments.

iii. Only domestic threats and vulnerabilities associated with legal persons incorporated were considered.

iv. Registries, companies, FIs, DNFBPs and competent authorities might not possess a good understanding and knowledge of risks involved in legal persons.

b) **Adequacy, accuracy and timeliness of information on beneficial ownership –** Inadequate measures to ensure that information on beneficial ownership was accurate and up-to-date e.g.

i. Information was not accurate – they are not adequately and actively verified, tested or monitored. There was no obliged party[13] to verify, test or monitor the information or the obliged party might not have rigorous implementation of customer due diligence (CDD) measures.

ii. Relevant parties were not required to keep records for a period of time (for at least five years).

iii. Legal persons did not update their beneficial ownership information or inform the company registry when there was a change of beneficial ownership.

iv. There was a lack of co-ordination among different sources of information and there was no cross-checking to ensure the accuracy of the information.

v. Information on beneficial ownership was difficult to identify when complex structure was involved.

vi. Information on beneficial ownership was not always available when foreign ownership was involved.

c) **Access by competent authorities –** Inadequate mechanism to ensure that competent authorities had timely access to beneficial ownership information on legal persons e.g.

i. There were obstacles to information sharing such as data protection and privacy laws which impeded competent authorities from getting timely access to adequate, accurate and up-to-date basic and beneficial ownership information.

ii. There was no information sharing among competent authorities.

iii. The competent authorities did not have established procedures to seek information from obliged parties.

iv. There was no registration/licensing mechanism of obliged parties so that the competent authorities had difficulties in identifying the source of information.

v. Competent authorities did not have sufficient resources to carry out investigations or law enforcement actions.

13 Obliged party refers to a gatekeeper that is subject to AML/CFT obligations to conduct customer due diligence, including verifying information on the beneficial ownership of the legal person

d) **Bearer share and nominee shareholder arrangements –** Insufficient risk mitigating measures in place to address the ML/TF risk posed by bearer share and nominee shareholder arrangements e.g.

   i. When bearer shares and share warrants were allowed in the countries, the ownership of bearer shares and share warrants was not sufficiently transparent and readily accessible by competent authorities.

   ii. The use of nominee shareholder obscured the ultimate control and ownership of the companies.

e) **Fines and sanctions** – Lack of effective, proportionate and dissuasive sanctions on companies which failed to provide accurate and up to date information on beneficial ownership (e.g. companies providing false information to company registries, or not keeping information about their shareholders or members up-to-date), and reporting entities which failed to apply specific CDD measures required for legal persons.

f) **International co-operation –** Inadequate mechanism for monitoring the quality of assistance received from other countries e.g.

   i. It took long time to obtain information on beneficial ownership as it might involve legal complexities and multiple agents to release the information.

   ii. Other countries concerned did not keep the information on beneficial ownership.

   iii. Language barrier posed a challenge in understanding the information.

Challenges for specific approach

31. Under R.24, countries are allowed to choose to implement one or more of the mechanisms to ensure the transparency of beneficial ownership[14]. This section provides analysis on the implementation of each mechanism and covers issues that could impact the reliability of the information. The detailed arrangement of each mechanism under R.24 is at Appendix 1.

32. The issues mentioned in this section may intersect with the common challenges faced by countries mentioned in Section II. Nevertheless, this section aims to provide an overall review (including challenges) from the perspective of each mechanism.

Registry Approach

33. Countries may implement R.24 by requiring company registries to obtain and hold up to date information on beneficial ownership.

34. Pursuant to R.24, all companies created in a country should be registered in a company registry which should record and maintain (at a minimum) basic information on a company, including company name, proof of incorporation, legal form and status, address of the registered office, basic regulating powers and list of

[14] Interpretive Note to R.24, para. 8, FATF (2013a).

directors[15]. The basic information held by registries should be made publicly available[16] to facilitate timely access by FIs, DNFBPs and other competent authorities.

35. A well-resourced and proactive company registry holding beneficial ownership information can be an effective mechanism because it provides a useful basis for competent authorities to access to such information. Other information agents and the public can also gain access to the information on beneficial ownership for cross-checking and verification.

36. The role of company registries varies greatly from country to country, as does the level and quality of information obtained on companies. The following are the implementation challenges identified from countries' experience:

a) The objectives of company registry may not be broad enough to cover the role of collecting, verifying/monitoring and maintaining information on beneficial ownership, leading to that:

   i. the company registry plays a passive role, acting as repositories of information or documents, rather than undertaking verifying and monitoring or other measures to ensure that the information they receive is accurate.

   ii. the company registry may not be obliged to conduct AML/CFT activities and its relevant performance may not be supervised.

   iii. there may also be lack of sanction powers/insufficient sanctions for missing/incorrect/false information.

   iv. the provision of information on beneficial ownership to the company registry may not necessarily be made a condition for incorporation.

   v. the company registry does not keep information of ultimate beneficial ownership, but only the immediate legal ownership of the company.

b) There may be a lack of mechanisms for ensuring that the information provided to the company registry is accurate and up to date.

c) There may be a lack of interface with other sources of information agents and/or other authorities and this may hamper the effectiveness of cross-checking.

d) Company registry may not have sufficient human and capital resources to enable it to undertake the additional functions of collecting, verifying/monitoring and maintaining information on beneficial ownership.

37. Most of the challenges in implementing the Registry Approach originate from the institutional level – whether the registry is established to collect accurate and updated information on beneficial information, whether it is empowered to do so and to perform its roles with sufficient resources.

38. Countries that make use of registers of beneficial ownership information should consider the resources and expertise that will be required in order to maintain these, and to ensure that the information recorded in the register is adequate,

15 Interpretive Note to R.24, para. 5, FATF (2013a).

16 Interpretive Note to R.24, para. 12, FATF (2013a).

accurate, and up-to-date, and can be accessed in a timely manner[17]. This is also true for the maintenance and supervision of company registries.

39. If the objective of the company registry is not well defined and the power and responsibilities of the company registry are not clear enough, the company registry will not be able to collect the right information in order to meet the objective. Without sufficient resources, the effectiveness of the company registry will also be compromised.

Company Approach

40. Another element that can help implement R.24 is the Company Approach. Countries should require companies themselves to obtain and hold up-to-date information[18] on beneficial ownership by maintaining a list of shareholders or members, and keeping it up-to-date. Companies should also keep updated the list of their representatives, including their roles, functions and authority[19].

41. Below are some problems which have been encountered in countries seeking to follow/rely on this approach for countries taking this approach:

a) Shareholder registers contain information on legal ownership, but not necessarily on beneficial ownership.

b) There is a lack of regulatory framework or mechanism to require and ensure that the beneficial ownership information collected by companies is accurate and up-to-date. For example,

   i. companies may not have sufficient powers to require updated information from their shareholders, including the power to request information on beneficial ownership at any time. Shareholders may not be required to notify the company within a set time period when there are changes in ownership or control.

   ii. shareholders may not be required to disclose the names of person(s) on whose behalf shares are held.

   iii. companies may not have sufficient powers to impose sanctions for shareholders failing to respond or provide false information.

   iv. law enforcement entities may find it difficult to enforce the requirements if these have to be implemented by non-resident subjects (e.g. directors), in particular when they cease to carry out their functions.

c) It is difficult for companies to verify or/and monitor the information received from their shareholders, as well as to up-to-date the information.

d) It is difficult for competent authorities to obtain information on beneficial ownership without alerting the company of a potential investigation.

42. As an alternative, countries may also require companies to take reasonable measures to obtain and hold up-to-date information on their beneficial ownership. From countries' experiences, it is not easy to establish a clear and practical framework

17 The Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018)

18 Interpretive Note to R.24, para. 4, FATF (2013a).

19 Interpretive Note to R.24, para. 3, FATF (2013a).

to set out the scope of reasonable measures. The difficulties lie in that the extent to which companies take measures to obtain and hold up-to-date beneficial ownership information should be proportionate to the level of ML/TF risk or complexity induced by the ownership structure of the company or the nature of the controlling shareholders. It is difficult for companies to perform their obligations if 'reasonable measures' are not well-defined and well-articulated to companies according to the risk levels involved for each type of legal persons.

43. If countries choose to implement this mechanism, countries should identify and assess the ML/TF risks associated with legal persons to enable it to implement a risk-based approach as required by R.1 and 24. Based on the countries' understanding of ML/TF risks through a comprehensive risk assessment, countries should then establish a legal or enforceable framework setting forth a mechanism governing how companies should take 'reasonable measures' to obtain and hold up-to-date beneficial ownership information.

44. In addition to the fundamental challenge on understanding ML/TF risks of different legal persons, another challenge is that the companies are usually not obliged/empowered/motivated to seek to apply restrictions against shareholders for failure to provide BO information.

45. In this case, countries should put in place a legal framework which requires and enables company to obtain updated and accurate beneficial ownership information through enforceable means e.g. seek information through appropriate courts or authorities, imposing restriction in relation to shareholder voting rights, or the sale of shares. The provision of false information by shareholders should also be subject to dissuasive administrative or criminal sanctions. Countries should also make sure that companies and shareholders are aware of their obligations. The authorities can provide guidance to companies or shareholders explaining their obligations, and make this guidance publicly available.

46. Last but not least, the legal framework should also govern that companies should provide lists of shareholders and beneficial owners to competent authorities upon request in a timely manner. Failure by a company to provide the information to authorities is subject to sanctions, which may include administrative penalties or restrictions on incorporation. Where lists of shareholders and beneficial owners are held with a third party provider on the company's behalf, the company should remain liable for the obligations.

Existing Information Approach

47. Countries may also implement R.24 by using existing information collected on the beneficial ownership of corporate entities to identify beneficial owner. Possible sources of information include company registries and other types of registries (such as, land, motor vehicle and moveable property registries); FIs and DNFBPs; other authorities (such as supervisors or tax authorities; information held by stock exchanges, and commercial databases) [20].

48. Below are the specific challenges for countries taking this approach via different channels:

[20] Interpretive Note to R.24, para. 8, FATF (2013a).

FIs/DNFBPs

a) Information may be only available where the relevant entity or structure has established or maintained business relationship with a FI or DNFBP.

b) FIs and DNFBPs may not adequately implement CDD obligations as required under R.10, including measures to identify and verify/monitor the identity of the beneficial owner, and also apply specific measures required for legal persons.

c) FIs and DNFBPs may not be adequately supervised or be provided with sufficient guidance on how to properly conduct CDD.

d) FIs and DNFBPs may not have good understanding and knowledge to assist competent authorities in determining the BO of a complicated legal structure.

Competent authorities

a) Competent authorities may not be aware of the relationship between the legal person and FIs/DNFBPs.

b) Competent authorities may not be able to identify and contact easily the FI/DNFBP if the FI/DNFBP is not subject to registration or licencing requirements.

c) Competent authorities may not have sufficient procedures in getting information from FIs and DNFBPs which may lead to undue delays in receiving information.

d) In relation to tax information, other competent authorities (particularly law enforcement authorities (LEAs)) may not be aware of the information collected and maintained by tax authorities. In addition, the extent to which tax authorities collect information on the ownership and control of legal persons varies greatly from country to country, depending on the tax regime.

Companies listed on a stock exchange

a) The information is only available if the company is listed on a stock exchange.

b) There may not be specific obligation for stock exchange to collect, verify/monitor and keep the information up-to-date for the purpose of AML/CFT.

49. The root causes of the challenges mentioned in paragraph 40 are the lack of established mechanism in obtaining existing information by competent authorities and the lack of mechanism on information sharing among competent authorities.

50. Competent authorities (particularly law LEAs) may not know where beneficial ownership information is held if there is no registration/licensing system for FIs and DNFBPs, which may affect their timely access to such information.

51. The lack of mechanism for information sharing among competent authorities is another obstacle to obtain and verify/monitor beneficial ownership information. In fact, the Existing Information Approach can be effectively used in investigations if there are mechanisms in place to facilitate authorities' access to information held by other authorities (such as tax authorities, supervisory authorities, or land titles offices).

52. The effectiveness of the Existing Information Approach also hinges on the implementation of other FATF Recommendations including:

a) R.2, 37 and 40: Country should rapidly provide international cooperation in relation to basic and beneficial ownership information.

b) R.10 and 22: FIs and DNFBPs to adequately implement CDD obligations, including measures to identify and verify the identity of the beneficial owner. Failure to adequately implement CDD under R.10 can lead to poor collection of BO information.

c) R.11: FIs and DNFBPs to record the CDD procedures performed and maintain these records for at least five years.

d) R.20 and 23: FIs and DNFBPs to report suspicious transactions;

e) R.26, 27 and 28: FIs and DNFBPs to be adequately supervised and supervisors should have adequate powers to supervise or monitor.

f) R.30: competent authorities to be able to access the CDD information held by FIs and DNFBPs in a timely manner

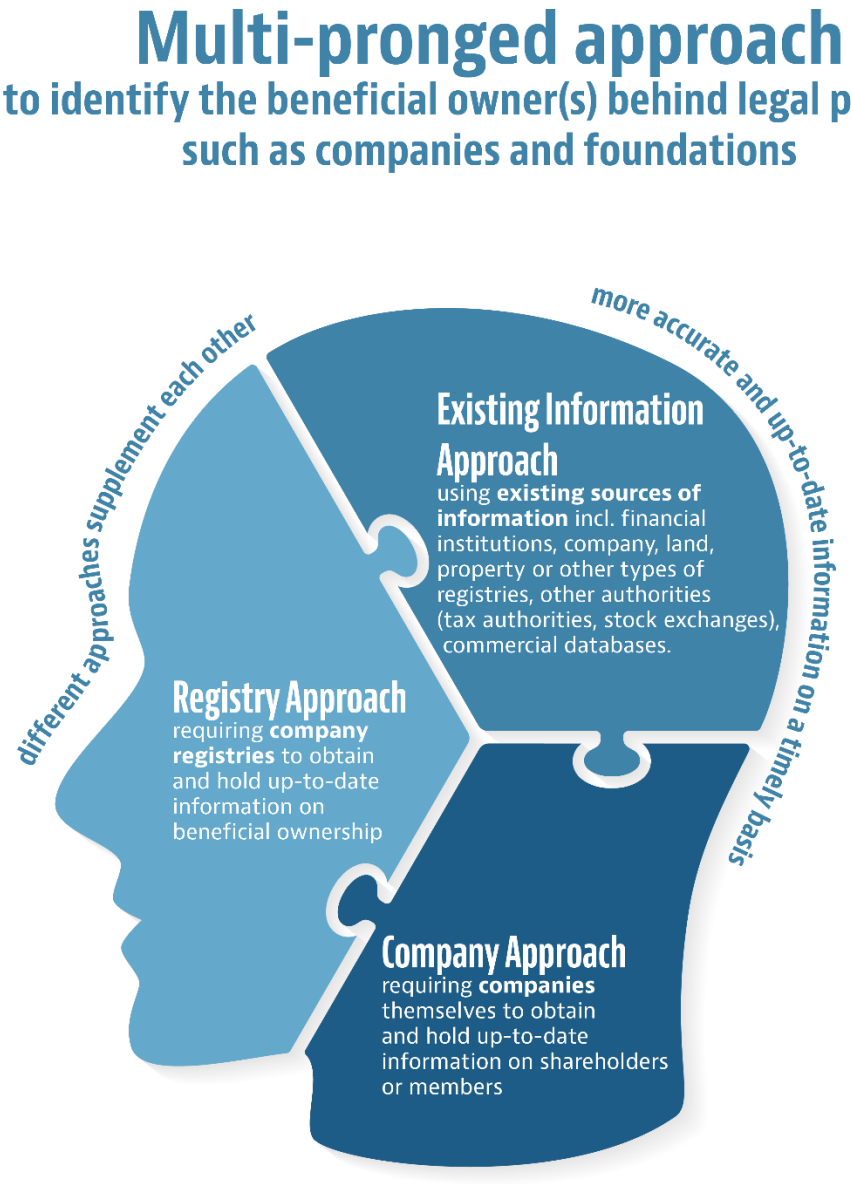
g) R.31: competent authorities to be aware of the existence of the legal person's accounts held by a FI.

h) R.34: FIs and DNFBPs to be provided with sufficient guidance on how to properly conduct CDD.

i) R.35: Countries should ensure that there is a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT requirements.

53. Therefore, it is important to take a holistic view in implementing the Existing Information Approach. It is important to define the roles and responsibilities of each stakeholder, empower them and equip them with the necessary resources and support to carry out their functions.

Section IV – The Suggested Effective System



Multi-pronged approach

54. As stated in Section II (paragraph 14 above refers), countries should use one or more of mechanisms (the Registry Approach, the Company Approach and the Existing Information Approach) to ensure that information on the beneficial ownership of a company is obtained by that company and available at a specified

location in their country; or can be otherwise determined in a timely manner by a competent authority[21].

55. Countries' experience shown in the FATF mutual evaluations echoes that jurisdictions using a single approach is less effective in making sure that competent authority can obtain accurate and up-to-date BO information to in a timely manner. Instead, a multi-pronged approach using several sources of information is often more effective in preventing the misuse of legal persons for criminal purposes and implementing measures that make the beneficial ownership of legal persons sufficiently transparent. The variety and availability of sources increases transparency and access to information, and helps mitigate accuracy problems with particular sources.

56. As illustrated in Section III, information on beneficial ownership of legal persons can be found in a number of different places, including company registries, the company itself, FIs, DNFBPs, and other national authorities, such as tax authorities[22] or stock exchange commissions. Implementing different approaches under R.24 can therefore complement each other to verify or/and monitor the information on beneficial ownership and make sure that the information is accurate.

57. For example, an openly and publicly accessible central registry does not necessarily mean that the information is accurate and up-to-date. It is important for an obliged party (e.g. notary, company registrar) to verify or/and monitor the information on beneficial ownership held under different approaches. The availability of other information agents (e.g. companies, FIs, DNFBPs) facilitates obliged party to cross-check, verify and/or monitor the information.

58. Under a multi-pronged approach, competent authorities can gain access to information on beneficial ownership through different sources. They can also ensure the accuracy of information by cross-checking.

59. It is also easier for key stakeholders (including companies, directors, shareholders, obliged parties such as FIs and DNFBPs) to identify incorrect beneficial ownership information in their database by looking up different registers or requesting information from different sources. This will then trigger the obliged party to seek clarifications from the companies, and if necessary, report suspicious activities to competent authorities. Therefore, such approach encourages key stakeholders to fulfil their obligations through peer interaction and supervision.

Roles and responsibilities of each key stakeholders

60. To effectively implement the multi-pronged approach, it is important to ensure that the responsibilities of various parties are clear and they have played their roles in defending the system of preventing misuse. The system is more effective if every key stakeholder can carry out "defence" in their roles duly. The roles of defence

21 Interpretative Note to R.24, para. 7 and 8, FATF (2013a).

22 For example, the Global Forum on Transparency and EOI (the GF)'s project on beneficial ownership, developed based on the FATF standard, encourages jurisdictions to develop complementary frameworks and enforcement programmes for tax transparency purposes. In March 2019, the GF's Beneficial Ownership Toolkit was launched, which contains policy considerations that jurisdictions can use to implement legal and supervisory frameworks to identify and collect beneficial ownership information.

may include, as appropriate, verification and monitoring of information, carrying out CDD, identifying suspicious patterns and trends on beneficial ownership, reporting suspicious cases and taking enforcement action.

61. Each key stakeholder should know their obligations, understand the risks involved in the form of legal persons, carry out their duties actively and continuously on a timely manner with sufficient resources. The effectiveness of supervision and law enforcement, as applicable, are also important to make sure that the relevant parties have performed their duties.

62. Section 4.3 specifies the basic roles and responsibilities of each key stakeholders and Section 5 supplements on the additional steps or defence that the stakeholders can take to help competent authorities to obtain accurate and up-to-date BO information to in a timely manner.

Suggested roles and responsibilities of each key stakeholder

63. The key stakeholders involved in the system include the company itself, company registry, obliged parties involved in company registration and verification of information (such as lawyers, notary, and accountants), FIs, DNFBPs, supervisors and self-regulated bodies (SRBs). The respective roles and obligations of each key stakeholder are suggested as follows:

a) Company and legal persons

i. Provide basic and BO information, via obliged parties (e.g. lawyers, notaries, accountant, FIs) as required, for the company registry upon registration.

ii. Provide basic and BO information, via obliged parties (e.g. lawyers, notaries, accountant, FIs) as required, both annually and when changes occur without delay to ensure that the information is up-to-date.

iii. Provide copies of documentation for verification of identity as requested.

iv. Keep shareholder registers, such as shareholder lists and information on beneficial ownership (including the disclosure of the names of person(s) on whose behalf shares are held), and make it available to competent authorities or obliged entities upon request in a timely manner.

v. Keep updated the list of their representatives, including their roles, functions and authority.

vi. Obtain updated information from their shareholders.

vii. Seek to apply restrictions against shareholders for failure to provide BO information through appropriate courts or authorities, such as in relation to shareholder voting rights, or the sale of shares.

viii. Understand and/or hold information on their ownership structure, including chain of ownership.

b) Shareholders

i. Provide accurate information on beneficial ownership and updates on changes to beneficial ownership without delay.

c) Company registry

i. Keep basic information and make it publicly available.

ii. Keep information on beneficial ownership and provide access to competent authorities, including full search capability. The company registry may make the information publicly available, or available to FIs and DNFBPs. The company registry authority may also collect information on the board of directors, senior management and the natural person authorised to act on behalf of the company. In addition, directors are required to be natural persons.

iii. Verify or/and monitor the identity of the beneficial owners.

iv. Apply sanctions when obligations are breached. Companies that fail to provide BO information are subject to dissuasive administrative sanctions, such as restrictions on incorporation. The company's representative could also be held personally liable.

v. Report trend/pattern of activities to competent authorities as necessary.

d) Obliged parties (e.g. company registry authority, lawyers, notaries or accountant, other FIs and DNFBPs, as required by the country[23])

i. Understand the ownership and control structure of the customer, and understand the ML/TF risks in relation to legal persons.

ii. Adequately carry out CDD measures at the incorporation stage and conduct ongoing CDD to make sure that the information on beneficial ownership is accurate and up-to-date.

iii. Identify indicators of misuse or unusual activity in the database and keep in view the trend/pattern of suspicious structure of beneficial ownership and report to relevant authorities as necessary e.g. using red flags, sample testing, cross-checking with other data, and public data.

e) FIs and DNFBPs

i. Adequately carry out CDD measures at the incorporation stage and conduct ongoing CDD on the business relationship, and scrutinise transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer and its business and risk profiles, including, where necessary, the customer's source of funds.

ii. Record the CDD procedures performed and maintain these records for at least five years.

iii. Report suspicious transaction activities.

f) Supervisors and SRBs

i. Conduct supervision and monitoring of all AML obliged persons including FIs and DNFBPs and to ensure that they are complying with CDD requirements.

23 An obliged party could be a company registry, FI or DNFBPs. In this case, the obliged party needs to fulfil their duties in their own role and the role of being an obliged party.

ii. Conduct outreach to obliged parties or as applicable, companies, to foster a greater understanding of the ML/TF risks, in particular of companies being created for the sole or main purpose of laundering funds.

iii. Produce guidance on additional steps which could or should be applied as part of (enhanced) due diligence on legal persons.

iv. Apply concrete and dissuasive sanctions (e.g. including monetary penalties) in the case of non-compliance.

g) Competent authorities

i. Know what basic and beneficial ownership information is available in the country, and which relevant parties are holding it.

ii. Establish process and procedures in obtaining information on beneficial information.

iii. Assess the risks of legal persons being misused for ML/TF purposes in order to improve the understanding of risks.

iv. Ensure that there is adequate sharing of information on ML/TF risks, trends and typologies between competent authorities and foster communication with the reporting entities. This would ensure that reporting entities, in particular, are more sensitive to and more familiar with typologies.

v. Provide guidance to companies or shareholders, FIs and DNFBPs explaining their obligations, and provide awareness raising activities as necessary (e.g. through the provision of information to companies upon registration).

vi. Carry out enforcement to ensure that effective, proportionate and dissuasive sanctions are applied in the case of breaches.

h) National authorities

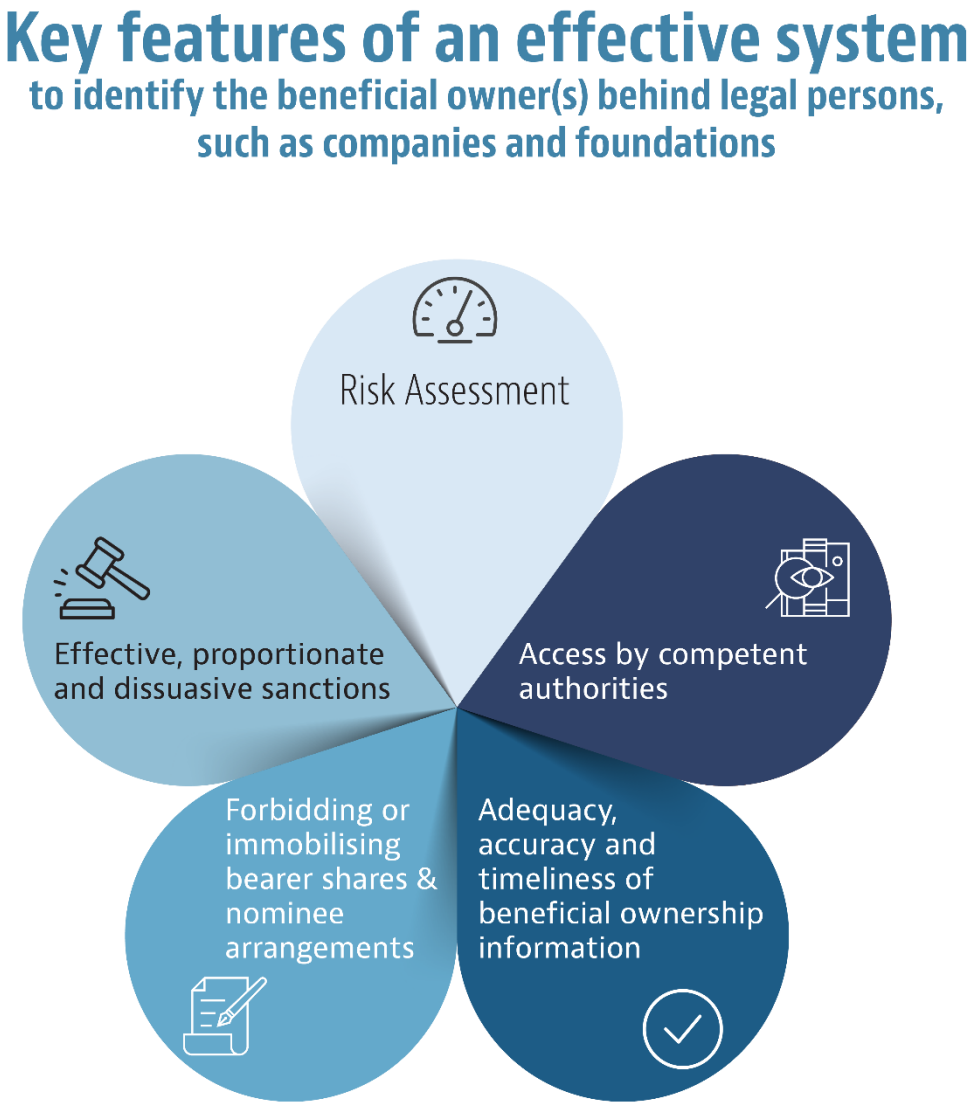
i. Ensure co-operation between government entities holding information on beneficial ownership and set out the mechanism(s) in legislation or regulations to make sure that competent authority can access to information on beneficial ownership in a timely manner.

ii. Identify and assess the ML/TF risks associated with legal persons, to enable it to implement a risk-based approach.

iii. Establish a legal or enforceable framework setting forth the appropriate approach (Registry Approach, Company Approach and Existing Information Approach) to ensure transparency of beneficial ownership.

iv. Introduce measures to prevent legal persons from being misused by criminals e.g. prohibiting bearer shares and bearer share warrants, converting them into registered shares or share warrants, or immobilising them by requiring them to be held with a regulated FI or professional intermediary, or requiring shareholders with a controlling interest to notify the company, and the company to record their identity.

Section V – Suggested key features of an effective system



64. Along with the multi-pronged principle, the FATF has identified the following suggested solutions to facilitate countries to tackle the challenges that they are facing. These suggested solutions are identified from the practical experience of countries as shown in the fourth round of FATF mutual evaluations and information provided by countries in the earlier Horizontal Study.

Risk assessment (relevant to core issue 5.2)

65. Countries should conduct a comprehensive risk assessment of legal persons so as to develop a more thorough understanding of vulnerabilities and potential of abuse of legal persons for ML/TF. This may also help countries to develop specific measures for legal persons that are easily being misused for ML/TF.

66. In some countries, there is a designated agent commissioned to analyse the ML/TF risks posed by all types of legal persons. Such agent considers relevant legal and regulatory contextual issues particular to the country and multi-agency information sources to identify trends and patterns, including:

a) review of relevant court cases;

b) suspicious transaction reports filed by obliged parties e.g. notaries, lawyers, company registry, other FIs and DNFBPs;

c) practical experience of competent authorities;

d) identified patterns/trends in ML/TF and relevant changes e.g. "preferences" amongst the various types of organised crime groups for certain forms of company.

67. The agent then conducts assessment regarding the risks of legal persons, and share information on ML/TF risks, trends and typologies with competent authorities and obliged parties. The sharing of current trends and typologies enables obliged parties to consider the risks at the incorporation stage, and they can pay attention to potential red flags at the incorporation stage.

68. For countries which are an important regional and international financial centre, more efforts should be put to identify, assess and understand the vulnerabilities of corporate structures for ML/TF particularly in relation to international threats.

Belgium

In 2018, an agent was hired at the Treasury (FPS Finance) to conduct a horizontal risk analysis on legal persons which could be established under the Belgian law. The analysis involved a study of the legal framework as well as meetings with competent authorities to identify trends and patterns. The purpose of the analysis was to enhance the understanding and knowledge of competent authorities on the vulnerabilities and potential abuses associated with each legal person, and also to identify the loopholes and necessary legal reforms or additional measures.

The analysis concluded that the most vulnerable structure is the private limited liability company (SPRL/BVBA). This is the most common form of legal persons. While most of them are properly registered, some of them pose ML/TF risks. Fraudsters are aware of certain loopholes which allow them to circumvent controls and misuse the structure to conduct unlawful activities. This may lead to inaccuracy of the Registry. Another risk is that legal persons that are registered are not necessarily active.

This affects the accuracy of statistics and also allows the trading of dormant companies to avoid the administrative process of creating or dissolving a company.

Belgian authorities are aware of the threats and vulnerabilities and have taken measures to address them. The Belgian Company Code has been recasted to reduce the number of types of legal persons and harmonise the rules applicable to profit and non-profit legal persons. Targeted actions have also been launched. For instance, a task force has been established by competent authorities to efficiently dissolve inactive entities.

Indonesia*

Sectoral Risk Assessment of Legal Person

The Indonesia National Risk Assessment (NRA) 2015 indicated that financial criminals perceived it safer to disguise illicit funds through legal person(s). Corrupt government officials and drug dealers can easily hide their illicit gain behind the complex structure and network of corporate transactions. In many cases, this was made possible by the lack of governance in beneficial ownership. Criminals can appoint nominees to appear as the owners of their assets while leaving no trails anywhere in the corporate legal documents.

In 2017, the Commission Eradiation Commission (KPK) together with PPATK (Indonesia's Financial Intelligence Unit (FIU)) and Financial Service Authority (FSA/OJK) conduct the Sectoral Risk Assessment (SRA) of Legal Persons. This money laundering SRA of Legal Persons is separate with the terrorist financing SRA of Legal Persons. The SRA of Legal Persons identified all types of legal person in Indonesia, which are limited liability companies, foundation, cooperative, firm, partnership, and association.

The money laundering SRA of Legal Persons identified six dimensions of risks, including(1) type of legal person; (2) type of business; (3) delivery channel; (4) reporting party; (5) international transaction (inflow); and (6) international transaction (outflow). The terrorist financing SRA of Legal Person identified four dimensions of risks, including (1) type of legal person; (2) type of business; (3) delivery channel; and (4) reporting party.

The result of SRA of legal persons shed light on the risks faced by different legal persons as follows:

- Indonesia's "Perseroan Terbatas ("PT" i.e. limited liability companies) are exposed to a higher ML risk, while "Yayasan" (i.e. foundations) are exposed to higher risk for TF.

- Companies that operate trading business are prone to ML more than other types of business, while social foundations and religious institutions remain the most vulnerable to TF.
- From delivery channels perspective, fund transfers are the most frequently used for in both ML and TF scheme.
- Despite of the stringent regulations, banking remains the reporting party with the highest ML risk.
- Indonesia specifically covered international transactions in the assessment and noted that some jurisdictions with perceived low ML risk appear to have been used by Indonesian-based corporations to keep their money.

**yet to undergo mutual evaluation as of September 2019*

The United Kingdom

A thematic review of relevant legal entities (RLEs) on the PSC Register

Following engagement with NGO community and Companies House facilitating data analysis by NGOs, the risk of accidental or deliberate misuse of the Relevant Legal Entity (RLE) exemption for the PSC register was raised. Companies House has undertaken to check each RLE registered, prioritising on a risk-based approach by focussing on those registered in financial centres or countries with weaker transparency laws.

Circular ownership of companies is prohibited by Companies Act 2006. The UK's experience is that circular registrations are a result of a misunderstanding of the person with significant control (PSC) requirements, not deliberate. For a company to deliberately register a circular loop would essentially disclose that they had breached s.136 of the Companies Act and committing a false filing offence.

UK National Crime Agency (NCA) Intelligence Report - "The use of corporate entities to enable international money laundering networks"

The NCA report examined the case of an overseas international money launderer utilising UK corporate entities to launder the proceeds of crime. In this example, the controller routed illicit funds to an overseas based company from 11 UK corporate entities (Ltd company, Limited Liability Partnerships (LLPs), Scottish Limited Partnerships (SLPs)), all of which banked exclusively outside of the UK. The ownership of these companies highlighted that they were often nominee partners or directors who had been linked to suspicious offshore structures.

The key insights from this report included: the use of several different "vanilla" structures for illicit purposes; the use of "nominee partners" can present a vulnerability; entities were often banked overseas where CDD requirements or enforcement of regulations might be lower; and criminals

take advantage of the perceived respectability of the UK business community in order to provide a façade of legitimacy. This intelligence report contributed to more fundamental reviews of the vulnerabilities posed by LLPs and SLPs in respect of high-end money laundering. After the report, the UK introduced several measures to improve transparency of these entities and is expected to have mitigated some of the vulnerabilities identified. For example, criminals can no longer hide beneficial ownership through one of the partners being a corporate body registered in an overseas jurisdiction.

Strategic intelligence assessment: 'The use of corporate vehicles to hide beneficial ownership'

This report identified the use of multiple corporate vehicles, and complex structures using multiple jurisdictions consisting of a series of corporate entities to obfuscate beneficial ownership. There are delays in identifying the relevant jurisdiction(s), requesting, and accessing the required information, assuming it exists. Organised crime groups and individuals will be aware of this and will seek to complicate the structures as much as possible. Furthermore, law enforcement have to rely on legal requirements of that country e.g., details required when incorporating a company, which vary considerably depending on the country. This is most apparent in a country where secrecy is one of the main attractions for using that jurisdiction. Furthermore, the report found that the use of SLPs created further complications as they do not need to register for tax or provide financial reports if the business is conducted abroad. SLPs can register companies abroad in foreign offshore centres, which limits Her Majesty's Revenue and Customs (HMRC)'s ability to perform background checks as the beneficial ownership is disguised in these companies. This analysis has been used to inform the UK's risk-based approach and to understand the vulnerabilities in the UK.

Switzerland

A dedicated inter-agency group for the assessment of AML/CFT risks

Switzerland has established a national AML/CFT co-operation and co-ordination framework led by the Interdepartmental Co-ordinating Group on Combating Money Laundering and the Financing of Terrorism (GCBF). All competent authorities regularly take part in this group. The Group is responsible for the ongoing identification of risks to which the country is exposed. Under the leadership of MROS (FIU), there is a specific working group dedicated to risk analysis. The GCBF, represented by high-level officials, proposes measures to address the identified risks. The results of the works of the GCBF are submitted each year to the Swiss Federal Council for information or for adoption of further measures.

In June 2018, GCBF published an in-depth analysis on the AML/CFT risk of legal persons and arrangements. This report, adopted in November

2017, compiles extensive quantitative and qualitative data from multiple sources of information from competent authorities, academia and the private sector. It identifies the main threats and vulnerabilities affecting Switzerland with regard to legal per-sons and arrangements and addresses the residual risks by proposing measures, including at the legislative level. The report is publicly available which ensures a wide dissemination and awareness raising.

Adequacy, accuracy and timeliness of information in beneficial ownership

Obliged parties to verify or/and monitor the accuracy of the information (relevant to core issue 5.3 and 5.4)

69. The country may appoint a fully regulated and effectively supervised gatekeeper i.e. an obliged party which is subject to AML/CFT obligations, to ensure the accuracy of the information. Such an obliged party should be fully aware of their obligations, understand thoroughly the risks associated with all types of legal persons, and verify or/and monitor the accuracy of information on beneficial ownership. The role of this obliged party in authenticating and verifying/monitoring the acts relating to the information on beneficial ownership throughout the whole lifecycle of legal persons reinforces the reliability of information in particular when its activities are constantly supervised and in sanctioned in case of identified non-compliance.

70. In some countries, the company registrar is the obliged party who shall perform CDD functions. The registrar checks information submitted by companies against other sources (such as national identity registers or tax administrative registers) to verify or/and monitor the information on beneficial owner. The registrar also identifies anomalies or inconsistencies and make reports to the competent authorities.

71. In some countries, the involvement of a notary, a lawyer or an accountant, who is an obliged party subject to AML/CFT obligations, is required at the company incorporation stage, as well as subsequent stages to validate and ensure accuracy of information reflected in the business register and authenticate changes in ownership. Such obliged party is under the supervision of a designated supervisor that is responsible for verifying compliance with these CDD obligations. Some countries implemented additional mitigation measures by verifying or/and monitoring the identity of the obliged party. The company registry will check against the relevant register to confirm that the obliged party is a qualified professional and that his/her licence has not been suspended or revoked.

72. In some countries, it is mandatory to open a bank account with an obliged FI (e.g. banks) before completing company registration. This entails a separate CDD process by FIs where beneficial owners of the company are identified. Such a requirement can help with verification of BO at the time the legal person is created. If there were a requirement to maintain this (or another) bank account throughout the life of the legal entity, then it could also contribute to maintaining up-to-date information, by leveraging the FI's ability to periodically refresh customer files or identify when changes occur.

Denmark

When establishing a company in Denmark, obliged parties subject to AML/CFT obligations (lawyers or auditors) are often involved at the incorporation stage as the business register requires confirmation from a lawyer, auditor or bank that the required capital has been paid in full. Hence, obliged entities that must perform CDD are very often involved at the incorporation stage.

Danish natural and legal persons that are creating or managing legal persons by making registrations in the Central Business Register (CVR) are required to use a special form of ID (NemID), issued by a government agency. NemID is a common secure login to the Internet that is used for a variety of purposes, such as online banking, finding out information from the public authorities, or engaging with businesses. This electronic login leaves an electronic footprint and gives the DBA digital information about the person making a registration which can be used in various control situations.

Further, when making a registration in the Central Business Register, everyone must sign an electronic declaration stating that the information put in the business register is correct.

Guernsey*

Validating beneficial ownership information and providing information to TCSPs on their "gatekeeper role" in the formation and administration of legal persons

Only licensed trust and company service providers (TCSPs) who are subject to full AML/CFT and prudential supervision in Guernsey by the Guernsey Financial Services Commission (GFSC) can incorporate legal persons in Guernsey. TCSPs have been subject to requirements to identify and verify the beneficial owners of all structures for whom they act under Guernsey's Proceeds of Crime legislation. In 2017, Guernsey introduced additional legislation requiring all Guernsey legal persons to disclose the identity of their beneficial owners to a central register of beneficial ownership. Transitional provisions in this law required accurate and up to date beneficial ownership information to be provided to the Register on existing legal persons before the end of February 2018.

In the second half of 2018, the GFSC undertook a thematic review to assess the effectiveness of the 2017 legislation for ensuring the accuracy of information on the Register about the beneficial ownership of Guernsey legal persons, which are administered by TCSPs. The review consisted of an extensive survey of all licensed TCSPs who were required

to provide detailed information on the proportion of beneficial owners wh**o** fell within each of the FATF's "3 tier ownership test" for the legal persons for whom they act. The results were examined and together with input from the Registrar and Guernsey's Financial Intelligence Unit. Twenty TCSPs were selected for focused on-site inspections to review the beneficial ownership records of up to twenty legal persons per firm. The GFSC also compared information on the beneficial ownership register with that on TCSPs' files to check the accuracy of beneficial ownership information submitted to the Register.

The GFSC issued a public report on its findings from the review in 2019 to help inform TCSPs of their obligations under both the Proceeds of Crime law and the 2017 law. The report included case studies on different types of beneficial ownership structures observed by the GFSC during the inspections to highlight examples of good practice and areas for improvement.

**yet to undergo mutual evaluation as of September 2019*

Hong Kong, China

Information provided to the Companies Registry (CR) are subject to checking and verification by the CR. Financial institutions are also subject to statutory CDD and record-keeping requirements when any company opens a bank account. The CR also conducts regular site inspections to check if significant controllers registers (SCRs) are properly kept or not by companies. The CR will check the accuracy of information contained in the SCR against other available sources on a risk based approach.

Italy

Notaries in Italy perform a public function. The information that they provide is deemed self-sufficient, and its content is verified through the automated checks. At the time of incorporation, the information is entered on the basis of a public deed prepared by a notary and processed online through the use of a digital signature. The public deed itself is available to external parties "as is." Basic checks are conducted by the IT system upon registration. They include an automated calculation of shares (to ensure that they don't exceed 100%) and of the capital (to ensure it does not exceed the proposed total) as well as an automated validation of information such as the tax ID number entered, digital signature –and therefore the identify– of the applicant, and of the payment of the mandatory fees and taxes. Additional automated checks are also performed with respect to new information entered into the system (for example to ensure that shares are only transferred by persons who are already in the system). Any anomaly highlighted by these automated checks is analysed by the Business Register staff before the publication is authorised.

Israel

In addition to the mandatory involvement of an Israeli lawyer for both the online and paper registration process to verify the signatures of shareholders and directors, the vast majority of applications made in paper form are submitted to the registry by lawyers who are subject to CDD obligations, including an obligation to obtain and retain beneficial ownership information. The Israel Companies Authority (ICA) confirmed that the vast majority of all registered company applications are submitted by Israeli lawyers. These lawyers are subject to CDD obligations on beneficial ownership. The MoJ is in charge of verifying compliance with these CDD obligations.

The ICA has implemented additional mitigation measures in relation to potential abuse by use of online applications. Such applications must be submitted by a lawyer subject to AML/CFT obligations, who is identified by an electronic certificate. The identity details of that lawyer are checked against the Bar Association's register to confirm he/she is a qualified lawyer and that his/her licence has not been suspended or revoked. There is one exception, which is rarely used, when the application is submitted by a shareholder who is the sole shareholder and a director of a company. Such applications require the identification of that shareholder on the on-line system by an electronic certificate (which is issued only after a face-to-face meeting with the shareholder/director concerned). In addition, the ICA requires the applicant (i.e. the lawyer or shareholder) to upload a copy of the by-laws, signed in the presence of a lawyer required to verify the signature of the shareholder on the articles of association – hence, sole shareholders making online applications are also subject to identification measures.

Japan*

On 30 November 2018, the amendment of the Ordinance for the Enforcement of the Notary Act came into force. Under the amended ordinance, to incorporate stock companies (the most commonly used form of legal entity), general incorporated associations and general incorporated foundations (hereinafter called 'stock companies etc.'), the founders (clients) are required to report to notaries the information regarding the identity of the person who ultimately owns or controls the legal person they establish when notaries certify articles of association. In Japan, the articles of association must be certified by notaries to incorporate these legal entities. The clients also need to report to notaries whether the person who ultimately owns or controls the legal person is a member of organised crime groups or international terrorists. The notary database is kept in a centralised and systemic way. Competent authority can access the information in the database through notaries.

Notaries are required to check the accuracy of the reported information regarding the identity of the person who ultimately owns or controls the legal person by examining the submitted articles of association and other documents. Notaries also make use of their database on organised crime groups and international terrorists and when the person who ultimately owns or controls the legal person falls into these categories, the notaries refuse to certify the articles of association. The information regarding the identity of the person who ultimately owns or controls the legal person acquired by notaries is stored in their database to which competent authorities can refer upon their request.

**yet to undergo mutual evaluation as of September 2019*

Jersey*

Fully regulated and supervised obliged persons are required to form and maintain legal persons, along with vetting by registry

The incorporation of most legal persons in Jersey is conducted by regulated trust and company service providers (TCSPs).[24] TCSPs are subject to full supervision in Jersey, including fit and proper requirements and regulation of both AML/CFT and prudential/conduct. TCSPs are required under the Money Laundering (Jersey) Order 2008 to find out, and to verify, the identity of the beneficial owners of structures that they administer, and to keep information and records up to date. TCSPs are also required to update the central register of beneficial ownership and control within 21 days of knowledge of a change of beneficial ownership.

24 Local trading companies may incorporate without the use of a TCSP, but are subject to additional identity verification and due diligence by the Jersey Financial Services Commission.

In 2018, with a focus on the accuracy of the Register, the Jersey Financial Services Commission (JFSC) carried out a series of themed examinations to a cross section of TCSPs who provide administration services to Jersey registered entities. The accuracy of client information held by TCSPs continues to be a focus of the JFSC. Customer data is reviewed against data held on the register of beneficial ownership during on-site examinations.

The Companies Registry itself conducts a three stage, sequential vetting process, which involves 3 separate individuals when vetting a) on incorporation; and b) on change of beneficial ownership or control. The vetting process on incorporation must be signed off by either a Head of Unit or a Director of the JFSC within which the Companies Registry sits.

Each beneficial owner and controller and the activities of each entity is vetted against sanctions lists and court regulatory decisions made anywhere in the world, using various sources including a consolidated sanctions and Office of Foreign Assets Control (OFAC) lists, World-Check, internal Customer Relationship Management systems check, internal intelligence/enforcement database check, open source internet searches and regulatory databases maintained by the JFSC.

Any negative information found during the vetting process will be escalated to Head of Unit or Director level and will either result in shared internal intelligence and/or filing of a Suspicious Activity Report. An active feedback loop is exercised to ensure that deficiencies are taken into account by the Supervision division of the JFSC, and, where relevant, the Enforcement division.

**yet to undergo mutual evaluation as of September 2019*

Spain

Notaries are required in all cases, to identify and record the beneficial owner of a newly incorporated entity on the basis of a declaration made by the company's representative Customer due diligence undertaken by obliged entities makes a significant contribution to Spain's systems for providing authorities access to beneficial ownership information and to ensuring the quality of that information. The notary profession is particularly relevant in virtue of the legal requirements for their involvement to validate most acts involving legal persons. Notaries are very aware of their significant gatekeeper role, as well as of the importance of the information they hold, and have actively worked with the authorities to develop systems to open up their wealth of information for the authorities.

Supplementary information platform in addition to company registry (relevant to core issue 5.3 and 5.4)

73. In addition to company registries, some countries have another database holding information on beneficial ownership. Competent authorities or obliged parties can access these repositories, and cross-check the information against that held by obliged parties and authorities such as company registry, notary profession, tax or stock market authorities.

74. In some countries, their notary profession, being the obliged party, keeps a centralised database on beneficial ownership of legal persons. This includes information obtained and recorded by notaries when incorporating entities or conducting certain other acts or transactions by persons and entities, and information on the transfer. This creates another repository of corporate information which is used to validate the information on the company registry.

75. Some countries may also have their tax authorities maintain beneficial ownership information for certain legal persons. The tax authorities may hold basic and beneficial ownership information on legal persons who have an income, have ownership and/or make transaction of real estate or hire employees. Some even require that all legal persons making disclosures to the tax authorities are required to have a bank account and are subject to banks' CDD requirements.

76. In some countries, professional associations have made free access to certain private databases available to their members. This facilitates the professionals to cross-check information with existing customers or exchange with other obliged parties while complying with data protection measures.

China

In March 2014, China launched the National Enterprise Credit Information Publicity System (NECIPS), which includes information of all enterprises registered with the State Administration of Market Regulation (SAMR). The NECIPS is an authoritative, nationally unified information system established by the competent authority to disclose statutory information. Written inspection, on-site inspection and network monitoring are conducted to randomly check the publicity information. Enterprises that violate the information disclosure requirements are listed on the "grey list" and "black list" for creditworthy sanctions, and may also be subject to fine or even licence revocation. The system strengthens the transparency of business operations, promotes the company's integrity and self-discipline, and strongly supports the supervision. Since 2017, the average number of visits has reached 19.4 million times per day, and the average number of inquiries has reached 3.2 million times per day.

The available information of the NECIPS includes the company's basic information, shareholders and funding information, mortgage registration, administrative licensing and sanctions, as well as some business information. This does not include beneficial ownership information, but may nevertheless contribute to efforts to identify the beneficial owner.

Indonesia*

Since 2018, all legal persons are required to disclose their beneficial owner and to provide beneficial ownership electronically through AHU Online. AHU Online is an application that consist of basic information and beneficial information of legal person that maintain by Ministry of Law and Human Right (companies registry). To ensure that the reporting parties can access the beneficial ownership information in timely manner, Presidential Regulation Number 13 year 2018 regulates specific requirement that oblige the companies registry to provide direct access for reporting parties.

Moreover, competent authorities, especially government agencies (e.g. Ministry of Energy and Mineral Resources, Ministry of Agriculture, Ministry Agrarian Affairs and Spatial Planning), are empowered to consider whether to provide business license to legal person which has not yet disclosed or designated its beneficial owner. Competent authorities will decide based on the assessment of the authorised institution, (a) audits of the legal person by the competent authorities; (b) information from a government institution or private entity that manages data and/or information of the beneficial owner, and/or report from certain professions that keep information of the beneficial owner; and/or (c) other relevant information.

**yet to undergo mutual evaluation as of September 2019*

Israel

Information held by Tax Authorities

The Israel Tax Authority (ITA) holds basic and beneficial ownership information on all legal persons which have an income, which own real estate, which buy/sell real estate, which have any employees in Israel, which have any assets in Israel or which undertake any financial transactions. All legal persons making disclosures to the ITA are required to have a bank account and are subject to banks' CDD requirements, including those on beneficial ownership.

Italy

The Guardia di Finanza (GdF) has been successful in a number of instances in identifying the beneficial owners of companies misused by criminals, especially mafia-type organised crime groups, through a combination of measures, including consultation of the information collected by reporting entities (mainly notaries and banks) and of various databases.

- on the basis of the data contained in Suspicious Transaction Reports (STRs) – Instructions issued by the FIU establish that the transmission of STRs shall always be complemented with indication of the beneficial owner. The incapability to identify the beneficial owner represents, in itself, a reason for filing a STR;
- from notaries – whereby the legal person under investigation has been part of public acts (e.g. purchase of properties). Information acquired from the Business Register, Anagrafe Tributaria, records held at notaries, and Notarial Archives;
- from accountants. Consultation of the Anagrafe Tributaria allows to identify the custodian of the accounting records or the intermediary who transmitted the compulsory returns for income tax and VAT purposes; and consultation of records (registers) held by professionals;
- from banks, other financial intermediaries and trust companies, identified through queries of the Archivio dei Rapporti Finanziari. After identifying the intermediary, the AUI (Archivio Unico Informatico) shall be consulted.

The same sources may also be utilised in criminal investigations on the basis of an ad-hoc decree (Article 248 Code of Criminal Procedure) issued by the relevant Judicial Authority.

Spain

In Spain, there are currently three databases that hold information on beneficial ownership of companies, each one of them set up with information collected by different obliged entities (Notaries, Registrars and credit institutions). All of them are accessible on-line to LEAs by means of web portals or web services. Such network of overlapping mechanisms together secure the availability of beneficial ownership information of all commercial entities operating in Spain. The mechanisms are as follows:

1. The Single Notarial Computerised Index: beneficial ownership information obtained by notaries through their CDD is held in the notary profession's Single Computerised Index. This database records separately the information obtained through customer declarations at the time of notarised transactions and the verified, aggregated information compiled by notaries.
2. The Business Registry also collects information on beneficial ownership as reported by the authorised representative of the company. On 21 March 2018 a Ministerial Order was issued, requiring all companies (except for publicly listed companies) to annually submit a form, identifying their beneficial owners, to the Business Registry when fulfilling the obligation to file annual accounts. Failure to file the annual accounts (including this form, as accounts deposited

without it shall be rejected for being incomplete) causes the Registry sheet of the company to be locked and has other legal consequences, such as a possible monetary fine, the exclusion of the company from any public tender and, in cases where the company reaches an insolvency state, there is the legal presumption that such state has been reached by negligence or fraud. Even though the period for depositing accounts is not closed yet, on 1st April 2019 more than 1 154 000 companies have already filed their 2018 annual accounts and more than 1.5 million beneficial owners have already been reported.

3. The third database is the Financial Ownership File held by Sepblac (the Spanish FIU and AML/CFT supervisor). Credit institutions will submit a monthly report about the bank and securities accounts opened/held by them to Sepblac. One of the fields required for credit institutions to fill in (except for publicly listed companies) is the identification of the beneficial owners of the account holders. Therefore, information that comes from the CDD carried out by banks to legal persons whenever opening or holding a bank or securities account is also accessible to LEAs for the purposes of preventing, detecting or investigating ML/TF cases.

Ongoing reporting at company level / to the reporting entities or company registry (relevant to core issue 5.3 and 5.4)

77. To ensure that the information on beneficial ownership is updated in a timely manner, a country may require legal persons to undergo ongoing reporting. If there is change to the beneficial ownership, legal persons are obliged to file changes that are verified by the obliged party.

78. In some countries, the company registry imposes an annual updating requirement on companies to make sure that the information of the company's beneficial ownership is up-to-date. Some registries may implement automated systems to monitor deadlines for filing annual returns or certifications. In addition, legal persons are required to file updates within a designed period if there is any change in beneficial ownership. Otherwise, the change may not have legal effects. Some registries require companies to provide an annual report confirming the basic information previously provided to the registry by the end of the calendar year and making such annual reports publicly available so that the public can see the contents of a report and when it was last submitted.

79. A point to note is that such updates on beneficial ownership to the company register are to be verified by an obliged party. In some countries, involvement of a notary is further required to validate changes in basic information. Information submitted to the company registry must be accompanied by a notarial document. Notaries also maintain the same information, as well as information related to changes in shareholders in a separate database that is updated within a specified timeframe.

80. For registers of shareholders, if these are held by the company itself or a depository institution, the company director is responsible for ensuring their accuracy, and for updating them immediately when changes take place. A Registry system that is held at the company level allows keeping a complete and full record of beneficial ownership information. The register can show the changes of beneficial owner. This allows competent authorities to obtain or retrieve beneficial ownership information from the company.

a) Ongoing reporting at company level

Switzerland

Companies in Switzerland must keep a record of their shareholders (SAs) or members (SARLs and SCs) and their beneficial owners (Art. 686, 697j, 697l, 747, 790, 837 CO), including for bearer shares. Shareholders must inform the company within a month of any acquisition of the shares (697i CO). All shareholders, of both registered and bearer shares, or of units where the holding reaches or exceeds the threshold of 25% of the capital or of the votes, must inform the company of the name of the natural person who is the beneficial owner of the shares or units. The information must be kept up to date. They must also notify the company of any changes (Art. 697i, Art. 697j and 790a CO). In addition, the company must be notified of any changes to the information identifying the shareholders or beneficial owner (first name, surname, address) (Art. 697i, 697j para. 2 and 790a para. 2 CO).

b) Ongoing reporting to the reporting entities or company registry

Austria

Based on Art. 3 of the Beneficial Owners Register Act (BORA), legal entities are required to conduct and review their due diligence requirements pursuant to Art. 3 para. 1 BORA at least once a year, and verify whether the beneficial owners listed in the Register are still up-to-date. Moreover, changes related to beneficial ownership have to be reported within four weeks of obtaining knowledge of these changes.

Legal entities will be required to not only perform their due diligence obligation at least once a year, but also to confirm the reported beneficial ownership data within four weeks after the due date of the annual review. All reporting requirements will be enforced by automated coercive penalties.

Belgium

In Belgium, there is a duty for legal entities and arrangements (LE/LA) to update the ultimate beneficial ownership information within a month of the change Such update should be registered directly in the online UBO Register platform. LE/LA also have the duty to confirm on an annual basis that the information registered is up-to-date, accurate and adequate.

Accountants or notaries can also file the UBO information directly in the UBO Register and do the annual confirmation for their clients. They can also choose to send an extract of the register to the legal representative and ask them to confirm the information by directly clicking on a link embedded in the email.

Denmark

In Denmark, corporate and legal entities covered by the BO rules are obliged to register its beneficial owners in the Central Business Register (CVR). If the entity is informed that there might have been a change of the beneficial ownership, the entity is obliged to investigate it and update the registration in the BO registry as soon as possible and no later than within two weeks.

Corporate and legal entities must keep information on the company's beneficial owners, including attempts to identify the beneficial owners, for five years after the ownership ended or identification was attempted. This information shall be provided if for example the Danish Business Authority (DBA), the State Prosecutor for Serious Economic and International Crime (SØIK) or the Danish Tax Agency (SKTST) considers the information necessary to fulfil its supervisory and control tasks. If the company ceases to exist, the last registered management must ensure that information and documentation regarding the investigation into the beneficial owner(s) can be produced five years after the ownership ended or identification was obtained.

In 2020, corporate and legal entities will be required to screen the BO information registered in the CVR at least once a year and, if necessary, update the BO information. The relevant information shall be presented on the meeting where the annual report is approved by the board of directors.

France*

In France, pursuant to Article R. 561-55 of the Monetary and Financial Code, any corporate or legal entity that has change(s) in its beneficial ownership chain needs to file an up-to-date BO document with the "greffier de

commerce" (commercial court's clerk) within 30 days following the change. Corporate and legal entities must keep updated and accurate BO information.

Failure to submit information within appropriate time or to provide accurate information is subject to 6 months of imprisonment and a fine of € 7 500, according to Article L. 561- 49 of the Monetary and Financial Code. Natural persons may also face a disqualification from practice of business activities or a partial privation from national and civil rights. The legal persons convicted may face a sanction payment equal to five times the sanction applicable for natural persons (37 500 euros) and supplementary penalties as described by Article 131.39 of Penal Code.

**yet to undergo mutual evaluation as of September 2019*

Jersey*

Legal Persons required to update the central register within 21 days of any change in beneficial ownership

Under the Control of Borrowing (Jersey) Order 1958 (COBO) every Jersey entity is required to obtain the consent of the Jersey Financial Services Commission (JFSC) on incorporation. The JFSC uses this regime to impose conditions on all Jersey companies which facilitate the collection of beneficial ownership and control information.

All TCSPs must provide information where an individual acquires beneficial ownership of 25% or more (the threshold being flexed on a Risk Based Approach) or becomes a controller (the Jersey Registry adopts the FATF "3 tier test"). TCSPs must notify the Companies Jersey Registry within 21 days of knowledge of a change.

In respect of legal persons formed not by TCSPs but by local residents, under COBO, there has always been a requirement to obtain the permission of the Commission before a change of beneficial ownership and to therefore update the central register upon change of beneficial ownership.

**yet to undergo mutual evaluation as of September 2019*

Italy

Changes to the ownership and control structure of the legal person must be recorded in the Register within different timeframes, namely within 30 days of the notarial act that validates them, in the case of limited liability companies (società a responsabilità limitata; SRL), and once a year for the joint stock companies (società per azioni) (i.e. at the time of filing the annual accounts). Transfers of shares must be filed with the Business

Register by a notary or be performed by a bank or stockbroker in the case of SRL, the information may be filed by notaries or chartered accountants. The checks are performed with respect to the information filed by notaries.

Verification through different means (relevant to core issue 5.3 and 5.4)

81. The effective mechanism also involves active and adequate verification of information to ensure that the information on beneficial ownership is accurate. Verification of information can be conducted through the following means.

Cross-checking

82. Countries may adopt cross-checking measures to verify or/and monitor the information on beneficial ownership, taking advantage of the availability of different information agents. For example, FIs and DNFBPs, as well as tax authorities, can cross-check the basic and beneficial ownership information provided to them by companies with the information available at the at the registry held by the company or by the registry. Obliged parties such as FIs and DNFBPs can also continuously monitor changes in the registries, including designations of violating companies (through automated computerised interfaces) and inquire with their customers with regard to any potential discrepancies.

83. Given the interrelatedness of the information available and the procedures implemented by government authorities, some countries implement automated cross-checking controls among databases held by different government authorities. For example, a common portal is developed so that the system of company registry can cross-check the beneficial ownership database against other government databases (e.g. law enforcement databases, tax administration database, land register, and other open sources) to verify or/and monitor the accuracy of information on beneficial ownership.

84. Some countries have developed a blacklist, where all individuals and organisations listed in the United Nations are included, in addition to any local individual or organisation which is subject to domestic listing. Those who are listed will not be able to register or own or transfer ownership of any kind. Obliged party can cross-check the identity of shareholder/director against the blacklist at the company incorporation and subsequent stages.

Red flags

85. Some countries identify indicators that suggest suspicious activities e.g. a single credit card or email address being used to incorporate many companies, which on the surface are unconnected. The company registry will then report to law enforcement/competent authorities regarding suspicious activities.

86. In some countries, the obliged party determines a set of indicators and then reviews and assesses the legal persons' financial statements to properly identify the nature and size of the business. For example, the obliged party may establish indicators on sector's income specifically cash income, and the level of assets. This is then compared to the industry average. Subsequent abnormal and/or significant results are deemed suspicious and are therefore subject to further assessment.

87. In some countries, the company registry system is capable of detecting any variations in the information submitted by companies (i.e. increase in shares, transfers of ownership) and to also compare the relevant indicators against the industry average. In case of abnormal variations, an alert is triggered and is subsequently sent to the concerned department for further investigation. Where the primary finding does not justify the business purpose of the behaviour that generated the alert, an in-depth investigation is conducted to determine whether such behaviour is associated with ML/TF risks.

Sample testing with public and non-public data

88. Some registries conduct ongoing sample testing or targeted audits to verify or/and monitor the accuracy of information on selected legal persons. In some countries, company registries conduct sample testing for specific industries/ companies of specific business nature/ risk features by using the annual reports provided by companies to conduct periodic verification. They may check the annual report submitted against the information in its database.

Co-ordination among authorities

89. In some countries, relevant obliged parties and authorities (e.g. company registry and tax authorities) have worked closely together on cases of fraud and market manipulation. The authorities may jointly conduct detailed analysis of transactions and trading patterns, leveraging of certain parameters e.g. IP addresses and use of telephone system information. This helps identify connections between beneficial owners and facilitate further investigations.

External parties engaged in verification of register information

90. Some countries introduce a reporting feature on the public register to encourage external parties to voluntarily notify it of suspected errors. Some organisations e.g. NGOs may then undertake data analysis and report on potential inaccuracies and issues of concern. Some countries also require FIs and DNFBPs to report inaccuracies when they conduct CDD process.

Austria

The BO Registry Authority is responsible for ensuring the correctness and completeness of the data as well as for the prevention of money laundering and terrorist financing. To fulfil these obligations, the BO Registry Authority is authorised to carry out analyses, or may at all times request information and documents from legal entities and their beneficial owners and perform off-site analyses of the correctness of beneficial ownership on the bases of the documentation received and other available sources.

Where an obliged entity determines during the application of its due diligence obligations towards customers that a different beneficial owner has been entered as beneficial owner than was determined, and is convinced that the entry is incorrect or incomplete, then the obliged entity may electronically report this case to the BO Registry Authority by setting

a remark – a "red flag" – for the respective legal entity. The same applies to all competent authorities.

By setting a remark the legal entity will automatically be notified about the remark (without identifying the obliged entity that set the remark) and informed that the reported beneficial owners could not be verified and that the legal entity therefore has to examine its report. The remark is only removed if the legal entity then files a new report. However, the remark will still be visible in the historical data.

Consequently, a remark will be visible in all excerpts from the BO Register. In addition the BO Registry Authority is monitoring the list of all remarks set in the register and may request documentation on beneficial ownership if a remark is not resolved by a correct report.

Belgium

In Belgium, a centralised beneficial ownership register (UBO Register) has been implemented for both legal entities and arrangements (LE/LA). It is developed, managed and controlled by the Treasury administration of the Federal Public Service Finance and is separate from the Commerce registry managed by the Federal Public Service Economy.

The UBO register is an online and fully digitalised platform through which all LE/LA can submit and update their UBO information and that can directly be accessed by competent authorities, obliged entities and members of the general public. An additional condition of demonstrating a legitimate interest is applicable to access the UBO information of certain LA.

For data-privacy protection reasons, the access to the platform is only authorised to persons (both nationals and non-nationals) that have a Belgian electronic identity card. The access is also extended to eIDAS (i.e. Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market) compliant jurisdictions.

Considering the limited resources available and extent of the task, the Treasury cannot conduct systematic *ex ante* controls of the information registered by LE/LA. However, in order to ensure a high level of data quality, several control mechanisms have been embedded in the platform. They are intended to avoid mistakes during the registration process and facilitate the implementation of (targeted) controls of the data. These include:

- To avoid spelling mistakes or typos during the registration phase, a direct link has been made between the UBO register and both the commerce registry (for LE/LA) and the national identification registry (for natural persons);

- The connection with the commerce and national register enables the prefilling of all the information pertaining to the LE/LA and the natural person available in those registries. This prefilling must however be confirmed by the legal representative of the LE/LA, the purpose being to avoid extracting inaccurate, inadequate or outdated information. If the information is not correct, the LE/LA will have to modify it directly at the commerce or national registry. It has been observed that during the registration of their UBO, LE/LA realise that the information is not up to date in the Commerce registry and make the necessary changes in said registry; this mechanism thus also enhances the quality of the information available in the commerce registry;
- This mechanism also enables the Treasury to implement the "only-once" regulatory framework by allowing public authorities to request the communication of an information/document if it has already been provided to another public authority; the resulting process is therefore less costly and more efficient for LE/LA and public authorities;
- Several business rules have also been set to avoid the registration of certain situations (e.g. ownership of more than 100% of the shares/voting rights, registration of a deceased person or a Belgian national that is not registered in the national register of natural persons, start of control before the incorporation of the company).

China

Under the current AML laws and regulations of China, all regulated institutions are required to establish and formulate proper CDD processes. The CDD process is embedded into various operational workflows of the organisation in order to improve the process effectiveness. The verification of corporate customers can be conducted through the National Enterprise Credit Information Publicity System established by the State Administration of Industry and Commerce, to verify the licenses, certification documents and the operation status of licenses in accordance with the law. The regulated institutions will not establish relationships or engage in business before CDD is completed. FIs should obtain information and materials related to legal person while conducting CDD to identify BO, which is very helpful for verifying the materials required in the CDD process.

The regulated institutions would commonly make use of either the official public channels to enquire and verify customer information, as well as maintain on-going understanding of the customers' background. The official public channels including Administration of Industrial and Commercial Registration Information System, National Enterprise Credit Information Publicity System, Unified Social Credit Code Inquiry of National

Organization System, Commercial Entity Registration Information Platform, Commercial Entity Credit Information Publicity Platform, Tax Registration Inquiry System and so on. The "grey lists" and "black lists" on the National Enterprises Credit Information Publicity System (NECIPS) are not only the sanction lists, but also the red flags. Once FIs find legal persons listed in these lists, they will conduct enhanced CDD measures and require more materials in identifying BO, which will in turn ensure the accuracy of BO information in FIs.

Denmark

Cross-checking

Denmark operates with an official online company registry called the Central Business Register (CVR). The CVR contains and publishes free of charge information on legal entities registered according to both company law and tax law. To secure data quality, several automatic control mechanisms have been incorporated in the Business Register. They are intended to avoid mistakes during the registration process and facilitate the implementation of targeted control. The CVR automatically checks information that is filed (which must be done electronically), and will cross-check this information with various governmental registers, the CPR number - Civil registration number / CVR number - Unique identification number for legal entities and other details such as address (Danish Address Register - DAR) and dates. Furthermore, business rules are set up in the system to avoid impossible situations ex. registration of a deceased person, and as the Business Register entails information about legal entities, certain information about the entity is prefilled in order to ease the registration and to avoid mistakes. These automated checks are then followed by more detailed manual checks in suspicious cases. The system is also designed to use large datasets and with machine learning to better identify potential risks.

Sample testing/checking

To ensure that BO information in the CVR is accurate and current, the Danish Business Authority (DBA) starts to select and manually control 500 companies and their registration of BOs in 2019.

The control is divided into two approaches: In the registration phase, and after the information is registered. In the registration phase, the BO information is in specific suspicious cases checked and verified by the DBA before the incorporation of the company is completed. If the BO information is not adequate when checked, the company will not be incorporated. If the BO information is checked in the following phase, the DBA has the legal basis to dissolve the company compulsorily. The possibility to enforce the winding up relates to both missing and inadequate

BO information and can also be used if the corporate or other legal entity does not hold BO information or the information held is inadequate.

External parties engaged in verification of register information

In 2020, entities within the CDD framework will be obliged to report to the DBA any discrepant BO information available in the CVR and the BO information available to them. In case of reported discrepancies, the relevant authority must take actions to resolve the discrepancies. It is possible for the DBA to make a note in the CVR about the reported discrepancy.

France*

In France, the verification of information is two-fold: firstly, the clerk verifies that the company has submitted all the necessary information. Secondly, the clerk verifies the declared information by mainly cross-checking against information held by the Trade Register.

As of April 2019, (Art. 561 46-3), the information contained in this register can be disclosed to : the legal entity itself, one of the 18 competent authorities, one of the entities subject to AML/CFT obligations or any person justifying a legitimate interest and authorised by the judge responsible for the surveillance of the BO register.

**yet to undergo mutual evaluation as of September 2019*

Hong Kong, China

The Companies Registry (CR) has introduced a complaint form for reporting breaches of the Companies Ordinance (CO). Companies or members of public can use the form to report any breaches of the CO (including failure to keep a Significant Controllers Register) to the CR for investigation.

The introduction of the complaint form greatly facilitates the public members to report any breaches of the Companies Ordinance to the CR in a timely manner. Among the 2 310 complaints received by CR between 2017 and 2019 (up to July), 40% of them were reported via the complaint forms.

Ireland

Data interfaces have been established between the Companies Registration Office (CRO) and Revenue, as the two key data repositories of corporate information in Ireland. Such interfaces allow the authorities to conduct ongoing red-flag monitoring and some verification of the information held. For example, Ireland has assessed that higher ML/TF and tax evasion risks attach to entities which, although incorporated through CRO, fail to engage with Revenue. The interface between CRO and the Revenue combats risks associated with 'non-engaged' entities and enquiry letters are generated.

The Netherlands*

The automated information system TRACK of the Scrutiny, Integrity and Screening Agency (part of the Ministry of Justice and Security) continuously monitors the integrity of legal persons, including its directors and affiliated persons or legal persons. The system was introduced in January 2011.

The Scrutiny, Integrity and Screening Agency performs risks analysis by automatically scanning several closed and public sources on a daily basis, to look for any relevant financial or criminal records of directors, and the (legal) persons in their immediate surroundings. Data includes the Company Registry, Citizens Registry of the municipalities and the Central Insolvency Registry, as well as other public sources. In addition, data is obtained from the tax authorities, the Judicial Information Service, and the National Police Services Agency. If the computer system reveals a heightened risk, either immediately upon registration or later on, during the life span of the legal person, this dedicated Agency will carry out a more in-depth analysis. If the analysis confirms that there is indeed a heightened risk, a risk alert will be sent to a group of recipients, including law enforcement and supervisory authorities such as the Public Prosecution Service, the Police, the Tax Intelligence and Investigation Service, the Dutch Central Bank, the Netherlands Authority for the Financial Markets and the Tax and Customs Administration. In 2018, 264 of such risk alerts were made, and another 50 in the first quarter of 2019. A risk analysis can also be performed upon request from these authorities. In 2018, 17 risk alerts were made following a request.

The Scrutiny, Integrity and Screening Agency also provides 'network maps' for inter alia law enforcement and supervisory agencies. A network map plots the relevant relationships between a (legal) person of interest, and other persons or legal persons, including bankrupted or disincorporated legal persons. In 2018, the agency provided 947 network maps, and 217 in the first quarter of 2019.

**yet to undergo mutual evaluation as of September 2019*

The United Kingdom

Civil society using PSC information

In November 2016, Global Witness worked in collaboration with DataKind UK, OpenCorporates, Spend Network and OCCRP to bring together a team of 30 volunteer data scientists to analyse the information provided in the first batch of data from the person with significant control (PSC) register. The team worked on the first three months' worth of data available (around 1.3 million companies out of 3.5 million). In a weekend, the team were able to provide a number of insights which illustrate the value and potential use of public PSC information:

- The team were able to build a map of complex corporate structures. As an example, they partially mapped the ownership structures of Reckitt Benckiser, the healthcare company. The PSC data enabled them to develop an understanding of complex ownership structures and while they did not identify any wrongdoing, it shows how the information can be used to increase transparency.
- The team were able to identify 9 800 companies that listed their beneficial owner as a foreign company. This is allowed if the foreign company was listed on one of the stock exchanges deemed equivalent to the UK system (e.g. the US, EU and Japanese exchanges).

Global Witness informed Companies House that there were over 4 000 companies who appeared to have filed details of a relevant legal entity (RLE) who may not be registrable; as they were based in jurisdictions such as Costa Rica, Panama and the Isle of Man. Companies House have taken action by writing to these companies. Upon receipt of the information, approximately 70% of the companies had already corrected their PSC information on the Companies House register. While Companies House would have identified many of these errors, by having publicly accessible information, it has accelerated the identification of these issues.

Sweden

Flagging suspected incorrect information in the beneficial ownership register

The Swedish system for information on beneficial ownership is based on a combination of the Company Approach and the Registry Approach. A report to the registry is made by a representative of the legal person and signed electronically.

The register of beneficial ownership is publicly accessible. In case the quality of an entry in the register is insufficient, relevant FIs, DNFBPs or state authorities are obliged to report this to the registry authority. The registry authority will then evaluate if the registered information is incorrect based on the report. If so, an official notice will be given to the

legal person either to submit a correction or to submit additional information that supports the registered information as correct. If that is not done, another official notice will be sent with an administrative fee. This has proven to be an effective measure during the relatively short period of time the Swedish register has been in effect. Most legal persons who receive the first official notice file a correction within the required timeframe.

Apart from keeping the registered information in the register correct through official notices, the registry authority may flag up registered information connected a the legal person with a warning triangle and an explicatory text that the registry authority has reason to presume that the information is incorrect. This flag is shown to anyone looking at the legal person in the registry and remains until a report with correct information has been registered. The flag functions as a warning for FIs, DNFBPs or any other party dealing with the legal person. This is an indication in a CDD situation that caution is needed and that clarifications should be requested before initiating or continuing a business relationship.

Enhanced measures for companies with foreign ownership/directorship (relevant to core issue 5.3 and 5.4)

91. It is understood that foreign ownership/directorship is a main concern on tracing beneficial ownership of legal persons.

92. In some countries, foreign individuals/legal persons who wish to carry out business or acquire ownership of local companies must obtain another licence from a designated competent authority. As part of the application process, the individual/legal person is required to provide a comprehensive set of information, including on the financial standing of the foreign individual/legal person, the ownership and control structure of the foreign legal person, and copies of founding documents and agreements regulating the powers to bind the legal person. Certified documents by obliged party have to be provided. The obliged party is required to undertake enhanced CDD and undertake a comprehensive screening and verification of each applicant's financial background, ownership and control structure, previous commercial activity, etc.

In some countries, where a shareholder/director is not a local citizen, the registry authority requires the applicant to provide a certified copy of the passport for individuals and a certified certificate of incorporation for legal persons. Some countries rely on the certification by an obliged party, or by an official local representative in the foreign country where the passport or certificate was issued to conduct verification to this group of foreign shareholders/ directors.

Austria

As part of the risk based approach of the BO Registry Authority, legal entities, which report beneficial owners with foreign citizenship or place of residence, or ultimate legal entities with a registered address in a foreign

country will receive a certain number of risk points based on the ISO Code of the foreign country. Thus those legal entities will be more likely be in the risk category high or very high, resulting in a greater chance that the BO Registry Authority will request documentation on beneficial ownership and will carry out an off-site analyses of beneficial ownership.

Belgium

The electronic identification system ("eID") in Belgium implemented since 2002 greatly facilitates the identification process of foreign citizens that had a prior contact with an administrative authority in Belgium.

If a foreign citizen has been in contact with an authority in Belgium for any reason, e.g. for VAT or other fiscal purpose, traffic offence, employment, they will be assigned a unique eID number that will be registered in the national register for natural persons. This eID will be used to identify them in the UBO register and verified by an authority.

In the medium term, the EU eIDAS (electronic IDentification, Authentication and trust Services) Regulation aims to ensure that people and businesses can use their own national eID schemes to access public services in other EU countries where eID is available. For non-EU citizens that do not have any (compatible) EU eID, several solutions are being investigated besides the request for substantiating documents upon registration (e.g. simplified remote authentication method).

Denmark

Under the beneficial ownership legislation, corporate and other legal entities are obliged to register BO information in the Central Business Register. This applies whether it is a foreign or national beneficial owner. If a beneficial owner is a foreign citizen, further registration information is necessary e.g. copy of passport, national identification number etc.

Hong Kong, China

Under Part 16 of the Companies Ordinance (CO), a non-Hong Kong company that has established a place of business in HKC is required to register under the CO. Corporate documents of the non-Hong Kong company such as constitution, certificate of incorporation and latest accounts have to be delivered together with the application of registration. Such corporate documents have to be certified in accordance with s.775 of the CO. For example, they should be certified by a notary public, lawyer, professional accountant, professional company secretary, etc.

Jersey

Foreign owned are subject to enhanced requirements reflecting their higher risk

All Jersey companies that are foreign owned are subject to enhanced requirements reflecting their higher risk.

The beneficial owners and controllers of companies, which will be owned by local residents, are subject to identity checks by the Companies Registry on incorporation and when new beneficial owners and controllers become connected with the company.

In addition to those checks, all companies incorporated at the behest of a foreign owner must engage the administration services of a locally regulated TCSP which is subject to AML/CFT regulation. The TCSP will hold the certified copy and conduct risk-based due diligence.

The Taxation (Companies – Economic Substance) (Jersey) Law 2019 strengthens the requirement for Jersey companies to demonstrate real economic substance in the Island and the overall level of responsibility that Jersey-resident directors shall take in relation to foreign-owned companies that they direct and administer.

The Netherlands*

There is a general obligation for all foreign incorporated companies with an office in the Netherlands, or who provide employment in the Netherlands, to register basic company information in the company register of the Dutch Chamber of Commerce.

FIs and DNFBPs are obliged to perform enhanced CDD if the country of residence of the customer is declared a high-risk country by the European Commission.

**yet to undergo mutual evaluation as of September 2019*

Switzerland

Enhanced measures for the identification of beneficial owners of non-operational legal entities (domiciliary companies)

The risk of the abuse of legal persons is taken into account in preventive due diligence measures applicable by the financial intermediaries. The complexity of the structures involved in the business relationship, particularly the use of domiciliary companies, whether Swiss or foreign, is one of the criteria of higher risk according to Art. 13(2)(h)of the FINMA

Anti-Money Laundering Ordinance (OBA-FINMA). Art. 2a OBA-FINMA defines domiciliary companies as entities such as legal entities, trusts or foundations, that do not have any operational activity. They do not carry out any commercial or manufacturing activity or any other activity as a commercial enterprise. Financial intermediaries adopt a very prudent approach with such types of entities and do not enter into business relations when a natural person cannot be identified as the actual beneficial owner of the company. A written declaration will be required from the domiciliary concerning its beneficial owners. (Art. 4 para. 2 of the Federal Act on Combating Money Laundering Act and Terrorist Financing). The threshold of 25% of the capital or voting rights in the legal entity does not apply to such type of entities. This means that all beneficial owners must be identified, regardless of the amount of their participation in the company.

Highly effective law enforcement authorities with adequate resources (relevant to core issue 5.4)

93. In some countries, the AML supervisors/law enforcement authorities (LEAs) prioritise ML/TF and financial investigations, and routinely and proactively pursues ML/TF investigations. Investigative tools and information-sharing gateways are robust, and resources are applied flexibly both within and across enforcement agencies to respond to investigative needs.

94. Where prosecution is not possible, LEAs actively use a wide array of other alternative measures to disrupt offenders, including pursuing the predicate offence, seeking civil recovery, taking action for tax offences, or obtaining serious crime prevention orders to restrict behaviour. The efforts are supported by adequate human and capital resources.

The Netherlands*

Dutch law enforcement agencies work closely and share information with each other, as well as with other agencies such as the Tax and Customs Administration. The national police and the Tax Intelligence and Investigation Service (in Dutch: Fiscale Inlichtingen en Opsporingsdienst or FIOD), which both work under the authority of the Public Prosecution Service investigate suspected ML/TF criminal activity and carry out extensive law enforcement measures. These authorities also work together in the Dutch Financial Expertise Centre (FEC), which is a partnership among authorities that carry out supervisory, prosecution or investigation activities in the financial sector. Partners of the FEC are: Dutch Central Bank DNB, AFM Netherlands Authority for the Financial Markets, FIU-Netherlands, Tax and Customs Administration, Tax Intelligence and Investigation Service (FIOD), National Police and the Public Prosecution Service. The Ministry of Finance and the Ministry of Justice and Security act as observers. The FEC also plays an important role in providing and

disseminating information. The various criminal law enforcement agencies, FIU-Netherlands and the Public Prosecution Service also work together in the Anti Money Laundering Centre.

**yet to undergo mutual evaluation as of September 2019*

The United Kingdom

The UK competent authorities manage to use Companies House records to identify those individuals acting as company officers, and undertake further enquiries to test the credibility of their appointments and of the company, through the examination of company records, tax returns, and both corporate and individual financial activity. Sometimes, these enquiries showed that the company officers were simply acting as the agent of the defendant, and knew nothing about the operation of each company. These companies were used as a device to hide the beneficial ownership of the assets.

Using technology to facilitate checking and validation (relevant to core issue 5.3 and 5.4)

95. In some countries, basic checks are conducted by the IT system in the company registry upon registration. They include an automated calculation of shares and of the capital as well as an automated validation of information such as the tax identification number entered, digital signature–and therefore the identify–of the applicant, and of the payment of the mandatory fees and taxes.

96. Some systems will perform automated checks when there is new information entered into the system (for example to ensure that shares are only transferred by persons who are already in the system). Any anomaly highlighted by these automated checks is analysed by the register staff before the publication is authorised.

97. In some countries, data mining technology is used to cross-check the information available and report suspicious activities to the various authorities. False information can be easily detected and the system can help highlight any inconsistency. Some countries even appoint a dedicated data miner to monitor cross-checking systems among different databases in order to ensure compliance of requirements on beneficial ownership.

98. For countries that adopted a national standardised electronic identification system, such electronic ID (for all directors and authorised signatories) is one of the required information to register companies in the company registry. Competent authorities can also make use of trustworthy electronic identification system to gather information.

Austria

The BO Register integrates existing information from other registers, such as the Central Register of Residents related to information on the beneficial owner or the other national registers containing information about legal entities concerning the reporting of ultimate beneficial ownership of legal entities.

Through an automated alignment with other registers, it is ensured that beneficial owners and legal entities can only be reported if their data is also contained in other public registers. If, for example, a person with a main residence address in Austria is entered as a beneficial owner, there is a real time check with the Central Residence Register in the background if the entered person has a valid main residence in Austria.

Another key factor is the reporting form for reporting beneficial ownership itself. The reporting form provides a digital guidance throughout the reporting process and makes reporting for both legal entities and their legal professionals as easy as possible. The reporting form itself is dynamic and tailor made to the specific legal form for which the report is made. Incorrect reports can be prevented largely by built-in conditions and error indications.

Denmark

Information on any natural person registered in the Central Business Register (CVR) is updated automatically for all Danish persons from the Danish CPR-register. The DBA's IT-system (CVR) also automatically checks the business address in the Danish Address Register (DAR) to make sure that the address exists. When a new business is registered or changes are made to a governing body, the DBA's IT-system (CVR) will automatically notify the affected person(s) to make sure that the changes are correct.

The digital self-registration systems have been designed with several built-in minimum requirements that must be met for completion of the registration. These include that certain types of document must be enclosed with the individual type of registration case, as well as requirements for the information that must be disclosed to the DBA. The IT-system (CVR) is under an ongoing development and most recent developments is using machine learning to check enclosed documents signatures and read if certain documents entail demanded text and conclusions. The DBA can perform checks to verify the registrations. In these cases, DBA can ask for documentation for the registrations. If the company cannot provide this, or the incorrect registrations are not rectified, DBA can enforce a forced winding up.

With the modernisation of IT systems for company registrations, the DBA has enhanced its enforcement activities to prevent misuse and to check

registrations, including 1) activities that take place automatically in connection with a registration in the DBA's systems, and 2) the manual follow-up activities that the DBA conducts up to three years after the registration.

Italy

The MOLECOLA platform* used by the Guardia di Finanza (GdF, the financial police), facilitates the identification of the real beneficial owner of legal persons incorporated in Italy by processing the information maintained in various sources (Business Register, law enforcement databases, tax administration database, land register, lists of designated persons under the United Nationals Security Council Resolutions (UNSCRs), and other open sources). As established in the cases provided, this has enabled the GdF to successfully identify the ultimate beneficial owner in a number of instances, including in cases involving complex, transnational corporate structures. The MOLECOLA platform has proven useful notably by considerably reducing the length of time needed to conduct cross-checks.

**MOLECOLA: This tool is used in financial investigations with software integrated within GdF and National Anti-mafia Directorate (Direzione Nazionale Antimafia). MOLECOLA imports electronically bulk information from different databases (e.g., the various law enforcement databases, tax administration database, land register, company register and information from other open sources). The information is analysed according to the operational activities investigated, allowing to elaborate standardised reports suitable for investigations and also operational analysis reports detecting links between people and financial operations, and the disproportion between incomes and expenses of the persons that are under investigation.*

The Netherlands*

The company register of the Dutch Chamber of Commerce performs automatic checks of specific information upon registration. For example, information on the identity of natural persons is checked against the citizens register (in Dutch: BRP or Basis register personen) automatically, amongst which the name, date of birth and the Dutch Citizen Service Number (Burgerservicenummer or BSN).

**yet to undergo mutual evaluation as of September 2019*

Access by competent authorities *(relevant to core issue 5.4)*

99. Competent authorities (including LEAs) may have direct access to the beneficial ownership information held by company registry, database held by other competent authorities and information held in FIs and DNFBPs (e.g. notaries' database). According to the 2018 FATF-Egmont report, FIUs should have access to the widest possible range of financial information. Consideration of possible measures to increase the breadth and depth of information available to FIUs is merited.

100. In some countries, competent authorities have direct access to the beneficial ownership information through the company registries and the centralised database kept by notary profession, which ensures the timeliness of the access to information on beneficial ownership. The private sector discloses information to the competent authorities in due time and within the time limits set by the requesting authority. Whenever necessary, the information is collected directly from and/or verified directly with the companies. Competent authorities (especially LEAs) can also compel the provision of beneficial ownership information through available investigative measures such as production or disclosure orders. Production orders can be obtained relatively quickly through an electronic filing and granting system. Moreover, access has been authorised by the data protection agency so that there is no impediment to competent authorities in obtaining information on beneficial ownership.

Belgium

In Belgium, the Ultimate Beneficial Owner register (UBO register) is accessible by competent authorities. The Security officer or Data Privacy Officer of each competent authority will be granted the right to manage the access to the platform for the employees of said competent authorities. This Security or Data Protection Officer is tasked to authorise any agent of the competent authority to consult the UBO register in accordance with the law. Such a system enables the Treasury to:

- Enable competent authorities to have access to the past and present UBO information instantly;
- Offer flexibility to competent authorities in the internal organisation of the accesses. They will be able to tailor the access to their needs and specificities. Subsequently, certain entities limit the access to the UBO register to certain categories of agents or employees (e.g. head of departments, specially designated investigators…);
- Assign clear responsibilities. The responsibility to consult the UBO register in accordance with the AML/CFT and UBO regulation lays on the competent authority and its agents;

This system also enables the Treasury to keep track of the logs of each user, for data privacy concerns and in order to enable an audit to be conducted on the use of the information.

Germany*

In Germany, access to the Transparency Register is possible through a central platform. The access is available depending on the type of the applicant. There are three possible types of applicants.

- Competent authorities are granted access for fulfilling their legal requirements. They have, as far as it is necessary in fulfilling their statutory tasks, full access to the database of the Transparency Register.
- Obliged entities are granted access to the register if they inspect the entries in the Transparency Register while acting in the exercise of their professional activities to fulfil due diligences. Obliged entities are for example credit institutions, financial companies, auditors, chartered accountants or tax advisors.
- Any natural or legal person, domestic or foreign, that can demonstrate a legitimate interest can access the information available. The decision is made on a case-by-case basis.

**yet to undergo mutual evaluation as of September 2019*

France*

According to article L. 561-46 of the CMF, 18 of competent authorities shall have access to the beneficial ownership register among which :

- Judicial authorities;
- The national Financial Intelligence Unit (FIU);
- The custom administration officials;
- The public finances officials in charge of control and recovery in fiscal matters.

The French FIU has a direct access to the electronic beneficial ownership register. When orientating the information or when further investigating, FIU officials are able to check instantly all the information transmitted by the company to the "greffier de commerce" (commercial court's clerk) when registering as mentioned above.

The aforementioned provisions differ from those of Section 3 of the Monetary and Financial Code on customer due diligences which provide that obliged entities shall identify the beneficial owner before entering in a business relationship or before performing a transaction. After applying those due diligences on beneficial ownership, if they suspect or know that the operation which is about to be performed is linked with ML or FT, they must transmit the information to the FIU.

Therefore, the French FIU has two different sources of information on beneficial ownership at its disposal and is able to cross-check it.

**yet to undergo mutual evaluation as of September 2019*

Hong Kong, China

On demand by a law enforcement officer for the purpose of performance of functions relating to the prevention, detection or investigation of money laundering or terrorist financing, a company must at any reasonable time make its Significant Controllers Register (SCR) available for inspection by the officer at the place at which the SCR is kept and permit the officer to make copies (s.653X of the Companies Ordinance (CO)). If the company fails to comply with the requirements of s.653X, the law enforcement officer can apply to the Court for a court order to direct the company to permit the inspection or making copies of the SCR (ss.653Y and 653Z of the CO).

Jersey

Jersey's FIU, the Joint Financial Crimes Unit of the States of Jersey Police (JFCU), has direct access to the register of beneficial ownership and control through a dedicated portal in the JFCU's headquarters. Searches can be made for entities based on entity registration number, name and/or country of incorporation. Searches can also be made for natural persons based on first name, surname, alias, date of birth and/or nationality.

The JFCU also acts as the designated contact point for exchanging beneficial owner and controller information with foreign law enforcement agencies. Since 1 July 2017, an agreement between Jersey and the United Kingdom has been in place to enhance the speed of information exchange between the jurisdictions (the 'Exchange of Notes'). The Exchange of Notes agreement provides for the exchange of adequate, accurate and current beneficial ownership information between Jersey and the UK within 24 hours on a normal request, or within 1 hour, where the request is urgent (due to TF concerns, for example).

Switzerland

In Switzerland, legal entities (public companies, private limited liability companies and cooperative companies) must be represented by individuals (directors or managers) domiciled in Switzerland. The presence of a representative of the company in Switzerland facilitates the cooperation with the competent authorities and timely access by authorities to beneficial ownership information, especially in case the information spans several jurisdictions.

The United Kingdom

UK authorities are able to access basic and BO information on legal persons and arrangements via one of three sources: from financial institutions and DNFBPs, from registers, or from the legal entity itself. The variety of sources increases transparency and access to information, and helps mitigate accuracy problems with particular sources.

There are several channels available for LEAs to obtain information on legal entities from FIs and DNFBPs. At the intelligence-gathering stage, LEAs can request information through Joint Money Laundering Intelligence Task Force (JMLIT) provided the request is justified, proportionate and necessary.

LEAs can also compel the provision of BO information through available investigative measures such as production or disclosure orders. These orders require judicial authorisation, which can be obtained in a matter of hours for urgent cases. Production orders can be obtained relatively quickly through an electronic filing and granting system. Once issued, the orders typically receive a response within seven days, although immediate disclosure can also be sought. Both production and disclosure orders require suspicion of an indictable offence so are used at the investigative stage once sufficient evidence has been collected to meet this threshold. The Serious Fraud Office (SFO) has access to additional investigative powers to compel the provision of information believed to be relevant to an investigation or inquiry within a timeframe set by the SFO (typically no longer than 14 days).

Forbidding or immobilising bearer shares and nominee arrangements (*relevant to core issue 5.3)*

101. The Interpretive Note to R.24 requires countries to take measures to prevent the misuse of bearer shares and bearer share warrants, as well as the misuse of nominee shares and nominee directors. Measures include prohibiting, dematerialising, immobilising and disclosing them. According to the 2018 FATF-Egmont report, given the vulnerabilities associated with use of nominees, individual countries and the FATF, working with the broader global community may wish to consider measures to limit their misuse.

102. In some countries, shares may be issued in bearer form in limited circumstances, and must be dematerialised. They must be deposited with a central depository and the exercise of the rights that they confer may only be performed through a reporting entity. The central deposit opens an account for each intermediary to record the movements of the financial instruments deposited into that account. In some countries, the holder of bearer shares is obliged to declare purchase or transfer of shares within a specified timeframe, and done through an obliged entity.

103. In some countries, shareholders may be represented by third parties, but the latter may only intervene on their behalf on the basis of a duly signed power of

attorney, which ensures the transparency of the operation. Companies must maintain a copy of the power of lawyer when the non-shareholder third party exercises the rights carried by the shares in the company's general assembly. The same applies to notaries (and, where relevant, accountants), in the case of a transfer of the shares performed by the third party on behalf of the shareholder, and the normal CDD requirements apply.

104. In most of the cases, although bearer shares and bearer shares warrants are not explicitly prohibited, there is no real incentive because of the lack of legal protection offered. The same applies to the nominee arrangement.

Demark

Corporate and legal entities are required to identify those individuals exercising their rights through a nominee scheme and hold information about this. A person may not exercise the rights conferred to an owner of capital unless he/she is registered in the registry of owners or has notified and documented the acquisition.

In 2015, Denmark abolished the possibility to issue bearer shares and established an obligation for holders of bearer shares below 5% to register those shares with the Danish Business Authority.

France*

Since April 2016, bearer shares are necessarily nominatives: from subscription, the bearer designates a beneficiary by its name (this latter being himself most of the time) without any possibility of further modification. This beneficiary can ask for the reimbursement of the share if he is in its possession.

**yet to undergo mutual evaluation as of September 2019*

Hong Kong, China

Since March 2014, Hong Kong, China (HKC) has prohibited the issue of bearer share warrants.

Section 6, Division 2, Schedule 5A of the Companies Ordinance (CO) states that a share held by a nominee for another person is regarded as being held by "that other person". If the nominee holds more than 25% of the issued shares of the company, "that other person" should be identified by the company and be entered into the Significant Controllers Register. Moreover, anyone who by way of business acts or arranges for another person to act as a shareholder or a director of a company for another person would be considered to be providing trust or company service under Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) and is required to obtain a license from the CR to do so. Since March 2018,

licensees are subject to statutory customer due diligence and record-keeping requirements under AMLO.

HKC applies director duties to "shadow directors". Under the interpretation of the Companies Ordinance (Cap. 622 of the Laws of Hong Kong), "director" includes any person occupying the position of director (by whatever name called). Under section 3 of the CO, the "responsible person" in the context of a contravention of the Ordinance, or of a requirement, direction, condition or order, includes an officer or shadow director who authorises or permits, or participates in, the contravention or failure.

The Netherlands*

The Netherlands prohibits companies from issuing bearer shares, and requires holders of bearer shares to change them to regular registered shares at the issuing company, or to deposit and register their shares at a central institution (Euroclear) or an intermediary such as a bank or investment firm. Companies are obliged to alter their articles of association, insofar necessary, to allow bearer shares to be changed to registered shares. Any bearer shares not deposited or registered before 1 January 2020 are deemed to be registered shares.

After this date, holders of (former) bearer shares that have not presented them to the company, nor deposited them at the central institution or an intermediary, cannot exercise their rights under those shares, such as voting rights and rights to dividend. All (former) bearer shares have to be presented at the issuing company or deposited at the central institution or intermediary before 31 December 2020. After the deadline, the issuing company will become the owner of these unregistered (former) bearer shares. Holders of (former) bearer shares then have a final chance to receive their registered shares by presenting their former bearer shares to the issuing company before 1 January 2026.

**yet to undergo mutual evaluation as of September 2019*

Switzerland

In Switzerland, there are mechanisms for identifying the holders of bearer shares, along with obligations on purchasers of such shares to declare their identity to the company either themselves or through a financial intermediary, and on the company to keep a list of the holders of these shares. Furthermore, the conversion of these shares into registered shares is facilitated: according to Art. 704a of the Code of Obligations, the shareholders' meeting may decide by a majority of the votes, to convert bearer shares in-to registered shares. The decision to convert must be taken by a simple majority, since it is prohibited to set a higher quorum in the Articles of Association.

Effective, proportionate and dissuasive sanctions *(relevant to core issue 5.6)*

105. Effective, proportionate and dissuasive sanctions may range from administrative sanctions and prosecution action against corporate entities that fail to comply with information filings. These include rejection of registration or business relationships, de-registration and abortion of business relationships, fines and penalties or criminal sanctions, measures taken by the courts to dissolve legal entities involved in ML schemes, or seize their assets.

106. In some countries, company registry, notaries and others obliged parties do not proceed with the requested activity in the absence of all the requested information. Entities that fail to provide information on beneficial ownership is not possible to register as a company or establish a business relationship with FIs or DNFBPs. Companies that fail to complete the required annual filings of information are ultimately liable to be struck off the company register. A change in legal status will not take effect if it is not recorded with and verified by the company registry/obliged entity. This significantly limits the ability of companies to obtain credit, change the company name or purpose, and register mergers. In some cases, the company registry can also deny the controlling shareholder and any director who has not paid a fine from registering new companies.

107. In some countries, disclosure of false information to notaries constitutes a criminal offence. In some cases, the courts are even empowered to dissolve legal entities involved in ML schemes, and or seize their assets. This forms a strong deterrent to the misuse of legal persons.

Austria

Under the Beneficial Owners Register Act (BORA), it will be penalised to violate the reporting obligation either by an incorrect or incomplete report or by a failure to submit a report with up to € 200 000 for intentional acts or up to € 100 000 for gross negligence (Art. 15 para. 1 BORA). This includes in particular the following cases: Inaccurate report of beneficial owners, unclear information leading to inability to identify beneficial owner, annual reporting obligation has not been fulfilled, report was not made within the statutory time periods; cases in which the legal entities are exempt from the reporting obligation, but have not reported another natural person as the beneficial owner through control (the additional beneficial owners are beneficial owners through a Treuhand or other control relationships) have not been reported to the BO Register; cases of not reporting changes of beneficial owners within four weeks of obtaining knowledge of the changes.

In case of a persistent failure to report, coercive penalties will be imposed twice according to Art. 16 BORA.

In addition, it will be sanctioned with up to € 75 000 for intentional acts or up to € 25 000 for gross negligence, if the legal entity has breached its obligation to retain copies of the documents and information required for their due diligence obligations based on the BORA.

Cases, where the correct information about beneficial owners has been reported, but in the course of the voluntary submission of a Compliance-Package false or falsified documents are transmitted to the BO Register, will be punished with up to € 75 000.

Cases, in which beneficial owners have been disclosed but individual details of beneficial owners are incorrect or missing or in which no copies of an official photo ID are submitted with the report, will be punished with up to € 25 000.

Cases, where the legal entity seemed to intend to provide a correct report but in which individual documents with the submission of the voluntary submission of a Compliance-Package were not transmitted or cases, where other obligations in relation to the submission of a Compliance-Package, that are not already covered by an individual sanction, will be punished with up to € 10 000.

Compliance with the obligation to report is ensured on an ongoing basis through the implementation of automated coercive penalties. If a report is not filed within the deadline – either within the initial reporting period or within 28 days of newly established legal entities – then the competent tax office will automatically send a reminder letter with the threat of a coercive penalty of € 1 000 to the legal entity. If the legal entity fails to report within the deadline given in the reminder, the penalty will be set and a higher penalty of € 4 à00 is threatened. If the legal entity still fails to report within the given deadline, the coercive penalty of € 4 000 will be set and the case will be forwarded to the responsible fiscal penal authority.

With this automated system, the BO Registry Authority was able to achieve an overall reporting rate of more than 93% as of July 2019.

Belgium

In Belgium, penalty (€ 4K-40K) and administrative fines (€ 250-50K) are available in case of non-compliance by legal entities and arrangements (LE/LA) with their obligation to hold information on their ultimate beneficial ownership (UBO) and register it.

The Treasury has identified additional mechanisms that could be implemented in the medium/long term. These include:

- Procedures for “automatic” administrative fines;
- Consider declarations as non-valid if no substantiating documents are provided;
- Loss/suspension of the rights associated with shares or suspension of the payment of dividends;
- Duty for UBOs to notify their status to LE/LA;
- Duty to notify when an intermediate LE/LA or a legal person refuses to provide UBO information
- Publication of a black list of non-compliant LE/LA;
- System of flags based on, among others, notifications received.

Denmark

The Danish Business Authority (DBA) can demand the documentation that prove the validity of the information registered within 3 years after a registration has taken place. If the documentation or the circumstances under which the registration has taken place is not sufficient, the DBA can file a report to the police or impose a daily/weekly fine to the company until the registration is complete.

Registering BO information is a pre-requisite to get a CVR-number for most types of legal persons. It is also possible to enforce a winding up of the existing entities if there is no or inadequate beneficial ownership information registered / inadequate recordkeeping. If a company does not register the BO information or provide it to the authorities, the company and their management have committed a criminal offence. If the company has an auditor (which most have), the auditor is legally obliged (according to the Danish audit regulation) to check if the management has fulfilled its obligations in the company law. If not, the auditor must make a note in the annual report about the offence of the company law. This way non-compliance of BO-registration will be visible in the annual report to the company stakeholders.

Compulsory dissolution is also possible if a corporate or other legal entity has not registered BO information or the registered information or recordkeeping is inadequate. It is possible to strike off Partnerships (I/S) and Limited Partnerships (K/S) (that are required to register accordingly to the Certain Commercial Undertakings Act) from the CVR register due to inadequate beneficial ownership information or recordkeeping or if no beneficial owners are registered.

By November 2018, the DBA had compulsorily dissolved around 7500 companies that had failed to register their BO information in due course. As of January 2019, approximately 96 % of all entities covered by the BO legislation had registered BO information. And 99.80 % of the entities covered by the company laws under the DBAs area of responsibility had registered BO information.

France*

France introduced dissuasive sanctions in the event of failure to declare a beneficial ownership document containing inaccurate or incomplete information (article L. 561-49 of the Code monétaire et financier (CMF)). In order to reinforce the effectiveness of the system, injunctions and penalties can also be imposed:

- - Art. L. 561-48 of the CMF allows the president of the court, spontaneously or at the request of the public prosecutor or any interested person, to order a company to proceed to the deposit of documents on beneficial owner, if necessary under penalty payments. The president may also appoint someone else to perform these formalities;
- -Art. L. 561-49 of the CMF punishes with imprisonment of 6 months and a fine of 7,500 euros the fact of not filing the document relating to the beneficial or filing a document containing inaccurate or incomplete information. Additional penalties prohibiting management and partial deprivation of civil and civic rights may also be imposed. The maximum amount of the financial penalty is multiplied by five in the case where the author of the breach is a legal person.

**yet to undergo mutual evaluation as of September 2019*

Hong Kong, China

Hong Kong, China (HKC) has various provisions in the Companies Ordinance (Cap. 622 of the Laws of Hong Kong) for sanctions against companies that fail to comply with information filings, below are some examples:

Section 662 of the Companies Ordinance provides that if a company fails to deliver to the Registrar of Companies for registration an annual return within the specified time, the company, and every responsible person of the company, commit an offence, and each is liable to a fine at level 5 (i.e. HK$ 50 000) and, in the case of a continuing offence, to a further fine of $ 1000 for each day during which the offence continues.

HKC will strike companies off the Companies Register if they fail to file annual returns for consecutive years, as this is a cause to believe that the companies are not in operation or carrying on business.

Section 653H of the Companies Ordinance provides that if a company fails to keep a register of its significant controllers, the company, and every responsible person of the company, commit an offence, and each is liable to a fine at level 4 (i.e. HK$ 25 000) and, in the case of a continuing offence, to a further fine of HK$ 700 for each day during which the offence continues.

Under section 895 of the Companies Ordinance, a person commits an offence if, in any return, report, financial statements, certificate or other document, required by or for the purposes of any provision of the Companies Ordinance, the person knowingly or recklessly makes a statement that is misleading, false or deceptive in any material particular. The person is liable on conviction to a fine and imprisonment.

Spain

Corporate criminal liability was introduced in Spain. With the ease of access to basic and beneficial ownership information, the strong preventive measures imposed on FIs and DNFBPs, (including notaries and company registrars, which are obliged entities under the AML/CFT law), and the measures taken by the courts to dissolve legal entities involved in ML schemes, and or seize their assets should, over time, act as strong deterrents to the misuse of Spanish legal persons.

Section VI – Getting information on beneficial ownership of overseas entities

108. For entities registered abroad, the information sources on beneficial ownership mainly used by competent authorities are the public companies/business register available in the country and information collected by FIs/DNFBPs of the country in question, information disclosed following requests made to foreign authorities, and information from foreign tax authorities. The exchange of information with a foreign counterpart is a critical component of measures pursuant to an international ML/TF investigation.

109. According to the 2018 FATF-Egmont report, increased sharing of relevant information and transaction records would benefit global efforts to improve the transparency of beneficial ownership. Further consideration of possible ways to enhance this information sharing is merited.

110. There is a good practice that basic information relating to legal persons is available online and in several languages, which can enable foreign authorities to continue their investigations without necessarily having to wait for a reply from the authorities. Nevertheless, it is also understood that countries have encountered difficulties in getting information on beneficial ownership that is not publicly available.

111. The effectiveness of getting beneficial ownership information of foreign legal persons is generally more reliant on foreign countries' active co-operation, with varying degrees of timeliness and success. Despite FATF general requirement on international co-operation and the specific requirements to provide co-operation on identifying the beneficial ownership of corporate vehicles under R.24, some countries do not effectively facilitate requests from their foreign counterparts by providing information held by domestic authorities and companies.

112. Imposing restriction on activities of foreign legal persons may affect a country's direct foreign investment. Balancing the need of obtaining information on beneficial ownership of foreign legal persons and ensuring legitimate business operation of foreign legal persons, countries can consider adopting the following approaches with an aim to achieving the objectives of R.24 and IO.5 based on the risk level of legal persons registered aboard identified from the risk assessment.

a) No specific prior requirements - Not applying specific ex-ante requirements on legal persons registered abroad, but only seeking mutual legal assistance when there is a problem.

b) Rating jurisdictions' level of co-operation - Rating jurisdictions based on the availability and extent of their co-operation. Impose defensive measures such as restriction of certain business activities accordingly.

c) Requiring re-registration with a local beneficial ownership.

d) Requiring re-approval by domestic national authorities based on detailed investigation of the relevant legal entities.

Information on beneficial ownership of overseas entities

No specific prior requirements

Not applying specific *ex-ante* requirements on legal persons registered abroad, but only seeking mutual legal assistance when there is a problem.

Re-registration

Requiring re-registration with a local beneficial ownership.

Re-approval

Requiring re-approval by domestic national authorities based on detailed investigation of the relevant legal entities

Rating jurisdictions' level of co-operation

Rating jurisdictions based on the availability and extent of their co-operation. Impose defensive measures, such as restriction of certain business activities, accordingly.

Section VII - Conclusion

113. Many countries have made progressive efforts in putting in place a more robust legal framework in preventing legal persons from being misused since 2012. With the flexibility provided by the FATF in implementing R.24 and achieving IO.5, it is also seen that countries are exploring different measures to ensure the transparency of beneficial ownership. With the sharing of best practices among countries, it is expected that countries will continue to improve their system particularly in relation to the requirements to ensure that adequate, accurate and up-to-date basic and beneficial ownership information is available to the authorities in a timely manner.

114. Under a multi-pronged approach, it is vital that there is effective monitoring of key gatekeepers (including company formation agents, lawyers, and trust-and-company-service providers) for compliance with their CDD obligations, and enforcing those requirements – including identifying and shutting down those who facilitate misuse of corporate structures.

115. More importantly, it is also expected that countries will take action to facilitate the timely sharing of basic and beneficial ownership information at the domestic and international level to address barriers to information-sharing (e.g. reviewing data protection and privacy laws). The FATF will continue to intensively monitor the steps taken by countries to meet the FATF Standards on legal and beneficial ownership and ensuring they are properly enforced.

ANNEX 1: Detailed Arrangement of Mechanisms under R.24

1. Under R.24, countries should use one or more of mechanisms (the Registry Approach, the Company Approach and the Existing Information Approach) to ensure that information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or can be otherwise determined in a timely manner by a competent authority[25].

2. Countries' experience shown in the FATF mutual evaluations points out that more than one approach may be needed in order to ensure a complete and effective system. Based on countries' experience and good practices, this Annex aims to set out the arrangements of the mechanisms (Registry Approach, Company Approach and Existing Information Approach) which vary in different aspects, including collection and verification of information on beneficial ownership, modalities of storage and access to information on beneficial ownership, and supervision and enforcement of the relevant obligations.

Registry Approach

Collection and verification of information on beneficial ownership

3. All companies created in a country are registered in the company registry. The registry records and maintains basic information of a company, including company name, proof of incorporation, legal form and status, address of the registered office, basic regulating powers and list of directors. Registries are also required to hold information on beneficial ownership or a separate register of beneficial owners might be set up. This register may include beneficial owner data as well as company information. Excerpts from the register may be used for CDD considering the risk-based approach.

4. The basic information held by registries are made publicly available and the availability of information on beneficial ownership varies with the practice of each countries. Information in the company register is generally recorded digitally and is preferably searchable. The search function supports searches by multiple fields.

5. In some countries, the registry is entrusted with oversight function, including verification of completeness or accuracy of filings, conducting CDD in certain cases, or cross-checking their information with data held by other authorities (e.g. with tax authorities). Some registries conduct sample testing or targeted audits to verify or/and monitor the accuracy of information on selected legal persons. Some countries rely on notarial systems or other gatekeepers to verify or/and monitor the information for company registration. Registry in some countries do not verify or/and monitor the information by itself, but rely on surveillance by civil society on reporting.

Modalities of storage and access to that information

6. Company registries generally keep the information on beneficial ownership in public domain and impose annual updating requirement for registered companies. When the company initiates a change, it should notify and submit supplementary

[25] Interpretative Note to R.24, para. 7 and 8, FATF (2013a).

information and relevant proof to the company registry, via obliged party if required, within a specified period.

7. Some company registries will verify or/and monitor information changes. In some countries, the company registry only accepts notary-certified information/ updates. Some registries accept self-declared information. Nevertheless, the reliability of self-declared information is in doubt.

8. Competent authorities generally have access to the company registry online, including full search capability on both basic information and information on beneficial ownership. Basic information of the company is publicly available. The trend of openly accessible information on beneficial ownership is on the rise among countries.

Supervision and enforcement of the relevant obligations

9. If a company fails to provide information or has provided false information on beneficial ownership, it is subject to proportionate and dissuasive administrative sanctions e.g. rejection of registration, de-registration. Owners and senior management that effectively control the company are also held personally liable and are subject to administrative and criminal sanctions.

10. The company registry authority regularly applies such sanctions by reviewing annual return, conducting sample testing, conducting investigations arising from report of suspicious activities, validating the information by cross-checking information by other authorities. Company registry may de-register/struck-off the company if the information is not accurate and up to date. It may also apply fines when the company fails to provide the requested information. In some cases, the company registry can refuse registration application from the same person/legal entity which breached the obligations before.

Company Approach

Collection and verification of information on beneficial ownership

11. Companies are required to maintain basic information, including company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (for example, memorandum and articles of association), and a register of their shareholders or members, containing the number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights).

12. Companies also hold information on beneficial ownership, and to achieve this they are generally provided with the authority to request information from shareholders on the beneficial ownership of shares.

13. In general, the company needs to rely on shareholders to provide them with information. It is rare for company to involve an independent third party to verify or/and monitor the information. Some companies may not have the legal knowledge and experience to identify and verify their beneficial owners. This could be in particular true, when knowledge of foreign jurisdictions and legal persons is necessary to determine their beneficial owners. Even if it is rare for company to involve an independent third party to verify or/and monitor the information, an

effective company approach could therefore allow the involvement of independent third parties (e.g. tax advisors, lawyers).

Modalities of storage and access to that information

14. Companies, or a third person under the company's responsibility, are required to keep shareholder registers, such as shareholder lists which are made available to competent authorities.

15. Under this approach, companies are generally provided powers to require updated information from their shareholders (including the power to request information on beneficial ownership at any time). Shareholders are required to disclose the names of person(s) on whose behalf shares are held. When there are any changes in ownership or control, shareholders are required to notify the company within a specified time period.

16. The information on beneficial ownership is maintained within the country at a location notified to the company registry. Lists of shareholders and beneficial owners may be held, and provided, in electronic form.

17. Companies are required to provide lists of shareholders and beneficial owners to competent authorities upon request in a timely manner. Companies are generally not required to disclose its information on beneficial ownership to public. Where information on beneficial ownership cannot be identified, companies may be required to publish this fact on their website.

Supervision and enforcement of the relevant obligations

18. Companies can seek to apply restrictions against shareholders for failure to provide information on beneficial ownership through appropriate courts or authorities, such as in relation to shareholder voting rights, or the sale of shares.

19. Failure by a company to provide the information to authorities is subject to sanctions, which may include administrative penalties or restrictions on incorporation. Where lists of shareholders and beneficial owners are held with a third party provider on the company's behalf, the company remains liable for the obligations.

Existing Information Approach – FIs/TCSPs and other DNFBPs

Collection and verification of information on beneficial ownership

20. Under R.10 and 22, FIs and DNFBPs are required to identify and take reasonable measures to verify the identity of the beneficial owner such that the FI/DNFBP is satisfied that it knows who the beneficial owner is. FIs and/or DNFBPs should obtain sufficient information from their clients so that they can identify and verify the identity of clients, and understand the nature of its business, and its ownership and control structure, including name, legal form, proof of existence, company arrangement and persons exercising control from the company. If there is a discrepancy between the records of FIs and DNFBPs with those on the central registry, the FIs and DNFBPs have an obligation to report such discrepancy to a responsible entity to carry out further investigation and make clarifications.

21. FIs and DNFBPs also collect information on beneficial ownership when they carry out CDD and ongoing monitoring, maintenance of records, training and reporting.

22. FIs and DNFBPs generally need to rely on information provided by the client (for example, certificate of incorporation, certificate of good standing, partnership agreement, deed of trust, memorandum and articles of association of a company, proof on address of the registered office) and existing information available in the public domain to verify the information. In some case, FIs and DNFBPs may hire risk management service providers that collect data on corporate entities when carrying out CDD.

23. The effectiveness of verification also hinges on the availability of a reliable independent source and whether they are authorised to authenticate the identity of the natural persons directly.

Modalities of storage and access to that information

24. FIs and DNFBPs generally store information on beneficial ownership, e.g. clients' files, in their private domains. In some countries, TCSPs (e.g. notary) maintain a central computerised platform that is accessible on public domain. How the information on beneficial ownership is stored and updated are subject to the requirement of financial supervisors and SRBs. FIs and DNFBPs are required to conduct ongoing CDD on the business relationship, and scrutinise transactions throughout the course of that relationship to ensure that the information on beneficial ownership is kept up-to-date.

25. Actions may include undertaking reviews of existing records, request information from their clients, cross-check information from reliable sources or hire services from a commercial database, particularly for higher-risk categories of customers.

26. FI and DNFBPs are required to provide information on BO to competent authorities upon request in a timely manner. In some countries, notary profession who is the obliged party has maintained and made publicly available a register on beneficial ownership of legal persons. In some countries, professional organisations maintain an internal register which is accessible by the profession themselves. In general, the public is not granted access to information held by FIs, TCSPs and other DNFBPs.

Supervision and enforcement of the relevant obligations

27. FIs and DNFBPs should adequately implement CDD obligations, including measures to identify and verify the identity of the beneficial owner, as is required by R.10 and 22. FIs and DNFBPs should be adequately supervised by supervisors, competent authorities or SRB in accordance with R. 26 and 28.

28. FIs and DNFBPs are provided with sufficient guidance on how to properly conduct CDD in accordance with R.34. Such guidance will facilitate implementation of the CDD requirements, thereby improving the quality and sufficiency of information on beneficial ownership being collected by these entities.

29. To ensure compliance, supervisors, competent authorities and SRBs will perform monitoring (e.g. inspections) and impose a range of disciplinary and financial sanctions e.g. penalties, disciplinary proceedings, suspension or ban of professional practice on FIs and DNFBPs.

Existing Information Approach – Competent authorities

Collection and verification of information on beneficial ownership

30. Competent authorities (particularly LEA) generally rely on information held by registries, companies, FIs and DNFBPs, and other asset registries such as for land, property, vehicles, shares or other assets. Therefore, the collection of information on beneficial ownership hinges on whether the concerned entities (registries, companies, FIs and DNFBPs, and other asset registries) hold accurate and up-to-date information and whether competent authority can have timely access to the basic and information on beneficial ownership of legal persons.

31. Competent authorities should be aware of the availability of information, and are able to identify the FIs, DNFBPs or entities concerned for access to information, for example, through a national register of bank accounts or a central register of transactions of shares, or a register of TCSPs.

32. The effectiveness of obtaining information on beneficial ownership hinges on whether competent authorities have adequate powers, mechanisms and expertise to access to information on beneficial ownership in a timely manner.

33. Competent authorities generally verify the information by conducting further desk-based reviews and on-site inspections. An authority responsible for the Beneficial Owner Register or the beneficial owner data held in the business register might also contribute to an effective system. Competent authorities should generally verify the information i.e. by conducting risk based reviews and having the power to request information on beneficial ownership from companies, legal and beneficial owners.

34. Desk-based reviews involve analysis of existing information available on different domains, e.g. annual independent audit reports and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identify the gatekeeper responsible for the filing.

35. On-site inspections involve reviewing internal policies, controls and procedures, gatekeeper's own risk assessments, spot-checking CDD documents and supporting evidence, sample testing of reporting obligations.

36. Taxation database is also a useful means of identifying indicators of criminality and schemes designed to obscure beneficial ownership and verifying information on beneficial ownership. Further investigation often uncovers dubious control structures or corporate dealings designed to conceal beneficial ownership.

Modalities of storage and access to that information

37. Competent authorities, including regulators, tax authorities, intelligence authorities store and update information in accordance with their functions and obligations – e.g. some tax authorities will keep an account of names of company owners and directors, some stock registries will hold information on meaningful shareholders or persons directly or indirectly controlling meaningful voting rights in public companies.

38. Competent authorities (such as supervisory authorities, tax authorities, or land titles offices) generally share information on beneficial ownership upon requests by other competent authorities. In some countries, certain electronic databases are made readily accessible among competent authorities. There should be sufficient mechanisms in place for information sharing between competent authorities so that competent authorities can gain access to information held by other authorities for verification and investigation in a timely manner.

Supervision and enforcement of the relevant obligations

39. Competent authorities are subject to national governance, for example, audit checking, monitoring and surveillance on their compliance.

Existing Information Approach – Companies listed on a stock exchange

Collection and verification of information on beneficial ownership

40. The information on beneficial ownership is usually collected when the company goes on initial public offering. The availability of information on beneficial ownership hinges on the disclosure requirement (either by stock exchange rules or through law or enforceable means).

41. The information of stock exchange is generally verified by the responsible FIs and/or DNFBPs that provided services to the company. The FI and/or DNFBP is held accountable for the verification of accuracy in performing their functions.

Modalities of storage and access to that information

42. The information on beneficial ownership may be stored at the stock exchange at the time of initial public offering. The information is generally accessible on the website of the stock exchange. Whether and how frequent it will be updated depends on the policy and rules of the stock exchange.

43. Public, FIs, DNFBPs, competent authorities can gain access to the information as long as the website of the stock exchange is public and contain information on beneficial ownership.

Supervision and enforcement of the relevant obligations

44. In general, there is no particular obligation for stock exchange to collect, verify and keep the information up-to-date for the purpose of AML/CFT.

BEST PRACTICES ON BENEFICIAL OWNERSHIP FOR LEGAL PERSONS

Transparency of beneficial ownership is essential to prevent the misuse of companies, associations or other entities for money laundering or terrorist financing. The Financial Action Task Force (FATF) is the global standard-setter for measures to fight money laundering and terrorist financing. Since 2003, the FATF Recommendations require countries to ensure that authorities can obtain up-to-date and accurate information about the person(s) behind companies, foundations and other legal persons.

This best practices paper, with examples from across the global network of FATF and FATF-Style Regional Bodies' members, will help countries effectively implement the FATF's requirements. The report highlights that jurisdictions using a multi-pronged approach with several sources of information are often more effective in preventing the misuse of legal persons for criminal purposes. The report identifies the most common challenges that countries face in ensuring that the beneficial owner(s) of legal persons is identified, and suggests key features of an effective system.

www.fatf-gafi.org / October 2019

Appendix Y:

FATF, *Guidance for a Risk-Based Approach: Securities Sector*
(Paris: FATF, 2018)

FATF

GUIDANCE FOR A RISK-BASED APPROACH

SECURITIES SECTOR

OCTOBER 2018

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2018), *Guidance for a Risk-Based Approach for the Securities Sector,* FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-securities-sector.html

Table of contents

ACRONYMS

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Customer[1] due diligence
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
IOSCO	International Organisation of Securities Commissions
ML	Money laundering
PEP	Politically- exposed person
R.	Recommendation
RBA	Risk-based approach
STR	Suspicious transaction report
TF	Terrorist financing
UN	United Nations

[1] The industry often uses the term "client" which has the same meaning as "customer" for the purposes of this document.

RISK-BASED APPROACH GUIDANCE FOR THE SECURITIES SECTOR

Executive summary

1. The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. It means that supervisors, financial institutions, and intermediaries identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed, and implement the most appropriate mitigation measures. This approach enables them to focus their resources where the risks are higher.

2. The FATF RBA Guidance aims to support the implementation of the RBA, taking into account national ML/TF risk assessments and AML/CFT legal and regulatory frameworks. It includes a general presentation of the RBA and provides specific guidance for securities providers and for their supervisors. The Guidance was developed in partnership with the private sector, to make sure it reflects expertise and good practices from within the industry.

3. The Guidance describes various types of securities providers that may be involved in a securities transaction and their business models. It also sets out key characteristics of securities transactions that can create opportunities for criminals, and measures that can be put in place to address such vulnerabilities.

4. The development of the ML/TF risk assessment is a key starting point for the application of the RBA by securities service providers. It should be commensurate with the nature, size and complexity of the business. The most commonly used risk criteria are country or geographic risk, customer risk, product or service risk and intermediary risk. The Guidance provides examples of risk factors under these risk categories.

5. The Guidance highlights that it is the responsibility of the senior management of securities providers to foster and promote a culture of compliance as a core business value. They should ensure that securities providers are committed to manage ML/TF risks before establishing or maintaining business relationships.

6. The Guidance clarifies the role and responsibilities of intermediaries that may provide services on behalf of securities providers to customers of securities providers, customers of intermediaries or both. It highlights that the nature of the business relationship between the securities provider, the intermediary and any underlying customers will affect how ML/TF risks should be managed. This includes clarifying when the FATF's Recommendations on reliance apply.

7. The Guidance clarifies that when determining the type and extent of CDD to apply, securities providers should understand whether its customer is acting on its own behalf or as an intermediary on behalf of its underlying customers. Even when CDD is the responsibility of the intermediary, an understanding of the intermediary's customer base can often be a useful element in determining the risk associated with the intermediary itself. The level of understanding should be tailored to the perceived risk level of the intermediary.

8. Some business relationships in the securities sector might have characteristics similar to cross-border correspondent banking relationships; the Guidance also contains a description of how AML/CFT requirements apply to such relationships.

9. The Guidance highlights the importance of ongoing transaction monitoring to determine whether transactions are consistent with the securities provider's information about the customer and the nature and purpose of the business relationship. In case of any suspicions, security providers are required to report promptly their suspicions to the Financial Intelligence Unit. It provides up-to-date examples of indicators of suspicious activity in relation to securities sectors, which may trigger filing of STRs or additional CDD measures by securities providers, or further investigation or ongoing monitoring.

10. The Guidance stresses the importance of the group level approach to mitigate ML/TF risks, including the development of group-wide assessment of ML/TF risks and the sharing of relevant information between supervisors involved. It also highlights the importance of guidance and feedback from supervisors to securities providers on regulatory expectations and quality of reporting by securities providers. This will develop a shared understanding between the public and private sector. In this regard, the Guidance provides examples of supervisory practices of certain countries in the implementation of RBA in the securities sector.

This Guidance should be read in conjunction with:

- the FATF Recommendations, especially Recommendations 1, 10, 13, 17, 19, 20 and 26 and their Interpretive Notes (INR), and the Glossary

other relevant FATF Guidance documents, such as:

- the FATF Guidance for a Risk-Based Approach: The Banking Sector
- the FATF Guidance on Correspondent Banking Services
- the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment
- the FATF Guidance on Politically Exposed Persons
- the FATF Guidance on Private Sector Information Sharing
- the FATF Guidance for a Risk-Based Approach: Effective Supervision and Enforcement

relevant FATF typology reports, such as:

- the FATF Report: Money Laundering and Terrorist Financing in the Securities Sector (October 2009)

INTRODUCTION AND KEY CONCEPTS

Background and context

11. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which were adopted in 2012[2]. This Guidance focuses on RBA for the securities sector[3], and includes an annex on suspicious activity indicators in relation to the securities sector. It takes into account the experience gained by public authorities and the private sector over the years in applying a RBA. This Guidance should be read in conjunction with the *FATF Report: Money Laundering and Terrorist Financing in the Securities Sector* (October 2009), which outlines vulnerabilities in the sector.

12. The RBA Guidance for the securities sector was drafted by a project group of FATF members and representatives of the private sector, co-led by representatives of the Royal Bank of Canada and the United States[4].

[2] www.fatgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[3] Securities activities are activities or operations described in the FATF Glossary under "Financial institutions", in particular points 7, 8, 9, 10 and 11.

[4] The FATF project group was composed of representatives from FATF members [International Organisation of Securities Commissions (IOSCO), Ireland, Luxembourg, Singapore and the USA] and from the private sector [Association for Financial Markets in Europe (AFME), Pershing, Philip Capital, Royal Bank of Canada, and the Securities Industry and Financial Markets Association (SIFMA)].

13. The FATF adopted this updated RBA Guidance for the securities sector at its October 2018 Plenary.

Purpose of this Guidance

14. The purpose of this Guidance is to:

a) Outline the key principles involved in applying a risk-based approach to Anti-Money Laundering /Countering the Financing of Terrorism ("AML/CFT") in the securities sector;

b) Assist countries, competent authorities, providers of securities products and services ("securities providers") and intermediaries in the risk-based design and implementation of applicable AML/CFT measures by providing general guidelines and examples of current practice;

c) Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on mitigation measures; and

d) Support the development of a common understanding of what the risk-based approach to AML/CFT entails in the context of the securities sector.

Target audience, status and content of the Guidance

15. This Guidance is aimed at the following audience:

a) Countries and their competent authorities, including AML/CFT supervisors of the securities sector, and Financial Intelligence Units ("FIUs"); and

b) Practitioners in the securities sector (including securities providers and intermediaries, and external examiners for AML/CFT purposes).

16. The Guidance consists of three sections. Section I sets out the key elements of the risk-based approach and needs to be read in conjunction with Sections II and III, which provide specific guidance to securities providers and intermediaries (Section II), and on the effective implementation of a RBA to supervisors of the securities sector (Section III). The annexes provide examples of countries' supervisory practices and suspicious activity indicators in the securities sector.

17. This Guidance recognises that an effective RBA will build on, and reflect, a country's legal and regulatory approach, the nature, diversity and maturity of its securities sector and its risk profile. It sets out what countries should consider when designing and implementing a RBA; but it does not override the purview of national competent authorities. When considering the general principles outlined in the Guidance, national authorities should take into consideration their national context, including the supervisory approach and legal framework. Similarly, as with any application of the risk-based approach, securities providers should tailor their own policies and procedures to the risks they face and the jurisdictional requirements in which they conduct their business. In light of the complexity and scope of the sector, this Guidance may address issues not relevant to all securities providers, as it will by necessity, not address in detail, the entire spectrum of activities or entities operating in the sector.

18. This Guidance is non-binding. It draws on the experiences of competent authorities as well as AML/CFT professionals in the private sector and may assist both competent authorities and the private sector to effectively implement some of the Recommendations.

Scope of the Guidance: terminology, key characteristics and business models

Terminology

19. This Guidance applies to the provision of securities products and services. However, given the commonality of issues between the securities and banking sectors, such as issues raised by pooled account structures, banks offering securities products and services should consider this Guidance in conjunction with the *FATF Guidance for a Risk-Based Approach: The Banking Sector*.

20. The term "securities" is broadly defined for the purpose of this guidance as including, for instance:

a) Transferable securities, including equities and bonds or similar debt instruments;

b) Money-market instruments;

c) Investment funds, including units in collective investment undertakings;

d) Options, futures, swaps, forward rate agreements and any other derivative contracts relating to securities, currencies, interest rates or yields or other derivatives instruments, financial indices or financial measures, which may be settled physically or in cash;

e) Options, futures, swaps, forwards and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash;

f) Derivative instruments for the transfer of credit risk;

g) Financial contracts for differences; and

h) Options, futures, swaps, forward rate agreements and any other derivative contracts relating to climatic variables, freight rates, emission allowances or inflation rates or other official economic statistics that are settled in cash, as well as any other derivative contracts relating to assets, rights, obligations, indices and measures not otherwise mentioned in this section, which have the characteristics of other derivative financial instruments.

21. The above definition is neither rigid nor exhaustive. Differences exist in legal and regulatory definitions across different jurisdictions and the securities sector continues to evolve constantly with the introduction of new securities products and services. Further, national authorities should have the flexibility to identify providers of securities products and services, which should be subject to AML/CFT obligations, taking into account risk and context and their role in the securities sector.

22. In some countries virtual assets and the associated Initial Coin Offerings ("ICOs") are recognised as securities (and subject to AML/CFT regimes), whereas other countries have banned them. Some countries are also evaluating the appropriate regulatory framework for these products and services.

Key characteristics of the securities sector

23. Securities markets are often characterised by complexity, internationality, a high level of interaction, high volumes, speed and anonymity. Many of the core economic functions of securities markets are critical to efficient price-formation and capital allocation, which contribute to economic growth, job creation and overall prosperity. However, some of the same characteristics associated with the sector can create opportunities for criminals. *The FATF Report: Money Laundering and Terrorist Financing in the Securities Sector* (October 2009) outlines the main ML/TF vulnerabilities in the securities sector. Some of the key characteristics of the securities sector for the purpose of this Guidance for a RBA are as follows:

a) The varying roles that securities providers and other intermediaries play in transactions; for example, a securities provider may be both an investment fund manager and a depository bank (see paragraphs 27-42 below);

b) Differences among jurisdictions in defining securities, securities products and services and their providers and the AML/CFT regulated status of these providers;

c) ML/TF risks stem mainly from the types of securities products and services, customers, investors and payment methods used in the securities sector; noting that cash is generally not accepted by securities providers in many jurisdictions;

d) Global reach of the securities sector and speed of transactions across a multitude of onshore/offshore jurisdictions and financial markets;

e) Ability to transact in securities products via an intermediary which may provide a relative degree of anonymity;

f) High liquidity of some securities products, which often enables their easy conversion to cash;

g) Complex products that may be offered before they are regulated (or not regulated at all) or rated for ML/TF risks (e.g. the crypto-assets mentioned above);

h) Common involvement of a multitude of securities providers and intermediaries on behalf of both buying and selling principals or agents, potentially limiting the ability of any one participant to have complete oversight of the transaction;

i) An often highly competitive and incentive-driven environment, which may lead to a higher appetite for risk, or failure to adhere to internal controls;

j) Pricing volatility of some products, particularly low-priced securities;

k) Transactions executed both on registered securities exchanges and elsewhere, such as over-the-counter (where parties trade bilaterally), and reliance on alternative trading platforms, electronic communication networks and internet-based trading;

l) Opportunity to use transactions in securities for generating illicit income within the sector, for example, market abuse or fraud; and

m) Challenges in pricing some securities products due to their bespoke nature or complexity.

24. Market abuse is a general term used to describe a wide range of types of unlawful behaviour in the financial markets including market manipulation, wash trading, insider trading, misappropriation, layering, unauthorized pooling, spoofing, front running and the like. Chapter 4 of the *FATF Report: Money Laundering and Terrorist Financing in the Securities Sector* (October 2009) provides additional information in relation to predicate offences for money laundering linked to securities.

25. Market abuse risk is relevant in the AML/CFT context for two principal reasons. Firstly, some forms of market abuse may constitute predicate offences for money laundering under applicable national laws. Secondly, certain controls which financial institutions may be required to implement to comply with market abuse laws, in particular, the surveillance of trading activity, may also be of use in monitoring for suspicious activity for AML/CFT purposes. Such commonalities and efficiencies are to be encouraged so long as both market abuse and AML/CFT obligations are each fully met.

26. This Guidance does not, however, purport to describe controls that financial institutions may be required to implement to prevent or detect market abuse. While applicable laws may require financial institutions to report suspicions of market abuse to certain authorities, references in this Guidance to reporting suspicious transactions relate to reporting suspicions of ML/TF (including market abuse, where appropriate) pursuant to R.20.

Securities providers (services and activities)

27. For the purpose of this Guidance, **securities provider** means any natural or legal person who is, or is required to be licensed or registered by a competent authority, to provide securities products and services as a business. Securities providers range from those that largely interact with retail investors, such as retail stockbrokers, wealth managers and financial advisors, to those serving a largely institutional market like clearing members, prime brokers, global custodians, sub-custodians and depository banks including securities depository participants. This is not an exhaustive list of all securities providers, and in some instances a securities provider may assume more than one of the above roles. One characteristic, particularly of larger securities providers, is that they may perform a diverse set of activities through different legal divisions or entities within the same group. These

different group entities may be subject to different regulatory and statutory requirements and the group's risk-based approach will need to consider this carefully.

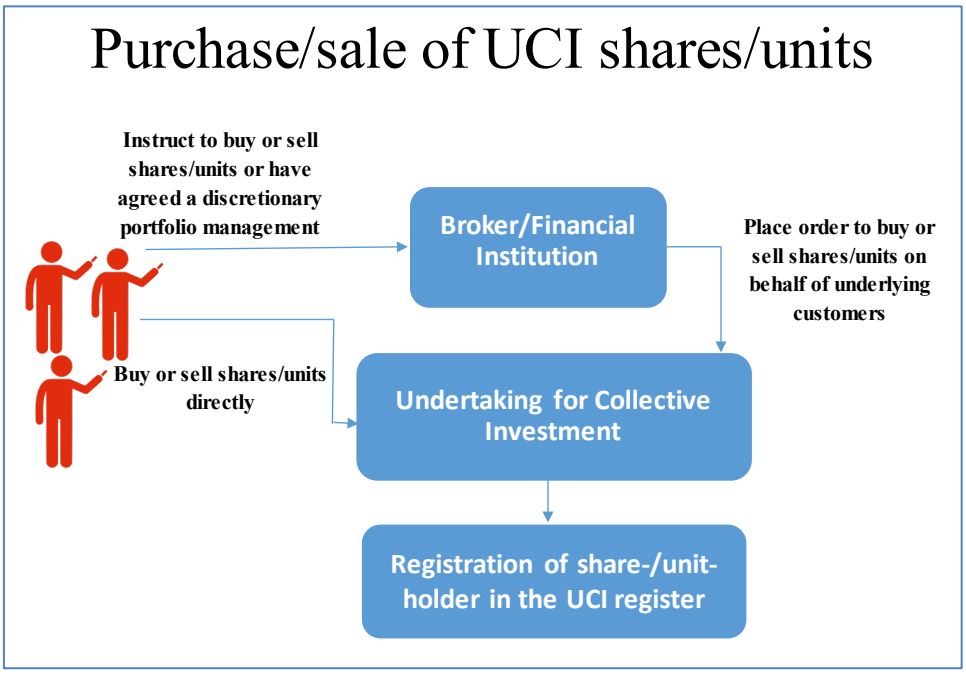
28. Securities providers offer various types of services, including capital market research and advisory, individual and collective portfolio management, investment funds distribution, order execution (trading in transferable securities), underwriting for issuers, private placements and other prospectus-exempt products, custody of client assets, lending money (providing margin) to clients and transfers of client cash (e.g. wire transfers). Mergers and acquisitions services and syndicate and secondary market financing are other types of securities services. Each of these activities and services may present different ML/TF risks depending on factors like the customer type, source and use of funds, customer business sector and geography. Securities providers typically specialise along retail, institutional and wholesale lines. Different risks may arise when a securities provider offers customers, securities accounts with a wide range of transactional and cash-management services associated with securities. Regardless of the role, the securities provider must continually tailor its own RBA to assessing and managing ML/TF risk.

29. The RBA to due diligence by securities providers can vary depending on a number of factors, such as the securities product involved in a transaction, custodial relationships, contractual obligations, the customer, and applicable AML/CFT regulatory requirements, including customer identification requirements.

30. **Investment funds**, including undertakings for collective investment ("UCIs") and pooled investment vehicles, are undertakings established as limited companies, limited partnerships or by contract that generally pool money from a number of third party investors and invest it in assets such as securities (e.g. stocks, bonds, and other mutual funds) or other assets (e.g. real estate, private equity and commodities). The combined investment holdings of the investment fund are known as its investment portfolio. Investors may buy and sell shares or units in the investment fund. Each share/unit represents an investor's part ownership in the fund and the income it generates. Investors may buy and sell investment fund units directly from the fund itself or indirectly through an intermediary, such as a broker or another financial institution. When an intermediary's name is recorded in the investment fund's share/unit register but it is holding units for its underlying customers, the arrangement is often referred to as an "omnibus account".

31. See illustration below, which demonstrates in simple terms one of the many distribution arrangements for investment funds (also refer to section 7.1.3 of this Guidance).

Diagram 1.Illustration of ways which UCI shares/units are distributed



32. Another type of securities provider is an **investment advisor**, which can be either an individual or a firm that gives advice about securities and financial planning to its customers, which may include individuals, institutions, trusts, or pooled investment vehicles.

33. A **broker** is a person or an entity that is in the business of buying and selling securities - stocks, bonds, mutual funds, and other investment products either on behalf of its customers or for its own account. A broker may have customers that are individuals or other legal entities (including financial institutions, corporate entities, partnerships and trusts).

34. Brokers serve retail customers and other institutions, such as pension plans, hedge funds, banks and other brokers. It is not uncommon that a number of different brokers are involved in a particular transaction, for example, an "**introducing broker**" may pass orders on to an "executing broker", who may execute the trade and give it up for clearing to a "clearing broker".

35. Securities providers known as **clearing members** or clearing brokers may provide record-keeping, confirmation, settlement, delivery of transactions and related functions associated with securities transactions, usually on behalf of other brokers, such as introducing or executing brokers.

36. **Institutional brokers** interact largely with large institutional clients and are often used to provide execution and custody services unaccompanied by investment advice. Customers of institutional brokers may and do use multiple institutional brokers to execute transactions.

37. **Prime brokers** provide execution, custody and other services to other financial institutions, such as hedge funds. This can include providing centralised clearing facilities for investment funds and allowing customers to borrow shares or money. Prime brokers may also act as record-keepers for other securities providers (e.g. investment advisors or investment managers) that may in turn be acting on behalf of customers' transactions.

38. Another type of securities provider, a **custodial broker-dealer**, can maintain custody of assets for its own customers (e.g. other broker-dealers, investment advisers, banks or other types of institutional clients) or their underlying customers. The underlying customers may be fully or partially disclosed to the custodial broker-dealer, while others may be non-transparent ("omnibus").

39. The **global custodian** provides safekeeping and settlement "custody services" for fund-managers, their underlying funds, asset managers and other institutional clients across multiple markets globally through a network of relationships with sub-custodians, banks, national and international central securities depositories (CSDs).

40. A **sub-custodian** provides safekeeping, clearing and settlement custody services in a domestic or international market on behalf of its customers. Although often employed by a global custodian, the sub-custodian, also referred to as an agent bank, might also service brokers and banks.

41. A **central securities depository** (CSD) provides securities accounts and, in many countries, operates a Securities Settlement System. A CSD also provides central safekeeping and asset servicing and plays an important role in helping to ensure the integrity of securities issues. The CSD will service many customers including sub-custodians, banks, brokers, global custodians, prime brokers, and issuers.

42. The size and complexity of securities providers vary significantly and as discussed above, they use various business models and may play different roles in different transactions. The complexity of the securities sector and the variety of securities provider roles highlight that where multiple securities providers are involved in a transaction, some securities providers may be in a better position than others, to have more complete transparency relating to a transaction. Thus, a securities provider should appreciate that it may not have a full picture of the entirety of business occurring through it and should therefore conduct an initial and ongoing risk assessment of its customers and activities to best understand and then mitigate any ML/TF risks identified.

Intermediaries

43. In the provision of their products and services, securities providers often interact with intermediaries, which may provide services on behalf of the securities provider to a person or entity who is the customer of the securities provider, a customer of the intermediary, or a customer of both.

44. Services provided by these intermediaries could include performing certain aspects of CDD, which are relied upon by a securities provider (reliance model - see paragraphs 114-116 for further description). Services may also include distribution services for selling securities products on behalf of a securities provider.

45. The distribution of securities products and services can also involve multiple parties, such as distributors appointed by a securities provider, transfer agents, registrars and administrators, tied agents or proprietary distributors, and platform service providers.

46. In other cases, securities providers may conduct transactions for certain other securities providers or intermediaries, which may be acting on behalf of their own customers. Indeed, an intermediary can be and very often is a securities provider itself, providing securities services within a chain of multi-step transaction.

47. All these different models and business practices may pose different ML/TF risks and require different approaches to risk mitigation.

48. The complexity of the securities sector and the variety of intermediary roles involved highlight that no one-size-fits-all AML/CFT approach should be applied. However, this variety and complexity highlights the importance of securities providers' understanding of how their business arrangements raise ML/TF risks both directly (e.g. through transactions executed by customers) and indirectly (e.g. risks associated with the underlying customers of the securities provider's customers, or risks associated with the possibility that an intermediary or other entity on which the securities provider relies to perform a task fails to do so). Securities providers should implement risk-sensitive measures to mitigate the ML/TF risk faced by them.

International provision of securities products and services

49. Some securities providers provide products and services across national borders through an intermediary or a network of intermediaries operating in another country. In instances where a securities provider operates in more than one country, the securities provider and competent authorities should verify that any ML/TF concerns are adequately addressed, in accordance with the FATF standards and regulations in the jurisdictions in which they operate. This is without prejudice to supranational rules that would enable securities providers to supply services throughout the supranational jurisdictions subject to the applicable legal framework.

50. Cross-border provision of products and services (including through intermediaries or over the internet or otherwise) highlights the importance of international cooperation among the competent authorities of the relevant jurisdictions. Such international cooperation can be spontaneous or upon request depending upon the nature of the specific situation.

51. This Guidance provides more detail on the recommended actions for securities providers and competent authorities in Sections II and III.

SECTION I – THE FATF'S RISK-BASED APPROACH TO AML/CFT (RBA)

WHAT IS THE RBA?

52. The RBA to AML/CFT means that countries, competent authorities and financial institutions[5] should identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

53. When assessing ML/TF risk, countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures[6]. For securities providers, this will require an understanding of the ML/TF risk faced by the sector as well as specific products and services, customer base, the capacity in which their customers are operating (e.g. on their own behalf or on behalf of underlying customers), jurisdictions in which they operate and the effectiveness of risk controls put in place. For supervisors, this will require maintaining an understanding of the ML/TF risks specific to the securities providers they supervise, and the degree to which AML/CFT measures can mitigate such risks. While institutions should strive to detect and prevent ML/TF, the RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate ML/TF risks, but it is still used for ML/TF in isolated instances.

54. A RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low[7].

THE RATIONALE FOR A NEW APPROACH

55. In 2012, the FATF updated its Recommendations to strengthen global safeguards and to further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime.

56. One of the most important changes was the increased emphasis on the RBA for AML/CFT for all relevant public and private sector entities, especially in relation to preventive measures and supervision. Whereas the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations consider the RBA to be an 'essential foundation' of a country's AML/CFT framework[8].

---

[5] Including both physical and natural persons, see definition of "Financial institutions" in the FATF Glossary.

[6] FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment, paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

[7] Where the ML/TF risks have been assessed as low, INR.1 allows countries not to apply some of the FATF Recommendations, while INR.10 allows the application of Simplified Due Diligence measures to take into account the nature of the lower risk – see INR.1 (paragraph 6, 11 and 12) and INR.10 paragraph 16 and 21.

[8] R.1.

The RBA is an over-arching requirement applicable to all relevant FATF Recommendations.

57. According to the introduction to the FATF 40 Recommendations, the RBA allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, so they can focus their efforts in the most effective way.

58. The application of a RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Standards[9].

APPLICATION OF THE RISK-BASED APPROACH

59. R.1 sets out the scope of the application of the RBA. It applies in relation to:

a) Who and what should be subject to a country's AML/CFT regime: in addition to the sectors and activities already included in the scope of the FATF Recommendations[10], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF.

b) How those subject to the AML/CFT regime should be supervised for compliance with this regime: AML/CFT supervisors should consider the securities provider's own risk assessment and mitigation, and acknowledge the degree of discretion allowed under the national RBA, while INR.26 further requires supervisors to themselves adopt a RBA to AML/CFT supervision; and

c) How those subject to the AML/CFT regime should comply: where the ML/TF risk associated with a situation is higher, competent authorities and securities providers have to take enhanced measures to mitigate the higher risk. This means that the controls implemented will be stronger, more numerous, wider in scope, more frequent, or a combination of these. Conversely, where the ML/TF risk is lower, standard AML/CFT measures may be reduced, which means that each of the required measures has to be applied, but they may be applied more narrowly, less frequently, or in a reduced way [11].

[9] The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take the risks, and the flexibility allowed by the RBA, into account when determining whether there are deficiencies in a country's AML/CFT measures, and their importance - *FATF Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems (2013).*

[10] See Glossary, definitions of "Financial institutions" and "Designated non-financial businesses and professions".

[11] R.10; INR.10, footnote 33.

CHALLENGES

60. Implementing a RBA can present a number of challenges:

Allocating responsibility under a RBA

61. An effective risk-based regime builds on, and reflects, a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector, and its risk profile. Securities providers' identification and assessment of their own ML/TF risk should consider all relevant national risk assessments in line with R.1 and take account of the national legal and regulatory framework, including any areas of prescribed significant risk and any mitigation measures defined at legal or regulatory level. Where ML/TF risks are higher, securities providers should consider applying enhanced due diligence and monitoring (e.g. varying the degree or frequency of ongoing monitoring), although national law or regulation might not prescribe exactly how these higher risks are to be mitigated[12].

62. Securities providers should have the flexibility in deciding the most effective way to address other risks, including those identified in the national risk assessment or by the securities providers. The securities providers' strategy to mitigate these risks must take into account the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which securities providers may be permitted to independently mitigate risk, countries should consider their securities sector's ability to effectively identify and manage ML/TF risks as well as their supervisors' expertise and resources, which should be sufficient to effectively supervise securities providers and take measures to address any failure by securities providers to do so.

63. Countries may also take into account evidence from competent authorities regarding the level of compliance in the securities sector, and the sector's approach to dealing with ML/TF risks. Countries whose financial services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that securities providers face challenges in effectively identifying and managing ML/TF risks and any flexibility allowed under the risk-based approach for simplified due diligence should therefore be limited[13].

64. Securities providers should not be exempted from AML/CFT supervision even where their capacity and compliance is good. However, the RBA should allow competent authorities to focus more supervisory resources on higher risk institutions and institutions providing higher risk products and services[14]. Nonetheless, countries and competent authorities should take steps to effectively supervise all entities covered by AML/CFT requirements.

[12] R.1.

[13] This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or FSAP (financial sector assessment program) reports.

[14] See FATF Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement.

Identifying ML/TF risk

65. Access to accurate, timely and objective information about ML/TF risks is a prerequisite for an effective RBA. INR.1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, financial institutions and other interested parties. Information sharing plays a vital role in allowing financial institutions and supervisory and law enforcement authorities to better deploy resources on a risk basis, and to develop innovative techniques to combat ML/TF[15]. Enabling greater information sharing is a key element of collaboration, whether it involves sharing across borders, between entities of the same financial group, between different financial groups or between private and public sector[16]. Jurisdictions should promote information sharing where possible, always seeking to ensure compatibility and coherence between local laws (including data protection laws) and AML/CFT laws. Where information is not readily available and adequate, it will be difficult for securities providers to correctly identify ML/TF risk and they may therefore fail to assess and mitigate it appropriately.

Assessing ML/TF risk

66. Assessing ML/TF risk means that countries, competent authorities and securities providers have to determine how the ML/TF threats identified will affect them. They should analyse the information obtained to understand the likelihood of these risks occurring, and the effect they could have on individual securities providers, the securities sector, large- scale financial institutions, and the national economy, if they did occur[17]. Risks identified through this process are often known as inherent risks, and risks, which remain after the risk mitigation process, are known as residual risks.

67. During the course of a risk assessment, ML/TF risks may be classified as low, medium and high, with possible combinations between the different categories (e.g. medium-high, low-medium). These classifications are meant to assist in communicating ML/TF risks and to help prioritise them. Assessing ML/TF risk, therefore, goes beyond the mere collection of quantitative and qualitative information: it forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.

68. Assessing and understanding risks means that competent authorities and securities providers should have skilled and trusted personnel, proportionate to the size and ML/TF risk and recruited through fit and proper tests, where appropriate. This also requires such personnel to be technically equipped to carry out their responsibilities.

[15] See R.18, R.20, R.21 and FATF Guidance on Private Sector Information Sharing.

[16] In the context of R.13, R.16, R.17, R.18 and R.26.

[17] Financial institutions are not necessarily required to perform probability calculations, which may not be meaningful given the unknown volumes of illicit transactions.

Mitigating ML/TF risk

69. The FATF Recommendations require securities providers, countries and competent authorities when applying the RBA, to decide on the most appropriate and effective way to mitigate the ML/TF risk they have identified. This implies that enhanced measures should be taken to manage and mitigate situations in which the ML/TF risk is higher; and that, correspondingly, in lower risk situations, less stringent measures may be applied[18]:

a) Countries looking to exempt certain institutions, sectors or activities from some of their AML/CFT obligations should assess the ML/TF risk associated with these financial institutions, sectors or activities and be able to demonstrate that the risk is low, and that the specific conditions required for one of the exemptions of INR.1.6 are met. The comprehensiveness of the risk assessment will depend on the type of institution; sector or activity; products or services offered; and the geographic scope of the activities that stand to benefit from the exemption. The nature and complexity of the securities sector mean that this exemption often will not apply

b) Securities providers looking to apply less stringent measures should conduct an assessment of the risks connected to the category of customers or products targeted, establish the lower level of the risks involved, and define the extent and intensity of the required AML/CFT measures. Specific Recommendations set out in more detail how this general principle applies to particular requirements[19].

Developing a common understanding of the RBA

70. The effectiveness of a RBA depends on a common understanding by competent authorities and securities providers of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. The legal and regulatory framework should spell out the degree of discretion appropriate for financial institutions in the sector to assume. Competent authorities and supervisors in particular should issue guidance to securities providers on how they expect them to meet their legal and regulatory AML/CFT obligations in a risk-sensitive way. Supporting ongoing and effective communication between competent authorities and securities providers is essential for the successful implementation of a RBA.

71. Competent authorities should acknowledge that in a risk-based regime, not all securities providers will adopt the same AML/CFT controls and that relatively isolated incidents of insignificant risk should not necessarily invalidate the integrity of a securities provider's AML/CFT controls. On the other hand, securities providers should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls. They should be able to explain to their supervisors the effectiveness of their AML/CFT controls and how those controls are commensurate with the risks identified.

---

18 Subject to the national legal framework providing for Simplified Due Diligence.

19 For example, R.10 on Customer Due Diligence and INR.10.

SECTION II – GUIDANCE FOR SECURITIES PROVIDERS AND INTERMEDIARIES

72. This section should be read in conjunction with the *FATF Report on Money Laundering and Terrorist Financing in the Securities Sector* (October 2009), especially the summary of Chapter 3 highlighting the main ML/TF vulnerabilities in the securities sector. The RBA consists of the identification of ML/TF risks and the definition and adoption of risk-sensitive measures that are commensurate with the ML/TF risks identified. In the case of securities providers, this applies to the types of products and services securities providers offer, the way they allocate their compliance resources, organise their internal controls and internal structures, and implement policies and procedures to manage and mitigate risk and detect and deter ML/TF. The RBA should also take into account intermediation networks.

RISK ASSESSMENT

73. Combating ML/TF is a global priority. The risk assessment should enable the securities provider to understand how, and to what extent, it is vulnerable to ML/TF. The risk assessment will also be developed because of regulatory requirements, guidance or expectations and will form the basis of a securities provider's RBA. It will often result in the categorisation of risks, including inherent and residual risks based on established controls and other mitigants, which will help securities providers determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk.

74. The risk assessment should be properly documented, regularly updated and communicated to the relevant securities provider's senior management. In conducting their risk assessments, securities providers should consider quantitative and qualitative information obtained from relevant internal and external sources to identify, manage and mitigate these risks[20]. This may include consideration of the risk and threat assessments, crime statistics, typologies, risk indicators, red flags, guidance and advisories issued by inter-governmental organisations, national competent authorities and the FATF, and AML/CFT mutual evaluation and follow-up reports by the FATF or associated assessment bodies. Many governments and authorities carry out ML/TF risk assessments for their jurisdictions, and securities providers should take these into account where relevant, when they are published or otherwise communicated. Furthermore, in identifying and assessing indicators of ML/TF risk to which it is exposed, a securities provider should consider a range of factors including:

a) The nature, diversity and complexity of its business, products and target markets;

b) The proportion of customers identified as high risk;

c) The jurisdictions in which the securities provider is operating or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other

[20] For example, in relation to terrorist financing, see the FATF Guidance on Emerging Terrorist Financing Risk (2015), and the countries that are in the FATF's International Cooperation Review Group (ICRG) process.

risk factors such as the prevalence of crime, corruption, or financing of terrorism, the general level and quality of the jurisdiction's prosecutorial and law enforcement efforts related to AML/CFT, the regulatory and supervisory regime and controls and transparency of beneficial ownership;

d) The distribution channels through which the securities provider distributes its products, including the extent to which the securities provider deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD or other AML/CFT obligations, the complexity of the transaction chain (e.g. layers of distribution and sub-distribution, type of distributors such as independent financial advisors, investment advisors) and the settlement systems used between operators in the payment chain, the use of technology and the extent to which intermediation networks are used;

e) The internal and external (such as audits carried out by independent third parties, where applicable) control functions and regulatory findings; and

f) The expected volume and size of its transactions, considering the usual activity of the securities provider and the profile of its customers[21].

75. Securities providers should review their assessments periodically and when their circumstances change or relevant new threats emerge. Securities providers should consider internal feedback within their organization, including from those who interact with customers, compliance risk management, and internal audit departments (where relevant), in performing their periodic risk assessments.

76. ML/TF risks may be measured using various methods. The use of risk categories enables securities providers to manage potential risks by subjecting customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer/investor risk; product/service risk and intermediary risk.

77. The extent to which these risk categories are applicable and the weight they should carry (individually or in combination) in assessing the overall risk of potential ML/TF risk may vary from one institution to another, depending on their respective circumstances and risk management framework. Securities providers must comprehensively review all risk factors relevant to their business, including how certain factors may interplay and have an amplifying effect. For example, the risks inherent in an under-developed securities sector could be amplified by regional risks (if it is located, e.g. in an area where there is high incidence of drug trafficking). Consequently, securities providers should determine the risk weights and at the same time, parameters set by law or regulation may limit a business's discretion.

78. As noted above, while there is no complete set of risk categories, the examples provided herein are the most commonly identified. There is no one single methodology to apply to these risk categories, and the following risk categories could be considered alone or in conjunction with other risk categories:

[21] See R.1 (c1.10 and c.1.11), INR.1 and R.10.

Country/Geographic risk

79. There is no universally agreed upon definition or methodology for determining whether a jurisdiction, in which the securities provider or intermediary operates, such as a particular country, geographic area or border region within a country, represents a higher risk for ML/TF. Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may be considered as indicators of higher risk include:

a) Countries/areas identified by credible sources[22] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.

c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Organisation.

d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

Customer/Investor risk

80. Securities providers should determine whether a particular customer/investor[23] poses higher risk and analyse the potential effect of any mitigating factors on that assessment. Such categorisation may be due to a customer's occupation, behaviour or activity. These factors considered individually may not be an indication of higher risk in all cases. However, a combination of them may certainly warrant greater scrutiny. Categories of customers whose business or activities may indicate a higher risk include:

a) Customer is sanctioned by the relevant national competent authority for non-compliance with the applicable AML/CFT regime and is not engaging in remediation to improve its compliance.

b) Customer is a PEP or customer's family members or close associates are PEPs (including where a beneficial owner of a customer is a PEP) as covered under R.12.

---

22 "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

23 The use of the term "customer" covers "customer/investor" throughout the guidance.

c) Customer resides in or whose primary source of income originates from high-risk jurisdictions (regardless of whether that income originates from a cash-intensive business).

d) Customer resides in countries considered to be uncooperative in providing beneficial ownership information.

e) Customer acts on behalf of a third party and is either unwilling or unable to provide consistent information and complete documentation thereon.

f) Customer has been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or to financial crimes.

g) Customer's transactions indicate a potential connection with criminal involvement, typologies or red flags provided in reports produced by the FATF or national competent authorities (e.g. FIU, law enforcement etc.).

h) Customer is also a securities provider, acting as an intermediary or otherwise, but is either unregulated or regulated in a jurisdiction with weak AML/CFT oversight.

i) Customer is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business

j) The number of STRs and their potential concentration on particular client groups.

k) Customer is a legal entity predominantly incorporated in the form of bearer shares.

l) Customer is a legal entity whose ownership structure is unduly complex as determined by the securities provider or in accordance with any regulations or guidelines.

m) Customers who have sanction exposure (e.g. have business/activities/transactions).

n) Customer has a non-transparent ownership structure.

Product/Service/Transactions risk

81. A securities provider may offer a range of products/services to customers. An overall risk assessment should therefore include determining the potential risks presented by specific products and services offered by the securities provider. These products and services commonly involve executing transactions for a customer by processing an order to transact or clear trades, handling the movement of funds or securities for the customer and settling a customer's transactions and liabilities. The securities provider may also offer brokerage accounts as a custodian of a customer's assets. Transactions may be conducted on a regulated exchange or other market or they may be conducted between parties directly. A securities provider should assess, using a RBA, the extent to which the offering of its products and services presents potential vulnerabilities to placement, layering or integration of criminal proceeds into the financial system.

82. Determining the risks of products and services offered to a customer may include a consideration of their attributes, as well as any associated risk mitigation measures. Products and services that may indicate a higher risk include:

a) Products or services that may inherently favour anonymity or obscure information about underlying customer transactions (e.g. bearer share instruments or the provision of omnibus account services).

b) The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions.

c) Products with unusual complexity or structure and with no obvious economic purpose.

d) Products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction.

e) Use of new technologies or payment methods not used in the normal course of business by the securities provider.

f) Products that have been particularly subject to fraud and market abuse, such as low-priced securities.

g) The purchase of securities using physical cash.

h) Offering bank-like products, such as check cashing and automated cash withdrawal cards.

i) Securities-related products or services funded by payments from or instructions given by unexpected third parties, particularly from higher risk jurisdictions.

j) Transactions involve penny/microcap stocks.

83. A customer may request transactions that pose an inherently higher risk to the securities provider. This may be detected during transaction monitoring, although in many cases the customer's transactional activity may be apparent during both the point-of-sale interaction and back-end transaction monitoring. Factors that may be considered as indicators of higher risk include:

a) A request is made to transfer funds to a higher risk jurisdiction/country/corridor without a reasonable business purpose provided.

b) A transaction is requested to be executed, where the securities provider is made aware that the transaction will be cleared/settled through an unregulated entity.

Distribution channel risk

84. An overall risk assessment should include the risks associated with the different types of delivery channels to facilitate the delivery of securities products and services. Securities products and services are typically distributed directly to customers (including online) or through intermediaries.

85. A securities provider that distributes products or services directly through online delivery channels should identify and assess the ML/TF risks that may arise in relation to distributing its products using this business model. In addition to the analysis of risks performed in advance of engaging in such an online business, the risk assessment process for online delivery risk should be performed when the securities provider develops new products and new business practices.

86. A securities provider should analyse the specific risk factors, which arise from the use of intermediaries and their services. Intermediaries' involvement may vary with respect to the activity they undertake and their relationship with the securities providers. Some intermediaries may only introduce customers to the securities provider, whereas in other cases intermediaries may also use the products and services for their underlying customers (e.g. where the business relationship is established between intermediary and customer).

87. Regardless of the model, a securities provider should understand who the intermediary is and perform a risk assessment on the intermediary prior to establishing a business relationship. Securities providers and intermediaries should establish clearly their respective responsibilities for compliance with applicable regulation. Assessing intermediary risk is more complex for securities providers with an international presence due to varying jurisdictional requirements, the potential risk of non-compliance by intermediaries with the applicable local AML/CFT regulations and the logistics of intermediary oversight. An intermediary risk analysis should include the following factors, to the extent that these are relevant to the securities providers' business model:

a) Intermediaries suspected of criminal activities, particularly financial crimes or association with criminal associates.

b) Intermediaries located in a higher risk country or in a country with a weak AML/CFT regime.

c) Intermediaries serving high-risk customers without appropriate risk mitigating measures.

d) Intermediaries with a history of non-compliance with laws or regulation or that have been the subject of relevant negative attention from credible media or law enforcement.

e) Intermediaries that have failed to attend or complete AML/CFT training programmes requested by the securities providers.

f) Intermediaries that have weak AML/CFT controls or operate sub-standard compliance programmes, i.e. programs that do not effectively manage compliance with internal policies and/or external regulation or the quality of whose compliance programmes cannot be confirmed.

RISK MITIGATION

88. Having assessed ML/TF risks in their business, securities providers should then develop mitigating controls proportionate to the ML/TF risks identified and to the complexity, nature and size of the entity and activity. Consistent with the RBA,

securities providers should allocate more resources to mitigating their most significant risks.

Customer/Investor due diligence

CDD general considerations

89. CDD processes should be designed to meet the FATF standards and national legal requirements. The CDD process should help securities providers assess the ML/TF risk associated with a business relationship. Securities providers should have policies, procedures, systems and controls which are up to date and effectively implemented to carry out CDD: (a) when establishing business relations with a customer; (b) when carrying out occasional transactions above the applicable monetary threshold; (c) where they have suspicions of ML/TF regardless of any exemption or thresholds; and (d) where they have doubts about the veracity or adequacy of previously obtained identification data. Where a securities provider cannot obtain the information necessary to carry out CDD, R.10 provides that the securities provider not enter into a business relationship or carry out an occasional transaction, or terminate an already existing business relationship, and consider making a suspicious transaction report in relation to the customer.

Initial and ongoing CDD

90. Securities providers should develop and implement policies and procedures to mitigate the ML/TF risks identified through their individual risk assessment. In light of that assessment, CDD processes should help securities providers understand who their customers are by gathering information on what they do and why they require their services. The initial stages of the CDD process should help securities providers assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

91. Based on information obtained in the CDD process, securities providers should prepare a customer risk profile. Customer risk profiles should be informed by the FATF Standards, including those covered in INR.10, R./INR.12-16 and by the risk and complexity of the securities products and services offered. This will determine the level and type of ongoing monitoring and support the securities providers' decision whether to enter into, continue or terminate the business relationship. Risk profiles can apply at the individual customer level or, where groups of customers display similar characteristics (e.g. customers with similar income range, or conducting similar types of securities transactions). On the basis of their risk assessment, securities providers should periodically update customer risk profiles, which should help them apply the appropriate level of CDD.

92. When carrying out the initial CDD, securities providers should identify and take reasonable steps to verify the identity of the customer's beneficial owner, where appropriate. This should be undertaken on the basis of reliable and independent information, data or documentation, to at least the extent required by the applicable legal and regulatory framework. The CDD process also includes understanding the purpose and intended nature of the business relationship to form a basis for ongoing

monitoring of the business relationship and with a view to facilitating the detection of potentially suspicious activity.

93. When designing CDD procedures and conducting CDD on customers, securities providers should, where appropriate, consider the following issues:

- **Purpose and intended nature of business:** A securities provider should ensure it has a clear understanding of expected activity to support ongoing transaction monitoring. Typically, the key consideration is being able to identify whether the customer's activity (e.g. transaction type, size or frequency) is in line with the securities provider's knowledge of the customer. Understanding the nature of the business relationship includes understanding any other parties involved within the relationship. This includes verifying the authorisation of persons purporting to act on behalf of the customer, their identification and verification on a risk-sensitive basis and understanding the role the securities provider plays. In higher risk situations, obtaining further information for ongoing monitoring of the business relationship and detection of potentially suspicious activity may be needed.
- **Beneficial ownership structures:** Where a customer appears to have a less transparent beneficial ownership or control structure, including the presence of corporate vehicles, nominees or private legal arrangements, a securities provider should ensure to undertake reasonable steps to verify the identity of beneficial owner(s). Securities provider should also consider whether the opacity of the ownership structure or the identity of one or more beneficial owners is an indicator of elevated risk and whether it is a cause or not for not performing the transaction or terminating the business relationship and considering making a suspicious transaction report.
- **Source of wealth and funds:** Under the RBA, a securities provider should take reasonable measures to establish the source of wealth and source of funds of relevant parties.

94. In addition, securities providers should take measures to comply with national and international sanctions legislation; sanction screening is mandatory and is not discretionary.

95. As a general rule, securities providers must apply CDD measures to all customers. The extent of these measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk associated with the individual business relationship. This means that the amount and type of information obtained, and the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher or decreased where the associated risk is lower.

96. A securities provider should conduct CDD on an initial and ongoing basis. A securities provider should endeavour to be aware of material changes to the customer's legal form, beneficial ownership and nature of business. A securities provider should implement procedures to periodically review the customer relationship and CDD information. The risk-based periodic review process should be based on a formal cycle, and additional reviews should be performed based on "trigger-event" causes.

The securities provider's customer

97. In addition to carrying out transactions and/or maintaining accounts for customers directly, securities providers may also deal with other securities providers and intermediaries who in turn have their own underlying customers. For illustration purposes, refer to paragraph 31, which provides an example of investment funds where the customer may be direct or indirect. Also, for a discussion of issues particular to similar correspondent relationships in the cross-border context, refer to section 7.1.5 of this Guidance.

98. The business relationship between the securities provider, the intermediary and any underlying customers, including the degree of transparency the securities provider has into any underlying customers and their transactions will affect a number of AML/CFT obligations and outcomes, such as who is responsible for conducting CDD, the securities provider's risk assessment of the intermediary and the securities provider's ability to monitor transactions associated with the intermediary and its underlying customers.

99. When determining the type and extent of CDD to apply, a securities provider should be clear as to whether its customer is acting on its own behalf or as an intermediary on behalf of its underlying customers. Even when CDD is the responsibility of the intermediary, an understanding of the intermediary's customer base can often be a useful element in determining the risk associated with the intermediary itself; the level of understanding obtained should be tailored to the perceived risk level of the intermediary.

100. While a detailed analysis of the wide variety of intermediary and customer relationships that occurs in the securities sector is beyond the scope of this Guidance, a brief discussion of the distribution of investment funds may illustrate some common themes and concerns. In this context, the CDD measures an investment fund should take will depend on how the ultimate customer invests in the fund. Depending on how the investment fund is sold, with whom the business relationship is established or who is registered in the fund's share/units register, the investment fund may be required to treat an underlying investor as its customer or the intermediary as its customer. Where an intermediary is treated as the investment fund's customer, the investment fund may not have visibility on the intermediary's underlying customers. This includes not having comprehensive identification nor transaction-related information on the customers of the intermediary in cases such as, for example, where the intermediary nets all of its customers' orders and submits a single net order to the investment fund each day.

101. Securities providers should also obtain (and intermediary should provide) information about the intermediary's AML/CFT controls, including information regarding the intermediary's risk assessment of its underlying customer base and its implementation of risk mitigation measures.

102. The above requirements may be adapted to particular conditions (e.g. additional onsite control or other more thorough controls when an intermediary is a non-regulated or non-supervised entity or is located in a country presenting high ML/TF risks).

Enhanced CDD ("EDD") and simplified CDD ("SDD")

103. The extent of CDD measures may be adjusted, to the extent permitted by applicable regulatory requirements, in line with the ML/TF risk. This means that the amount or type of information obtained, or the extent to which this information is verified, must be enhanced where the risk associated with the business relationship is higher. The type of enhanced due diligence measures applied should be effective and proportionate to the risks. It may also be reduced where the risk associated with the business relationship is lower. Ongoing monitoring can also lead to a reassessment of the customer's risk profile, and should inform whether additional CDD or EDD is required.

104. The derogation described in INR.1.6(b), which permits countries to decide not to apply some FATF Recommendations to financial institutions conducting financial activity on an occasional or very limited basis is not generally appropriate, unless there is proven low risk of ML/TF. SDD measures are also not acceptable whenever there is a suspicion of ML or TF, or where specific higher-risk scenarios apply.

105. One example of when SDD measures may generally be appropriate is a pension product funded directly from a reputable company's payroll as such a product may present a lower ML/TF risk compared to other products. Conversely, EDD measures must be required for a PEP customer since such a customer presents heightened risks. Illustrative examples of both SDD and EDD measures are detailed below. However, these examples are intended to form a non-exhaustive list, and financial institutions are encouraged to apply a risk-based analysis that takes account of the particular circumstances of each case.

Box 1. Non Exhaustive List of Examples of Enhanced Due Diligence/Simplified Due Diligence measures (see also INR.10)

Enhanced Due Diligence

- Obtaining additional customer information, such as the customer's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the customer risk profile
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the customer risk profile
- Carrying out additional searches focused on financial crime risk indicator (i.e. negative news screening) to better assess the customer risk profile
- Obtaining additional or more particular information about the intermediary's underlying customer base and its AML/CFT controls
- Undertaking further verification procedures on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may be involved in criminal activity
- Obtaining additional information about the customer's source of wealth or the source of funds involved in the transaction
- Verifying the source of funds or wealth involved in the transaction or business relationship to seek to ensure they do not constitute the proceeds of crime
- Evaluating the information provided with regard to the destination of funds and the reasons for the transaction
- Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship
- Requiring that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the customer
- Increasing the frequency and intensity of transaction monitoring

Simplified Due Diligence

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer pieces of customer identification data
- Altering the type of verification carried out on customer's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established, without collecting additional information or carrying out additional measures related to understanding the nature and purpose
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if transaction or account values rise above a defined monetary threshold)
- Reducing the frequency of customer identification updates if the securities provider implements or is required to implement a periodic review process based on a formal cycle
- Reducing the degree and extent of on-going monitoring and scrutiny of transactions, for example based on a reasonable monetary threshold

Correspondent Relationships [24]

106. INR.13 stipulates that for correspondent banking and other similar cross-border relationships, financial institutions should apply criteria (a) to (e) of R.13, in addition to performing normal customer due diligence measures. Because certain relationships in the securities sector have characteristics similar to cross-border correspondent banking relationships, they are addressed in this Guidance.

107. A typical cross-border correspondent relationship in the securities sector is a relationship between the securities provider (correspondent), with an intermediary (respondent), which is regulated and supervised by a supervisory authority, for securities transactions. In such cases, the customer of the respondent would not be considered as a customer of the correspondent, and the FATF Recommendations do not require the correspondent securities providers to conduct CDD on the customers of their respondent institutions. One example of these types of relationships could be between a global securities firm (correspondent) executing securities transactions on a stock exchange for a cross-border intermediary, acting as a respondent for its underlying local customers, subject to complying with R.13 requirements.

108. Not all cross-border correspondent relationships pose the same level of ML/TF risk and the securities providers should adjust the type and extent of CDD measures to account for the risk posed by the respondent. The correspondent institution should monitor the respondent institution's transactions with a view to detecting any changes in the respondent institution's risk profile (i.e. compliance with AML/CFT measures and applicable targeted financial sanctions), any unusual activity or transaction on the part of the respondent, or any potential deviations from the agreed terms of the arrangements governing the correspondent relationship. Where such concerns are detected, the securities provider should follow-up with the intermediary by making a request for information on any particular transaction(s), possibly leading to more information being requested on the underlying customers of the intermediary on a risk-sensitive basis.[25]

109. Due diligence with regard to a correspondent relationship with a respondent generally takes place at two levels:

- Risk-based due diligence on the respondent by using reliable, independent source documents, data or information (Rec. 10 (a)) and its beneficial owners, such that the securities provider is satisfied that it knows who the beneficial owner(s) of the respondent are.
- Additional due diligence on the correspondent relationship with the respondent, as described below.

110. In accordance with R.13, correspondent securities providers in addition to performing customer due diligence on the respondent intermediaries should also:

- Gather sufficient information about the respondent to understand the nature of the respondent's business and to determine from publicly available information the reputation of the respondent and the quality of its

24 FATF Guidance on correspondent banking services (October 2016).

25 See Paragraph 3 of the FATF Guidance on correspondent banking services (October 2016).

supervision, including whether and when it has been subject to targeted financial sanctions, a ML/TF investigation or regulatory action;

- Assess the respondent's AML/CFT controls. The assessment should include confirming that the respondent institution's AML/CFT controls are subject to independent audit (which could be external or internal). A more detailed/in-depth review should be conducted for higher risk relationships, possibly including reviewing the independent audit, interview of compliance officers, a third party review and potentially an onsite visit;
- Obtain approval from its senior management before setting up a correspondent relationship;
- Clearly understand the respective AML/CFT responsibilities of each institution.

111. In the case of such relationships, the correspondent generally does not have direct relationships with the customers of the respondent. There is no expectation or requirement for the correspondent to apply CDD on a respondent's customer, which is, instead the responsibility of the respondent. Nonetheless, it is consistent with the risk-based approach for the correspondent to have some general sense of the respondent's customer base as part of ascertaining the risks associated with the respondent itself.

112. In case the respondent allows its underlying customers to have direct access to its correspondent accounts (for example through a power of attorney or permitting the underlying customer to place orders directly with the securities provider while settling them through the correspondent account), the securities provider must be satisfied that the respondent has conducted CDD on the customers having direct access to these accounts, and that it is able to provide relevant CDD information upon request.

113. Securities providers should also be prohibited from entering into, or continuing, a correspondent relationship with shell banks or shell securities providers. They should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks or securities providers.

Reliance on third parties

114. In accordance with R.17 and where permitted by local legislation, a securities provider may reasonably rely on third parties for performing some elements of initial CDD (identification of customer, identifying and taking reasonable measures to verify identification of beneficial owner and understanding the purpose and intended nature of business relationship). However, it may not rely on such parties to perform ongoing monitoring, ongoing due diligence and scrutiny of transactions. The term 'third parties' means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under R.17. Specifically the securities provider should complete appropriate due diligence on the third party to determine whether reliance can be placed on the AML/CFT risk and control framework of financial institution or DNFBP and whether they are based in a country whose risk has been assessed by the securities provider (in accordance with R.17(1) (c and d).

115. When reliance is appropriate, after consideration of the above, the ultimate responsibility for CDD remains with the securities provider- in other words, the provider can delegate the task but not the responsibility. In such situations, the securities provider should verify that the third party is conducting checks similar to or at a higher level than the securities provider's own internal standards. The securities provider should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in R.10, and also take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the relied upon institution upon request and without delay.

116. Where appropriate, securities providers should ensure that formal agreements, which clearly set out the terms and conditions, including the roles and responsibilities of both the securities provider and the institution relied upon, are in place.

Outsourcing

117. The reliance model above can be contrasted with an outsourcing or agency scenario, where the outsourced entity conducts CDD on behalf of the securities provider, in accordance with the procedures of securities provider and under its instructions. In such case, the securities provider is the principal while the outsourced entity acts as its agent.

118. Under an outsourcing arrangement, a securities provider may also outsource ongoing monitoring and transaction monitoring. Securities providers should ensure that formal agreements which clearly set out the relevant terms and conditions, including the roles and responsibilities of both the outsourced entity and the securities provider, are in place.

119. The ultimate responsibility for CDD and/or ongoing monitoring remains with the securities provider; again, it cannot delegate responsibility. In this regard, the securities provider should implement appropriate processes to monitor that the outsourced entity is performing effectively in accordance with the instructions set by the securities provider.

Electronic wire transfers requirements

120. R.16 establishes the requirements for countries with respect to wire transfers. R.16 apply to both cross-border wire transfers and domestic wire transfers[26]. Securities providers who make wire transfers must include relevant originator and beneficiary information, where appropriate, on those wire transfers and ensure that the information remains with the wire transfer throughout the payment chain, as set out in the INR.16. Countries may adopt a *de minimis* threshold for cross-border wire transfers, below which verification of the customer and beneficiary information is not required unless there is an ML/TF suspicion[27]. That is, for occasional cross-border wire transfers below USD/EUR 1 000, or the equivalent amount in local currency, the requirements of the INR.16 apply and the name of the originator and of the

26 INR.16 paragraph 3.

27 INR.16 paragraph 5.

beneficiary will be requested, as well as an account number for each or a unique transaction reference number. However, such information will not have to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to the customer should be verified.

121. Securities providers that make wire transfers should adopt effective risk-based policies and procedures for determining when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information, as well as for defining and taking the appropriate follow-up actions[28]. In case of doubt, securities providers should clarify the responsibility for monitoring wire transfers between themselves and any other person involved in the wire transfer.

122. Where securities providers rely on payment service providers for fund transfers, depending on the arrangement, the responsibility for AML/CFT compliance with relevant electronic wire transfer requirements may likely be with the payment service provider.

Suspicious transaction monitoring and reporting

Risk-based monitoring

123. Ongoing risk-based transaction monitoring is the scrutiny of transactions to determine whether they are consistent with the securities provider's information about the customer and the nature and purpose of the business relationship. This should include surveillance of securities transactions and fund movements. Monitoring also involves identifying changes to the customer risk profile - for example, the customer's behaviour, use of products and the value involved, and keeping this information up-to-date, which may trigger the application of enhanced CDD measures. When suspicious activity or high-risk behaviour is identified, appropriate steps should be taken in a timeline commensurate with the risk.

124. Transaction monitoring is essential for identifying suspicious transactions. Transactions that are not in line with the customer's risk profile, that exhibit red flags of established money laundering typologies, or that deviate from the usual pattern, may be potentially suspicious. Securities providers may also draw upon surveillance frameworks and tools used to detect predicate offences to money laundering, such as market abuse and insider dealing in securities, to identify suspicious transactions. Integration of existing data sets more efficiently into AML/CFT framework can produce more effective results.

125. In many wholesale business relationships, such as principal to principal execution-only, the securities provider will generally have limited visibility of the end-to-end transaction; it is also typical for the underlying instructing party to have multiple brokers and deal in various products and asset classes, meaning that securities providers will only have visibility of a part of the overall trading activity. In such circumstances, effective transaction monitoring measures are likely to consist of leveraging existing market surveillance controls, rather than implementing electronic transaction monitoring systems similar to those in retail relationships. For example, in wholesale markets, securities providers may reasonably determine that, given the

[28] INR.16 paragraph 18 and 22.

difficulties in developing meaningful rules for electronic monitoring, it may be appropriate to implement alternative methods of monitoring. Whatever the approach taken, the securities provider should be able to demonstrate the rationale for their monitoring strategy.

126. A customer may transact in multiple jurisdictions and with multiple financial firms, which perform a variety of activities in relation to securities transactions. A securities provider may consider the following to determine the nature and extent of monitoring activity:

a) The nature of the securities provider's customer base, including the country risk and whether customers are regulated or unregulated entities, and publicly or privately owned;

b) The risk and complexity of products offered to customers;

c) The volume and frequency of transactions processed by the securities provider; and

d) The execution, clearing or settlement processes facilitated by the securities provider, including consideration as to whether payments to third parties are permitted.

127. Transaction monitoring should be carried out on an ongoing basis and may be triggered by specific and unusual transactions. For example, a sudden spike in trading volumes for a particular issuer can be a red flag of potentially suspicious activity, such as a fraud associated with low priced securities. However, market events, like corporate announcements, news or rumours on likely mergers or acquisitions may also contribute to unusual trading patterns; this means that such a sudden spike in trading volume may not be suspicious upon further consideration, but instead was simply a red flag worthy of further inquiry. Therefore, in conducting effective transaction monitoring, the securities provider should take into account such market events.

128. Securities providers should consider adjusting the extent and depth of monitoring based on their institutional risk assessments, customer risk profiles and the complexity of products offered. For example, having less visibility into the underlying customer of an intermediary might increase the risk profile of the intermediary itself. Enhanced monitoring should be required for higher risk situations. The adequacy of monitoring systems and the factors leading securities providers to adjust the level of monitoring should be reviewed regularly to verify that it is in line with the securities provider's overall AML/CFT risk programme.

129. Monitoring under a RBA allows securities providers to create internal thresholds based on a range of factors, such as transaction number or value to determine which activities should be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. Monitoring system should flag unusual movements of funds or transactions for further analysis and scrutiny in a timely manner for determining as to whether the funds movements or transactions are suspicious.

130. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be readily explicable. If a securities provider establishes different customer segments for monitoring, it should document and state

clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers.

131. Where automated systems are appropriate, securities providers should understand their operating rules, verify their integrity on a regular basis and check that they consider the identified ML/TF risk typologies applicable for the securities sector.

132. Securities providers should properly document, retain and communicate to the relevant staff the results of their monitoring and any queries raised and resolved.

Reporting suspicious activity

133. R.20 requires all financial institutions - including securities providers - that suspect, or have reasonable grounds to suspect, that funds are the proceeds of crime or related to terrorist financing to report their suspicions promptly to the relevant FIU.

134. Transactions or movements of funds that are considered suspicious should be promptly reported to the FIU, in the manner specified by the competent authorities. Securities providers' processes to escalate suspicions and ultimately report to the FIU should reflect this. While the policies and processes leading securities providers to form a suspicion can be applied on a risk-sensitive basis, a securities provider should report the activity once ML/TF suspicion has been formed.

135. Some jurisdictions require that suspicious market abuse (see paragraphs 24-26 above in relation to market abuse) be reported to a different authority (other than or in addition to FIU), generally the markets regulator. A securities provider should be aware of the specific reporting obligations required by the jurisdiction in which it is operating.

INTERNAL CONTROLS AND COMPLIANCE

Internal controls and governance

136. Adequate internal controls are critical for an effective AML/CFT framework. Internal controls include appropriate governance arrangements that clearly allocate AML/CFT responsibilities, and controls to monitor the integrity of staff and intermediaries, implemented in accordance with the applicable local legislation. Securities providers should consider national or sectoral risk assessments and controls to validate that their policies and processes are effective for identifying, assessing, and monitoring ML/TF risks where they operate. Securities providers should modify their internal controls according to relevant changes in their size, operational complexity or risk exposure. Accordingly, securities providers should maintain systems that are adequate and effective to manage and mitigate their risks. Where the risks are low, less sophisticated systems will suffice.

137. Securities providers, which distribute their products or services through intermediaries, such as stockbrokers or funds platforms, should include these networks in their AML/CFT internal risk assessment processes.

138. The successful implementation and effective operation of a RBA to AML/CFT also depends on strong leadership by a securities provider's senior management, which includes oversight of the development and implementation of the RBA across business.

139. Senior management should consider various ways to support AML/CFT initiatives, including:

a) The fostering of a culture of compliance and promoting compliance as a core value of the securities provider by sending a clear message that the securities provider is committed to ensuring that:
   - ML/TF risks will be managed before entering into, or maintaining, business relationships or offering services that are associated with significant ML/TF risks; and
   - Business relationships will not be established when the ML/TF risks cannot be mitigated and managed.

b) Together with the company board of directors (where applicable), taking responsibility for setting up robust risk management governance and controls mechanisms that:
   - Reflect the company's established risk policy;
   - Implement adequate internal communication processes appropriate for the ML/TF risks faced by the securities provider. Where applicable, these processes should link the board of directors, the top AML/CFT compliance officer, any relevant committee (e.g. the risks or ethics/compliance committee), the information technology unit and each of the business areas;
   - Help to determine the measures needed to mitigate the identified ML/TF risks and the extent of residual risk the securities provider is ready to accept; and
   - Allocate adequate resources for the securities provider's AML/CFT function.

140. Senior management should not only be aware of the ML/TF risks to which the securities provider is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. This would require that senior management:

a) Understands the regulatory and supervisory requirements where the securities provider operates;

b) Receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the securities provider is exposed through its activities and individual business relationships;

c) Receives sufficient and objective information to understand whether the securities provider's AML/CFT controls are effective;

d) Receives updates on government enforcement actions and other communications related to the AML/CFT obligations of securities providers and ML/TF risks; and

e) Ensures that processes are in place to timely escalate important decisions that directly affect the ability of the securities provider to address and control risks.

141. A sufficiently senior person within a securities provider should have the responsibility to ensure the effectiveness of AML/CFT controls. This is to highlight the importance of ML/TF risk management and compliance and for bringing ML/TF issues to senior management's attention. This includes the appointment of a skilled compliance officer at the senior management level[29]. The group top AML/CFT officer should have the necessary independence, authority, seniority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including across lines of business, and across foreign branches and subsidiaries).

142. R.18 requires financial institutions to have an independent audit function to test the effectiveness of its AML/CFT programme, policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestic and cross-border. Such independent testing should allow senior management to validate the development and operation of the risk assessment and management processes and internal controls, in order to ensure that the adopted measures reflect the risk profile of the securities provider. This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, specialist consultants or other qualified parties who are not involved in the design, implementation or operation of the securities provider's AML/CFT compliance programme. The testing should be risk-based; evaluate the adequacy of the securities provider's AML/CFT policies and programme and the quality of risk management for its operations, departments and subsidiaries; and cover all activities.

143. Both the compliance and audit functions should base their assessment on all information relevant to their task including, where relevant and appropriate, information obtained confidentially through relevant internal mechanisms or whistleblowing hotlines. Other sources of information can include training pass rates, compliance process or control failures or analysis of questions received from staff.

Compliance controls

144. A securities provider's internal control environment should be designed to achieve high standards of the integrity, competence and compliance of staff with relevant policies and procedures.

145. The nature and extent of AML/CFT controls will depend upon a number of factors, including the nature, scale and complexity of a securities provider's business. This includes the diversity of its operations, geographical location, customer base, product and activity profile and the degree of risk associated with each area of its operations (e.g. the extent to which the securities provider is dealing directly with the customer or through intermediaries, third parties, or in a non-face-to-face setting without appropriate mitigating measures).

29 INR.18.

146. The framework of AML/CFT compliance function and internal controls should:

a) Place priority on the securities provider's operations (products, services, customers and geographic locations) that are more vulnerable to abuse.
b) Provide for regular review of the risk assessment and management processes, taking into account the environment within which the securities provider operates and the activity in those locations in which it operates.
c) Provide for an AML/CFT compliance function and review programme that includes the testing of key components.
d) Verify that adequate risk assessment and controls are in place before offering new products or services.
e) Regularly inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports.
f) Provide for programme continuity despite changes in management or employee composition or structure.
g) Focus on complying with applicable regulatory requirements on record keeping and reporting for AML/CFT compliance and timely response to changes in regulations.
h) Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
i) Provide for adequate management and oversight of its intermediaries, including initial intermediary due diligence, oversight of AML/CFT training, and ongoing risk-based monitoring.
j) Provide for adequate supervision of employees who handle transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the business's AML/CFT programme.
k) Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
l) Ensure that staff or firm performance is not the driver for taking disproportionate ML/TF risks.
m) Provide for appropriate initial and refresher training to for all relevant staff.
n) Provide for initial and refresher training for intermediaries, as applicable, at appropriate intervals.

Vetting and recruitment

147. Securities providers should conduct background checks on staff as part of the recruiting process to satisfy themselves that the staff they employ have integrity, are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls, whether in the compliance or front-line functions.

148. The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management's roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

Training and awareness

149. The effective application of AML/CFT policies and procedures depends on the understanding of securities providers' staff of the relevant requirements and accompanying processes they are required to follow and the risks these processes are designed to mitigate. This training is designed to mitigate potential ML/TF risks occurring by, at or through a securities provider. Staff should receive AML/CFT training, which should be:

a) Relevant to the securities provider's ML/TF risks and business activities and up to date with the latest legal and regulatory obligations and internal controls;

b) Obligatory for all appropriate staff, including senior management;

c) Tailored, where applicable, to particular lines of business within the securities provider, equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks. This may be particularly important with regard to staff responsible for identifying fraud and market abuse, which may be reportable as a suspicious transaction;

d) Effective, as measured, for example, by requiring staff to pass tests as part of the training or by monitoring levels of compliance with the securities provider's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;

e) Regular, relevant, and not a one-off exercise when staff are hired, in line with INR.18; and

f) Complemented by AML/CFT information and updates that are disseminated to relevant staff, as appropriate.

150. Overall, the AML/CFT training should also seek to build a culture in which compliance is embedded in the activities and decisions by its staff. Training may also be provided by a third party, though the securities provider remains responsible for the quality of the training.

SECTION III – GUIDANCE FOR SUPERVISORS

151. The RBA to AML/CFT aims to develop prevention or mitigation measures that are commensurate to the ML/TF risks identified. For supervision, this applies to the way supervisory authorities allocate their resources and conduct supervisory tasks to facilitate the application of a risk-based approach by securities providers.

THE RISK-BASED APPROACH TO SUPERVISION

152. R.26 requires countries to subject securities providers to adequate AML/CFT regulation and supervision. INR.26 requires supervisors to allocate supervisory resources to areas of higher ML/TF risk, based on supervisors' understanding of the ML/TF risks in their country, and to have on-site and off-site access to all information relevant to determining a securities provider's risk profile. There is a higher supervisory standard for the supervision of institutions subject to core principles.

Box 2. Recommendation 26: Regulation and Supervision of Financial Institutions

[…..] For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions (for intermediaries) should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. […..]

Additional sources of information

- Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis - The Risk-Based Supervision Guidelines published by the European Supervisory Authorities (April 2017).
- Principles on customer identification and beneficial ownership for the securities industry published by the IOSCO (May 2004).
- AML Guidance for collective investment schemes published by the IOSCO (October 2005).

Understanding ML/TF risk

153. Supervisors should understand the ML/TF risks to which the securities sector is exposed[30], and the ML/TF risks associated with securities providers, both at an individual firm level and a financial group level, and the different securities sub-

[30] Consistent with IOSCO Core Principle (ICP) 6.

sectors in which they operate. Supervisors should draw on a variety of sources to identify and assess ML/TF risks, including information from stock exchanges and self-regulatory bodies.

154. For sectoral risks, these are likely to include, but will not be limited to, the jurisdiction's national and sectoral risk assessments, domestic or international typologies and supervisory expertise, as well as FIU feedback.

155. For individual securities providers, supervisors should take into account the level of inherent risk for that provider including the nature and complexity of its products and services, size and business model, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location and countries of operation. Supervisors should also look at the controls in place, including the quality of the risk management policy, the effectiveness of the internal oversight functions, the history of the securities provider's compliance with regulations, STR reporting history (including quality, timing and volume of STRs submitted) and other open source information.

156. Some of this information should be obtained from the supervised entities (e.g. on the size, business model, location and nature of business). Some of this information can also be obtained through prudential supervision or routine supervisory oversight of the sector. Other information, which may be relevant in the AML/CFT context, includes the fitness and propriety of the senior management and the adequacy of the compliance function[31]. In some jurisdictions, this may involve information sharing and collaboration between prudential and AML/CFT supervisors or between different AML/CFT supervisors, especially when the responsibilities belong to two or more separate agencies.

157. Information from the securities providers' other stakeholders such as other supervisors, industry bodies, FIUs and law enforcement agencies may also be helpful in determining the extent to which a securities provider is able to effectively manage the ML/TF risk to which it is exposed.

158. Supervisors and other competent authorities should review their assessment of both the sector's and a specific securities provider's ML/TF risk profile periodically, and when a provider's circumstances change or new threats or vulnerabilities emerge. These could include, for example, new products and delivery channels that pose ML/TF risks, or the absence of local regulations to govern them sufficiently.

Mitigating ML/TF risk

159. The FATF Recommendations require supervisors to allocate more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risk to which the sector and individual securities providers are exposed. It also means that where detailed supervision of all securities providers for AML/CFT purposes is not feasible, supervisors should give priority to the areas posing higher risk, either in the individual securities provider or to securities providers operating in a particular sector.

31 As specified in ICP 3.

160. Examples of ways in which supervisors can adjust their approach include:

a) **Performing additional enhanced checks, as appropriate, as part of their authorisation function:** supervisors can adjust the level of information they require to prevent criminals or their associates from holding a significant or controlling interest in a securities provider. Where the ML/TF risk associated with the applicant is considered low (e.g. due to ownership structure, nature of business and role in a securities transaction), the associated opportunities for ML/TF may also be limited and thus supervisors may decide to approve applications on a review of relevant documentation. Where the associated ML/TF risk is considered high, supervisors may ask for additional information and set out more elaborate processes, including for example face-to-face interviews, criminal record and background checks, liaisons with other authorities, etc.

b) **Adjusting the type of AML/CFT supervision:** supervisors should have both on-site and off-site access to all relevant risk and compliance information. To the extent permitted by their regime, supervisors can also determine the correct mix of on-site and off-site supervision. Off-site supervision alone may not be appropriate in higher risk situations.

c) **Adjusting the frequency and nature of ongoing AML/CFT supervision:** supervisors should adjust the frequency of AML/CFT supervision in line with the risks identified. They should combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g. due to information received from law enforcement or whistle-blowers). General supervisory findings on thematic areas (e.g. focused reviews of particular products or services or types of providers or customers, or particular areas of interest such as beneficial ownership, distribution channels used etc. by securities providers) may also inform these supervision decisions.

d) **Adjusting the intensity of AML/CFT supervision**: supervisors should determine the scope or level of supervision in line with the risks identified in order to assess the adequacy of a securities provider's policies and procedures. Examples of more intensive supervision could include detailed review of the implementation and adequacy of the provider's risk assessment, files on CDD and reporting, record-keeping policies and processes and internal auditing. This may also include interviews with operational staff, senior management and the board of directors and AML/CFT assessment in particular lines of business.

161. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and framework remains adequate. Whenever appropriate, these findings should also be communicated to the provider to enable them to enhance their RBA.

162. In line with R.26 and the application of the International Organisation of Securities Commissions (IOSCO) Core Principles relevant for AML/CFT[32], securities supervisors should consider the results of other prudential or financial supervision in their AML/CFT supervisory activities. Similarly, they should check that the broader

[32] IOSCO Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D.

prudential findings that drive the overall supervisory strategies of securities providers are informed by, and adequately address, the findings of the AML/CFT supervisory programme.

163. FATF R.27 and R.35 requires supervisors to have the power to impose adequate sanctions on securities providers and intermediaries when they fail to comply with AML/CFT requirements. Supervisors should use proportionate actions, including a range of supervisory interventions; remedial/corrective actions to ensure proper and timely correction of identified deficiencies and punitive sanctions for more egregious non-compliance, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or significant failure in controls will result in a more severe supervisory response.

AML/CFT supervision of securities providers in a cross-border context

164. For cross-border supervision, supervisors of the home jurisdiction should have access to the customer, account and transaction information maintained by the financial institution in the host jurisdiction, to the extent permissible under the legal frameworks of both jurisdictions. This should include STR or STR-related information, where this is necessary to assess compliance with AML/CFT obligations and the robustness of risk management procedures. While host supervisors will be assessing compliance with local laws and obligations, home supervisors should have the ability to assess compliance with group-wide AML/CFT policies and procedures.

165. Lack of such access may inhibit the ability of the home supervisor to effectively assess group compliance, thereby affecting the effective implementation of FATF Recommendations. If the reasons for the denial of access prove to be insurmountable and there are no satisfactory alternative arrangements, the home supervisors should inform the host supervisor that the financial institution may be subject to additional supervisory actions. This could result in enhanced supervisory measures on the group, including, as appropriate, requesting the parent group to close down its operations in the host country.

166. In adopting a RBA to supervision, countries and competent authorities may consider allocating supervised entities sharing similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of business, type of customers serviced, geographic areas of activities and delivery channels. The setting up of such groupings could allow competent authorities to take a comprehensive view of the securities sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual securities provider or intermediary. If the risk profile of a securities provider or intermediary within a grouping changes, the supervisor may reassess the supervisory approach, which may include removing the securities provider or intermediary from the grouping.

SUPERVISION OF THE RISK-BASED APPROACH

General approach

167. Supervisors should encourage and monitor securities providers' adoption of a RBA that is in line with the FATF recommendations, and that is risk-appropriate given the provider's respective business models, size of operations, and operating environments.

168. Supervisors should note that under the RBA, particularly in the securities sector, given the diversity in size, scale of operations, business models and domestic regulatory requirements, there may be valid reasons for differences in securities providers' controls. There is therefore no one-size-fits-all approach; proportionality is an important element to be considered. In evaluating the adequacy of their RBA, supervisors should take into consideration the merits of these differences.

169. The securities sector is inter-connected with the rest of the financial system, in particular the banking system. Supervisors should get a good understanding of the effect of such interconnections on the ML/TF risk of the securities providers, and make appropriate adjustments where necessary to the supervisory RBA.

170. The task of supervising the implementation of the risk-based approach is a challenging one. To be effective, the following are some of the necessary preconditions:

- **Adequate understanding of ML/TF risk in the sector, sub-sector and individual firms.** Supervisors should adopt measures to acquire and maintain adequate and up to date knowledge of the ML/TF risks faced by the industry. They should have a thorough understanding of the higher and lower risk lines of business. This understanding should help supervisors form a sound judgment about the proportionality and adequacy of AML/CFT controls.
- **Adequate resources and skillsets.** Supervisors should have adequate financial, human and technical resources to properly conduct the risk-based supervision. In assessing the adequacy of resources, considerations include the size and complexity of the sector and the level of ML/TF risks faced by the sector.
- **Strong supervisory focus on effective implementation of controls by securities providers.** Basic compliance with the relevant laws and regulations is necessary but not sufficient. For an effective RBA, supervisors should also focus on assessing the quality of the securities providers' controls and effectiveness of their implementation to mitigate the ML/TF risks. Supervisors should clearly articulate and communicate their expectations, including the necessary rectification measures where there are deficiencies in providers' controls.

171. Examples of supervisory practices adopted in a number of countries for implementation of the RBA in the securities sector are set out in Annex A.

Training

172. Training is important for the supervision staff to understand the securities sector and the various business models that exist. In particular, supervisors should ensure that the staff are trained to assess the quality of a securities provider's ML/TF risk assessments and the adequacy, proportionality, effectiveness, and efficiency of the securities provider's AML/CFT policies, procedures and internal controls in light of its risk assessment.

173. Training should allow the supervisory staff to assess and form sound judgments about the quality of the securities provider's risk assessment and effectiveness of the securities provider's AML/CFT control. It should also aim at achieving consistency in the supervisory approach at the national level in case of multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

174. Given the diversity and complexity within the securities sector (e.g. due to emergence of new business models and technologies), supervisory authorities should conduct continuous training programmes for supervisors, so that they can develop and maintain their proficiency. A training programme could include the following topics:

a) General AML/CFT issues;

b) Business models of various sub-segments of the securities sector (e.g. broker-dealers, fund managers) and the associated ML/TF risk issues;

c) Interaction among the various sub-segments of the securities sector, and with other parts of the financial system (e.g. the banking system), as well as the impact on the scale and nature of ML/TF risks;

d) International regulatory actions, such as economic sanctions;

e) National and international supervisory cooperation mechanisms; and

f) Other pertinent issues (e.g. implementation of common reporting standards, enhancing transparency of beneficial ownership, and the effect of financial technology developments on ML/TF risks).

Guidance and Feedback

175. Supervisors should communicate their expectations of financial institutions' compliance with their legal and regulatory obligations. This could be done through a consultative process after engaging with relevant stakeholders. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Guidance issued to securities providers should also discuss ML/TF risk within their sector and also outline ML/TF indicators (transactional and behavioural) in order to help them identify suspicious transactions.

176. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the industry, which may cover operational issues, and be more detailed and explanatory in nature. Securities

providers should note, however, that the private sector guidance they take into consideration should be consistent with national legislation and with any guidelines issued by competent authorities and international standards.

177. Supervisors should communicate with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities. This is particularly important where more than one supervisor is responsible for supervision (e.g. where the prudential supervisor and the AML/CFT supervisors are in different agencies or in separate divisions of the same agency). Multiple guidance should not create opportunities for regulatory arbitrage, loopholes or unnecessary confusion among securities providers. When possible, relevant regulatory and supervisory authorities should consider preparing joint guidance.

178. To the extent possible, supervisors and FIUs should provide timely feedback to securities providers on effectiveness of their monitoring/reporting systems, quality of STRs filed and AML/CFT controls in general. A well-defined and institutionalised feedback mechanism can enhance the effectiveness of the monitoring and surveillance system to capture as many suspicious transactions as possible while efficiently avoiding too many false-positives. Guidance on potential risk indicators in the securities sector, in consultation with the industry, where feasible, can also be considered.

ANNEX A. EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RBA IN THE SECURITIES SECTOR

Canada

179. As the AML/CFT supervisor in Canada, FINTRAC issues sector specific workbooks that help reporting sectors design a risk-based approach that is tailored to their business, including for securities: http://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-sec-eng.asp.

Guernsey

180. Guernsey is an international finance centre with a significant collective investment funds sector. There are more than 800 Guernsey domiciled funds authorised or registered by the Commission, which is the regulatory authority responsible for AML/CFT, conduct and prudential supervision of Guernsey's financial services sector.

181. Prudential and conduct supervision is undertaken by sector specific supervisory divisions with a dedicated AML/CFT supervisory division responsible for risk-based AML/CFT supervision across the industry as a whole. The AML/CFT supervisory division works closely with the relevant supervisory divisions. This collaboration includes sharing prudential, conduct and AML/CFT issues because of the crossover implications an issue may have for both supervisory teams, and in undertaking joint onsite inspections to optimise its resources.

182. The AML/CFT supervisory division also undertakes its own onsite inspections depending upon the firm's ML/TF risk profile, which is assessed annually utilising business and compliance data received from the firm, together with open source and confidential information available to the Commission, such as information from Guernsey's FIU. Each Guernsey fund must appoint a designated fund administration company which is responsible for discharging the fund's AML/CFT obligations, and in particular for the initial and ongoing customer due diligence on investors into the fund. Five of these administration firms administer approximately half of the assets under management in the funds sector. These administrators are subject to structured supervisory engagements, including onsite inspections at least every three to four years, under the Commission's risk-based supervisory model.

183. Smaller administration firms are subject to less frequent structured supervisory engagements, the Commission uses thematic reviews to assess key issues on a firm and sector basis. As an example, the prudential and AML/CFT supervisory divisions undertook a joint thematic supervisory review of this sub-sector to analyse and assess the effectiveness of the governance, risk and compliance frameworks within these administration firms for managing both ML/TF and prudential risks. Whilst individual findings were raised with the relevant firm, anonymised findings together with examples of good and poor practice were published in a report on the thematic review to assist the whole industry in its development of effective AML/CFT controls. The Commission monitors the external use of its website and it recorded 801 online views of the report in the first two weeks after its publication. The thematic exercise also provided information for the Commission to use in its presentations to industry.

184. The AML/CFT supervisory division has also undertaken AML/CFT themed reviews on the provision of AML/CFT training within the industry.

Ireland

Central Bank of Ireland's AML/CFT Supervision of the Funds Sector

185. There are approximately 7,000 funds authorised by the Central Bank of Ireland (the Central Bank). Each fund is required to appoint an Irish authorised Fund Service Providers (FSPs) to administer the fund. The FSP is often the point of contact in the customer relationship between the investor and the fund. When appointing an FSP, the fund will typically contract the FSP to provide certain AML/CFT services to the fund; however this does not absolve the fund from its own obligations.

186. In order to utilise its supervisory resources in the most effective manner and maximise supervisory coverage, the Central Bank's AML/CFT supervisory strategy is to supervise funds through supervisory engagement of FSPs. Five FSPs account for almost 85% of the total amount of assets of Irish authorised funds. While the Central Bank's minimum AML/CFT supervisory engagement model provides for on-site inspections of FSPs at least once every five years, these five FSPs are subject to an on-site inspection at least once every three years. In addition, these five FSPs are also subject to an AML/CFT review meeting at least once every two years and are required to complete an online AML/CFT return at least once every two years. This supervision strategy enables the Central Bank to regularly assess the AML/CFT control framework of both the funds and the FSPs, through sample testing, interviews and reviews of policies and procedures. The Central Bank has also has a dedicated relationship manager for the funds industry to deal promptly and effectively with any issues that may arise on occasion.

187. The Central Bank's supervisory engagements are complemented by an AML/CFT communications and outreach programme to the funds sector. This includes presentations by the Central Bank at a number of industry events each year, as well as the publication of bulletins and reports that set out in aggregate and anonymised form the findings from the Central Bank's supervisory engagements. The publications also state the Central Bank's expectations around AML/CFT compliance.

Hong Kong, China

Securities and Futures Commission's AML/CFT Supervision Securities Sector

188. The Securities and Futures Commission (the "SFC") of Hong Kong conducts on-site inspections and employs various off-site monitoring tools to supervise licensed firms' compliance with AML/CTF requirements and monitor their ML/TF risks. The frequency, intensity and scope of the inspection and off-site monitoring carried out on an individual firm vary with, and are proportionate to, the risk level of the firm assessed based on a number of risk and impact factors. The SFC also conducts enforcement actions in relation to suspected breaches of AML/CFT legal and regulatory requirements and related internal control failures, for which a range of remedial measures and dissuasive sanctions may be imposed.

189. The SFC places emphasis on senior management responsibility (Manager-In-Charge or MIC), with detailed expectations regarding compliance and control functions that are relevant to MICs for AML/CFT as set out in the SFC's AML/CFT guidelines. If an MIC fails to ensure that the licensed firm complies with AML/CFT

requirements, the failure may render the MIC liable to disciplinary sanctions (e.g. pecuniary fine and reprimand) imposed by the SFC. SFC's investigations will, whenever appropriate, focus on the culpability of individuals with oversight of the AML/CFT function and other core functions.

190. The SFC places emphasis on sharing its supervisory observations, and signalling to all licensed firms its regulatory priorities and the focuses of compliance inspections. The goal is to promote and assist the efforts of licensed firms and their senior management in discharging their responsibilities. To this end, the SFC has initiatives in place to alert the industry of different areas of compliance concern from time to time. This includes communicating supervisory findings to the industry via circulars and seminars.

191. The SFC also provides transparency of its enforcement actions by issuing press releases on its enforcement actions. In disciplinary cases, a copy of the Statement of Disciplinary Action summarising the material facts and conclusion of a disciplinary action is available on the SFC's website.

Luxembourg

192. Luxembourg Investment funds and their Luxembourg Investment Fund Managers as well as service providers established in Luxembourg are obliged entities under the applicable AML/CFT framework. The CSSF is the competent supervisory authority for all the entities falling under its remit. The Luxembourg investment fund industry is notably characterised by its cross-border distribution nature. Thus, subscription into Luxembourg-based funds is often performed through intermediaries acting on behalf of their own customers in other countries.

193. Consequently, the supervisory approach of the CSSF has been tailored to take into account this operational reality and it requires the investment funds, their Investment Fund Managers, or where applicable, any proxy, to perform AML/CFT enhanced due diligence on those intermediaries.

194. The AML/CFT supervisory approach of the CSSF takes into account the roles and responsibilities of the several parties involved in the investment fund industry. The supervisory life cycle starts with AML/CFT controls performed at licensing, continuing on an ongoing basis through off-site and on-site supervisory actions. For instance, dedicated on-site inspections are performed at the level of the Investment Fund Managers as they often decide on the channels and countries of distribution of the funds. These on-site inspections are complemented by supervisory actions on-site and off-site at the level of Luxembourg service providers such as at registrar and transfer agents and at the custodian/depositary bank of the funds.

195. The CSSF's AML/CFT Risk Based Supervisory ("RBS") approach to the sector is subject to a continuous improvement. Lastly, through the addition of two new components. First, an Automatic Score, calculated from a dedicated AML/CFT online questionnaire filled in by investment fund managers, registrar and transfer agents and depositary banks. Second, through an internal Expert Judgement Score. The combination of both sources aims at providing a final score, taking into account several risk criteria and respective mitigation measures implemented by the obliged entities. The RBS is a dynamic process in that the score of an entity may be changed at any point of time, if affected by new information or trigger events. This enables the CSSF to adapt its supervisory actions to emerging threats.

196. Furthermore, the CSSF maintains a database of main findings identified during its AML/CFT onsite inspections and shares them with the private sector on an anonymous basis through its annual reports. Other interactions with the private sector take place notably via regular meetings with obliged entities, events with professional associations, and the publication of AML/CFT guidance through CSSF circulars. In addition, the CSSF makes contact with other competent authorities within Luxembourg and abroad in order to discuss AML/CFT matters and to exchange information through Memoranda of Understanding.

Mexico

National Banking and Securities Commission's AML/CFT Supervision of Securities Sector and guidance provided for the implementation of the RBA

197. The National Banking and Securities Commission's (the "CNBV") of Mexico is responsible for the licencing and registration, prudential and AML/CFT supervision for the brokerage firms, investment funds and investment advisors. CNBV supervises other financial institutions as well, such as banks, savings and loan companies, money transmitters, among others.

198. The AML/CFT supervision consists of on-site inspections and off-site monitoring in order to verify the securities providers and intermediaries' compliance with AML/CFT requirements and monitor their ML/TF risks. The RBA on supervision is applied at different levels and stages of the supervision process. Off-site monitoring activities are carried out for all supervised entities. However, depending on their ML/TF level of risk, additional supervision measures are taken.

199. CNBV has a methodology that measures the ML/TF risks for all supervised entities considering the inherent risk for both ML/TF (two separate measures are performed, and the results are combined to obtain the entities ML/TF inherent risk), taking into account information provided by the entities themselves, the prudential supervisors and other authorities, such as the FIU, other supervisors and the federal law enforcement agency (PGR). The results of previous supervision actions are considered as the evaluation of their mitigating measures, which may reduce the inherent risk. Other factors are considered as risk intensifiers that may increase the inherent risk, such as the non-compliance with periodic obligations, findings indicated in the annual audit report, low quality of the STRs, obtaining at the end the residual risk for each entity.

200. The annual on-site visiting program takes into account the results from the aforementioned methodology and other additional factors, such as the systemic relevance and those related to special concerns from the AML/CFT and prudential supervision. With the resulting ratings, it is decided which entities will have stronger supervisory actions, starting with the on-site visits from the AML/CFT supervisors, on-site visits from the prudential supervisors including some specific AML/CFT topics, and continuing with other off-site additional monitoring programs.

201. Once the annual on-site visiting program is defined under a RBA, for each on-site visit it is necessary to identify the mitigating measures that are going to be revised considering as well a RBA. A document called "entity's diagnostic" is executed at least one month in advance from the on-site visit including all the CNBV's available information as well as information from the FIU, and considering all the gathered elements, the visit strategy (intensity and scope) is defined. Additionally, during the

on-site visit the selection of the entity's clients for a deeper revision is made based on the risk they represent for the entity itself, meaning another way to implement the RBA in the supervision process.

202. In 2017, the AML/CFT legal provisions in Mexico were modified in order to include as an obligation the design, implementation and assessment of an internal RBA for all entities supervised by the CNBV. In order to give guidance on the implementation of this new obligation, the CNBV has put into practice several actions:

- Issue a guideline in order to explain in a more detailed manner what is expressed in the legal provisions in terms of how to accomplish the design, implementation and assessment stages for their internal RBA.
- Organize forums by supervised sector in order to give some examples of how to apply the RBA given each sector's specific characteristics, including, products, type of clients, distribution channels and geographic areas of operation.
- Publish a video-tutorial with the most important information from the forums in the previous bullet, in order to have a wider range of reach among all the supervised entities, especially for those who were unable to assist to those forums.
- Carry out workshops where the supervisor's expectations regarding this new obligation are clarified and to perform some exercises for the design of the RBA methodology and supervisor's feedback regarding these exercises.
- Release the supervisor's on-site visit guidelines for all the supervised entities to make more transparent the supervision process and the entities could be aware of the supervisor's expectations in terms of compliance of all their AML/CFT obligations, especially regarding this new one.

USA

203. The SEC conducts examinations of SEC registrants using a risk‐based approach. A firm may be selected for examination for any number of reasons including, but not limited to, a tip, referral, or complaint; the firm's risk profile; or in connection with a review of a particular compliance risk area. The reason why firms have been selected for examination is non-public information, and typically will not be shared with the firm under examination. ML risks, among others, may be considered in developing a firm's risk profile and the scope of each examination.

204. During examinations, SEC examiners seek to determine whether the entity being examined is, among other things, conducting its activities in accordance with the federal securities laws and the rules thereunder, the bank secrecy act as applicable and the rules of self-regulatory organizations (SRO).

205. Over the past several years, the SEC exam group has recruited industry experts to enhance the national examination program's technology and data analytics and thus advance its risk-based examination approach. The examination staff is increasingly incorporating into its AML reviews such enhanced technology and tools to review vast amounts of data so that the staff can identify suspicious activity from the source trade data rather than relying on the broker-dealer's surveillance reports. The staff can compare the activity it identifies to activity identified by the firm, to test

for weaknesses in a firm's monitoring and reporting of suspicious activity, including assessing the reasonableness of the parameters set by firm. Thus, rather than a simple verification of an AML program's existence, examiners can perform nuanced assessments of the quality of the program.

206. FINRA, the SRO for US broker-dealers, has supervisory duties over approximately 3 700 brokerage firms and 6 29 000 registered securities representatives and conducts the majority of broker-dealer AML examinations. FINRA also examines its member firms on a routine basis for compliance with its rules (including its own AML rule) and the federal securities laws, related to both sales practices and financial operations in its Firm Examination Program. The Firm Examination Program is risk-based, and the frequency of an examination of a member firm is determined through a risk assessment. Thus, a member firm may be examined pursuant to a one or four-year cycle, with higher risk and higher impact firms being examined each year, with a frequency no less than every four years for all firms. AML may be considered for inclusion based on an assessment of risk at that particular firm. When AML is selected for review on a Firm Examination, reviews for particular areas of AML compliance can be narrowly or broadly focused, depending on the specific risks posed by the firm.

207. Firms also may be examined for compliance with certain AML rules and regulations through a Cause Examination or as part of a Sweep Examination, which may encompass multiple firms. Cause Examinations are initiated through terminations for cause, tips, referrals from other regulatory agencies, complaints or by identifying high-risk activity through data analysis. Ongoing risk monitoring is conducted on all FINRA member firms, which includes reviews for compliance with AML-related rules and regulations.

208. In addition, in 2013, FINRA established an AML Investigative Unit to conduct examinations where highly complex or novel money-laundering and AML compliance program concerns exist. In addition to conducting examinations, these AML regulatory specialists provide technical assistance to other examiners and constantly pursue an expansion of knowledge and professional development in the AML arena. The AML Investigative Unit also provides training and education to FINRA staff members and members of the brokerage industry. FINRA has found that this approach leads to better-informed examiners and higher-quality exams.

ANNEX B. SUSPICIOUS ACTIVITY INDICATORS IN RELATION TO SECURITIES

This Annex provides examples of suspicious indicators in relation to securities, which may trigger filing of STRs and/or require additional CDD measures, including further investigation and ongoing monitoring, before a decision on filing is made by the securities provider. This is not an exhaustive list; each element may not be relevant in all countries, for all securities providers, for different customer relationships (retail vs. institutional), or for all business activities described in this document.

I. Product/Customer transactions suspicious activity indicators

1. Transactions do not have apparent economic rationale.
2. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/reporting thresholds.
3. A concentration ratio of transactions relating to a particular and/or higher risk jurisdiction that is notably higher than what is to be expected considering its normal patterns of trading of a customer.
4. Frequent trades resulting in losses for which the customer appears to have no concern.
5. Sudden spike in transaction volumes, which deviates from previous transactional activity absent any commercial rationale or related corporate action event.
6. Mirror trades or transactions involving securities used for currency conversion for illegitimate or no apparent business purposes.
7. A pattern of securities transactions indicating the customer is using securities trades to engage in currency conversion. Examples of securities that can be used in this manner include dual-currency bonds, American Depositary Receipts (ADRs) and foreign ordinary shares traded in the Over-the-Counter Market.
8. Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.
9. Trading or journaling in the same security or securities between numerous accounts controlled by the same people (e.g. potential wash sales and/or directed trading).
10. Two or more unrelated accounts at the securities firm trade an illiquid or low-priced security suddenly and simultaneously.
11. Purchase of a security does not correspond to the customer's investment profile or history of transactions (e.g. the customer may never have invested in equity securities or may have never invested in a given industry) and there is no reasonable business explanation for the change.
12. Transactions that suggest the customer is acting on behalf of third parties with no apparent business or lawful purpose.

13. Funds deposited for purchase of a long-term investment followed shortly by a customer request to liquidate the position and transfer the proceeds out of the account.

II. Distribution channel suspicious activity indicators

1. Intermediaries whose transaction volume is inconsistent with past transaction volume absent any commercial rationale or related corporate action event.
2. A transaction pattern indicating a value of transactions just beneath any applicable reporting threshold.
3. Unclear or complex distribution channels that might limit the ability of the investment fund or asset management company to monitor the transactions (e.g. use of a large number of sub-distributors for distributions in third countries)

III. Selected indicators of suspicious trading or market manipulation

1. Making a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security, which may be suggestive of potential insider trading or market manipulation.
2. A request is made to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
3. Accumulation of stock in small increments throughout the trading day to increase price.
4. Engaging in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low-priced securities.
5. Marking the closing price of a security.
6. Front-running suspected with regard to other pending customer orders.

IV. Suspicious indicators associated with CDD and interactions with customers

1. Customer has no discernible reason for using the securities provider's services or the firm's location (e.g., customer lacks ties to the local community or has gone out of the way to use the firm).
2. Customer's legal or mailing address is associated with other, apparently unrelated, accounts.

3. Locations of address of the customer, bank or financial institution seem unconnected to the customer and little or no explanation can be given by the customer for the disparate addresses.
4. Customer is a trust, shell company, or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
5. Customer is a legal person having issued bearer securities for a large part of its capital.
6. Customer is publicly known to have criminal, civil or regulatory proceedings against it for corruption, misuse of public funds, other financial crimes or regulatory non-compliance, or is known to associate with such persons. Sources for this information include news items or Internet searches.
7. Customer's background is questionable or differs from expectations based on business activities.
8. Customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
9. Customer's account information reflects liquid and total net worth that does not support substantial account activity.
10. Customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
11. Non-profit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
12. Customer is reluctant to provide information in relation to its identity and/or transactions.
13. Customer is reluctant to provide information needed to file reports to proceed with the transaction or requests an inordinate amount of secrecy around a transaction.
14. Customer exhibits unusual concern with the firm's compliance with government reporting requirements, the firm's systems or the firm's AML/CFT policies and controls.
15. Customer tries to persuade an employee not to file required reports or not to maintain the firm's required records.
16. Law enforcement or regulators have issued subpoenas and/or freeze letters regarding a customer and/or account at the securities firm.
17. Customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.
18. Customer does not exhibit a concern with the cost of transactions or fees (e.g. surrender fees, higher than necessary commissions) or of investment losses.

V. Suspicious indicators in deposits of securities, particularly low-priced securities; these can often be indicators of low-priced securities fraud, distribution of an unregistered offering, or market manipulation schemes

1. Customer opens a new account and deposits physical certificates or delivers in shares electronically representing a large block of thinly traded or low-priced securities.
2. Customer has a pattern of depositing physical shares certificates or a pattern of delivering in shares electronically, immediately selling the shares and then wiring or otherwise transferring out the proceeds of the resale(s).
3. A sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.
4. The lack of a restrictive legend on shares physically or electronically deposited seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock, and/or the volume of shares trading.
5. Customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.
6. Customer's explanation of how the customer acquired the securities does not make sense or changes.
7. Customer deposits physical securities or delivers in shares electronically and requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

VI. Movement of funds or securities

1. The securities account is used for payments or outgoing wire transfers with little or no securities activities (i.e. account appears to be used as a depository account or a conduit for transfers with no reasonable business explanation for such).
2. Funds are transferred to financial or depository institutions other than those from where the funds were initially received, specifically when different countries are involved.
3. Customer "structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
4. Customer engages in excessive journal entries of funds or securities between related or unrelated accounts without any apparent business purpose.

5. Payment by third party check or money transfer from a source that has no apparent connection to the customer.
6. Customer uses a personal/individual account for business purposes.
7. Payment to a third party to which the customer has no apparent connection.
8. Frequent transactions involving round or whole dollar amounts.
9. The customer requests that certain payments be routed through nostro[33] or correspondent accounts held by the financial intermediary instead of its own accounts.
10. Funds transferred into an account that are subsequently transferred out of the account in the same or nearly the same amounts, especially when origin and destination locations are high-risk jurisdictions.
11. A dormant account suddenly becomes active without a plausible explanation (e.g. large amounts are suddenly wired out).
12. Frequent domestic and international automated teller or cash machine activity out of character with the customer's expected activity.
13. Many small, incoming wire transfers or deposits made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history. This may be an indicator of, for example, a Ponzi scheme.
14. Wire transfer activity, when viewed over a period of time, reveal suspicious or unusual patterns.
15. Transfers of funds or securities are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
16. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
17. Customer transfers/receives funds to/from persons involved in criminal or suspicious activities (as per the information available).
18. In/out transactions for substantial amounts on a short-term basis.
19. Receipt of unexplained amounts, followed, shortly thereafter, by a request to return amounts.
20. Frequent transfers of securities' ownership.
21. Use of bearer securities with physical delivery.
22. Frequent change of bank account details or information for redemption proceeds, in particular when followed by redemption requests.
23. The usage of brokerage accounts as long term depository accounts for funds.

[33] Nostro accounts are accounts that a financial institution holds in a foreign currency in another bank, typically in order to facilitate foreign exchange transactions.

FATF

GUIDANCE FOR A RISK-BASED APPROACH
SECURTIES SECTOR

The risk-based approach (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

This Guidance focuses on RBA for the securities sector and includes an annex on suspicious activity indicators in relation to the securities sector. It takes into account the experience gained by public authorities and the private sector over the years in applying a RBA.

This Guidance should be read in conjunction with the FATF Report: Money Laundering and Terrorist Financing in the Securities Sector (October 2009), which outlines vulnerabilities in the sector.

www.fatf-gafi.org | October 2018

Appendix Z:

APG, *APG Typology Report on Trade Based Money Laundering*
(Paris: FATF, 2012)

Asia/Pacific Group on Money Laundering

ASIA/PACIFIC GROUP ON MONEY LAUNDERING

APG Typology Report on Trade Based Money Laundering

Adopted by APG Members at the 15th Annual Meeting

20 July 2012

.

(Telephone: +612 9277 0600 Fax: +612 9277 0606 Email: mail@apgml.org)

Table of Contents

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

1. Trade Based Money Laundering (TBML) was recognized by the Financial Action Task Force (FATF) in its landmark 2006 study as one of the three main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy. This method of money laundering (ML) is based upon abuse of trade transactions and their financing. The 2006 FATF Study highlighted the increasing attractiveness of TBML as a method for laundering funds, as controls on laundering of funds through misuse of the financial system (both formal and alternate) and through physical movement of cash (cash smuggling) become tighter.

2. In recent years APG members have continued to highlight vulnerabilities for TBML, but very few cases investigations or prosecutions appear to have been undertaken in the Asia/Pacific region and very few case studies had been shared.

3. The APG's TBML study aims to build on the existing studies, in particular those of the FATF, in order to study the extent of the prevalence of TBML and highlight current methods, techniques and modus operandi for TBML as well as to identify 'red flags' to detect and respond to TBML.

4. In determining the magnitude of TBML, the study considered why so few cases of TBML have been detected since the FATF's 2006 study. The Paper has sought to clarify and furnish explanations for terms and processes of 'trade finance' which are comprehensible to Money Laundering (ML) investigators.

5. This Paper has focused on TBML occurring in the course of international trade in goods. The study does not include in its scope capital flight, tax evasion, trade in services and domestic trade. The features of the dynamic environment that distinguish TBML from other forms of ML are its occurrence through intermingling of the trade sector with the trade finance sector in cross- border transactions. The foreign exchange market and the long supply chain make international trade particularly vulnerable to TBML.

6. The study included circulation of a questionnaire to APG and FATF members seeking statistically significant indicators. The Paper sets out a number of Case Studies to illustrate trends of TBML. Simplified explanations of the terms and processes of trade finance have been attempted through interaction with the private sector. A brief review of the literature on the subject generated by the FATF, FSRBs and other authors has been made.

7. There is a growing concern on how the rapid growth in the global economy has made international trade an increasingly attractive avenue to move illicit funds through financial transactions associated with the trade in goods and services. TBML is a complex phenomenon since its constituent elements cut across not only sectoral boundaries but also national borders. The dynamic environment of international trade allows TBML to take multiple forms.

KEY FINDINGS

8. Statistical analysis has been conducted on the basis of responses received on 64 questions from 19 jurisdictions and 1 organisation.

9. Few TBML cases have been reported. The extent of TBML in the region was not able to be accurately estimated in this study. However, during the course of the study it has become evident that TBML is a problem for many of the participating jurisdictions and has serious significance as an avenue to launder proceeds of crime.

10. There is lack of awareness and training on TBML among the jurisdictions. Training for those responsible for detection and investigation of TBML as well as to those who collect trade data and handle trade finance is critical to raise their awareness about TBML and build capacity to identify TBML.

11. Most jurisdictions do not distinguish TBML from other forms of ML. A major obstacle in devising strategies to tackle TBML has been the lack of reliable statistics relating to it. There is presently no standardization with regard to the practice of collection and maintenance of data on TBML. Trade related data is collected to serve purposes other than those of detecting TBML.

12. The lack of TBML investigators and absence of systems capable of cross-referencing trade and trade finance data are significant limitations. In most of the reporting jurisdictions customs authorities or equivalent collect and manage trade data but do not have the authority to conduct ML investigation.

13. Over 50% of the reporting jurisdictions indicate referrals from other agencies which trigger TBML investigations. Again, over 50% of the reporting jurisdictions seek information from international counterparts. However there are impediments in domestic coordination and international cooperation among the competent authorities. The main impediments which have been identified are requirement of maintaining confidentiality, delays in response and conveying of information with restrictions.

14. Reporting jurisdictions have listed a large number of patterns and red flags which this Paper has categorised in five broad groups viz. Trade Finance, Jurisdictions, Goods, Corporate Structure and Predicate Offences. The last four categories have been dealt with in the past papers under the broad category of trade. With regard to trade finance the important red flags relate to methods of payment and letters of credit. Existence of duty free zones and prevalence of high duty structure can make jurisdictions sensitive to TBML. The discrepancy about description, quality, quantity and value of the goods which are traded can be important red flags. Front or shell companies are often used as corporate structures to facilitate TBML. Tax evasion and customs offences are important predicate offences for TBML.

15. The trade finance products identified in this study reveal a menu of choices that are available to genuine traders to facilitate trade. Exporters and importers enter into an agreement to trade more often than not by way of cash payment or through some more

complex form of trade financing. Such trade finance products include bills of exchange, counter trade, letters of credit and open account facilities. A range of open account facilities may encompass factoring, forfaiting and other forms of credit. While the trade finance products were innovated to reduce trade transaction costs, their accessibility have also made them vulnerable to TBML abuse. Thus the trade in commodity has become as good as means of movement of cash and of transfer of funds to indulge in laundering.

16. Financial sector representatives indicate a trend toward the use of open account financing in trade. This has implications for detecting the abuse of trade finance for ML.

17. The case studies included in the Paper, besides identifying the elements of trade that facilitate TBML, also bring out the mechanisms of trade finance used in TBML. One case study highlights the financing of different segments of trade through diverse mechanisms of trade finance that can introduce risks in the trade transactions which are difficult to assess by financial institutions. The mechanisms of financing trade through factoring and through disbursement of trade credit to overseas suppliers are fraught with risks for financial institutions unless due diligence is exercised over the overseas trading partner, are brought out in another case study. Another case study shows how the operations of 'exchange houses' owned and controlled by criminals coupled with 'compromised' working of a bank make trade finance mechanisms means for indulging in TBML. There are other case studies which demonstrate the use of alternative remittance systems and of corporate structures to facilitate TBML. A final case study shows multiple forms of international trade and various mechanisms of trade finance which give inherent flexibility to criminals to adopt those forms and types which suit the demands of a situation.

18. The 2006 FATF Paper on TBML focused on trade based techniques used in TBML, which have been mentioned as over/under invoicing of goods, multiple invoicing of goods, over/under shipments of goods and false description of goods. These techniques need to combine with techniques which abuse trade finance mechanism, for TBML to occur. Four of these techniques have been identified in this paper as cash inflow based payment, third party payment, segmental modes of payment and alternative remittance payment.

POLICY OBSERVATIONS

19. Any strategy to prevent and combat TBML needs to be based on dismantling TBML structures while allowing genuine trade to occur unfettered. An emphasis on inter-agency coordination and international cooperation, needs to be adopted by policy-makers. A comprehensive strategy which takes into account sectoral peculiarities, agency specialization and jurisdictional frameworks can only address the challenges in tackling TBML.

20. There is a need to have common formatting for recording and maintaining trade-relevant statistics so that data sets can be analysed to identify trends related to TBML. Cross-referencing of data relating to trade and trade finance can be the starting point for adopting a risk based approach to identifying TBML. There is an acute need to correlate trade data

with the foreign exchange data to detect TBML and identify cases where value is in the form of goods without corresponding outgo of foreign exchange as payment.

21. Multiple agencies are involved either directly or indirectly in combating TBML. Levels of specialization in mandated roles to combat TBML varies. However, the strategy to prevent and combat TBML requires expertise created through the combination of all such authorities. One way-forward to combine the respective competencies of relevant authorities for combating TBML is to form domestic task-forces. Task-forces focused on TBML investigations will need to have the ability to utilize the expertise of each agency without compromising its functional skills.

22. There is an urgent need to strengthen the existing bilateral arrangements like Trade Transparency Units (TTUs) and to build multilateral mechanisms for international cooperation. The bilateral arrangements must ensure prompt exchange of information with regular follow-ups which should result in more efficient delivery. The multilateral mechanisms may entail equal commitment of all trading jurisdictions for coordination in matters relating to TBML.

23. TBML focused training is an absolute necessity for the anti-TBML strategy to succeed. Customs, ML investigating LEA, FIU, Tax Authorities and Regulators have all identified a pressing need for more focused training so that their personnel can have an adequate knowledge base to detect, prevent and combat TBML. The sharper focus on TBML in existing training programs can be brought about by incorporating specific topics which relate to TBML. The case studies, the red flags and typology papers on TBML may be disseminated during such programs. As trade essentially involves multiple jurisdictions, there is a need for Law Enforcement Officers to understand the legal and procedural aspects of other jurisdictions. Training should be aimed at making use of trade data analysis as well as cross referencing trade data with trade finance data and understanding any useful tools developed to identify trade anomalies which may lead to investigation and prosecution of TBML cases. Inter-linkages of tax frauds and customs violations with TBML also need to be explained.

CHAPTER I - SCOPE & COVERAGE

INTRODUCTION

24. The Asia/Pacific Group on Money Laundering (APG) produces regional typologies studies of money laundering (ML) and terrorist financing (TF) in the Asia/Pacific region. This is done to share information and support a better understanding of ML and TF methods, techniques and trends in the region.

25. Typologies of ML and TF allow Governments and the private sector to understand the nature of the ML and TF environment and design effective AML/CFT strategies to address threats. Typologies help APG members to implement effective strategies to investigate and prosecute ML and TF, as well as design and implement effective preventative measures.

26. Trade Based Money Laundering (TBML) has been recognized by the Financial Action Task Force (FATF) in its landmark study published in 2006, as one of the three main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy. This method of ML is based upon abuse of trade transactions and their financing. The FATF Study 2006 highlighted the increasing attractiveness of TBML as a method for laundering funds, compared with misuse of the financial system (both formal and alternate) and through physical movement of cash (cash smuggling).

27. The revision of FATF standards undertaken in 2003 entailed stricter controls on the financial system and on cash couriers, which may have had an unintended consequence of leaving the trade finance sector more vulnerable to ML and TF. The increasing volume, speed and value of global trade and the complexities inherent in trade transactions and in its financing arrangements coupled with limited awareness and understanding of how such trade can be abused, have made TBML an important avenue for moving illicit funds.

AIMS OF THE STUDY

28. The APG Annual Meeting in Kochi, India in July 2011 resolved to take-up further study on TBML as an APG Typology Study. The Study commenced with the following aims:

i) to build on the existing studies and in particular that of FATF published in 2006;
ii) to study the extent of the prevalence of TBML;
iii) to highlight current methods, techniques and modus operandi for TBML so as to short list 'red flags' to detect and respond to TBML; and
iv) to clarify and furnish explanations for terms and processes of 'trade finance' which are comprehensible to ML investigators.

SCOPE OF THE STUDY

29. It is useful to consider the fundamental elements of trade in goods that this study will consider when discussing TBML. Conceptually, trade can be broken into various elements which may be overlapping:

- arrangements to trade goods
- financial steps to facilitate the trade (financing, insurance, etc.)
- movement of goods
- reconciliation or settlement of financial accounts

30. TBML was defined by the FATF in 2006 as 'the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.' The FATF Paper on Best Practices (2008) broadened the definition by stating, "TBML and terrorist financing (TBML/FT) refer to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origin or finance their activities." Such broadening of the definition, allows for illegal activities such as terrorist financing to be covered within the scope of TBML.

31. The FATF Study of 2006 excludes the coverage of the movement of money for tax avoidance, evasion and capital flight, on the grounds that such movement of funds usually involves transfer of legitimately earned funds across borders while TBML involves the 'proceeds of' or 'instruments of' crime. However, the FATF 2008, Paper on Best Practices does cover within the definition of TBML, the movement of licit funds for the purpose of illegal activities such as terrorist financing. This broadening of the definition, coupled with the intermingling of licit and illicit funds imply that the abuse of capital flight and the movement of funds for tax avoidance / evasion are within the scope of TBML.

32. This paper excludes consideration of domestic trade in its study of TBML. While the FATF definitions of TBML do not exclude domestic trade from their ambit, the framework chosen by this and other papers leaves domestic trade out of scope. This is not to deny that TBML can occur through domestic trade, however given that domestic trade is less regulated and large in terms of number of transactions, the time resource available to compile this Paper and the amount of 'noise' that exists in the domestic market does not allow for its coverage.

33. Whilst the definition of TBML being considered includes international trade in 'services' which has also been addressed in previous FATF Papers, trade in services and other intangibles is also out of scope of this Paper. The lack of standardization of the definition of 'services' and difficulties in estimating the 'fair value' of their provision, will not allow for its meaningful treatment in the present study. The project team believes that separate studies devoted to trade in services and other intangibles, keeping their peculiarities in view, are called for. The implications of the capital flight and the movement of funds for tax evasion for TBML need to be examined separately. Mechanisms like transfer pricing are still largely in the domain of taxation. Therefore the present Paper while adopting the

definition of TBML given by the Best Practices Paper 2008 of FATF does not include in its scope capital flight, tax evasion, trade in services and domestic trade.

34. The rapid expansion of global trade has increased the possibilities for TBML. Trade is the 'engine of growth' and ensures optimal use of resources. Thus the need to have a 'free and fair' trade regime has been emphasized. The dilemma which is faced by policy makers is the requirement to balance the needs of a free, fair and predictable trade regime with the needs for regulation of trade so as to prevent its abuse. Total Global Merchandise Trade stood in 2010 at US $ 30.729 Trillion {US $ 15.237 Trillion exports + US $ 15.492 Trillion imports}1 which indicates the potential for absorption and movement of funds of criminal origin through international trade and the need to study TBML.

35. One common thread running through studies of the FATF, of FATF-style regional bodies (FSRBs) such as the APG, and other literature is acknowledgement of the lack of awareness of TBML. Such studies have consistently highlighted difficulties in detecting TBML cases. A lack of understanding of those features of TBML that are distinct from other forms of ML is viewed as one reason for a lack of TBML cases. While acknowledging the commonalities between TBML and other forms of ML, attempts have been made in this Paper to identify a few distinguishing features of TBML. Recognition of such features may help develop better 'red flags', support increased awareness and lead to more detections.

36. Distinguishing features of the dynamic environment for TBML include:

a) TBML using international trade occurs over more than one jurisdiction, while other forms of ML may be only of a singular jurisdiction. **Cross border transactions** provide opportunities to take advantage of differences in legal systems of various jurisdictions. A jurisdiction may have less restrictive Customs checks (Free Trade Zones) and less stringent AML set-up than trading partner. The high volume, regularity and speed of international trade increase vulnerabilities.

b) TBML necessarily requires **intermingling of the trade sector with the finance sector.** Criminals take advantage of vulnerabilities of both the sectors. Merely having an AML regime for the finance sector becomes inadequate unless such a regime effectively covers the corresponding trade sector. Moreover, cross-referencing of trade-data, with that of trade finance becomes essential when investigating TBML.

c) International trade is denominated in terms of internationally acceptable currencies. Trade becomes exposed to the **vulnerabilities of the foreign exchange market.** The conversion of currency at market determined exchange rates enhance the scope for criminals to launder the proceeds of or instruments of crime.

d) The **long supply chain** necessary for international trade make the trade more vulnerable to TBML. This chain of manufacturer, trader, consigner, consignee, notifying party, financier,

[1] Source:(http://stat.wto.org/StatisticalProgram/WSDBViewData.aspx?Language=E

shipper, insurer and freight forwarder broaden the scope for abuse of the system by the criminals because of all the vulnerabilities that exist.

METHODOLOGY

37. The Methodology which has been adopted in this Paper has the following important elements:-

a) A Questionnaire was prepared and circulated among the jurisdictions for completion by relevant agencies (see Annex B). A statistical profile was drawn from responses to the questionnaire. However responses were received from only limited number of jurisdictions which has resulted in making the size of the sample small. Results based on a sample of small size may not be regarded as statistically significant. Nevertheless, the statistical responses have brought the project team to the conclusion that there are commonalities amongst various jurisdictions with regard to the challenges in understanding and tackling TBML.

b) Case studies were sought as part of the questionnaire. APG members' Typology Status Reports from previous year were examined for cases and other reference materials. A limited number of case studies were reported. Those case studies have been used to appreciate the recent trends of the modus-operandi and techniques adopted for TBML as well as to develop 'red flags'.

c) Terms and 'processes of trade finance' have been examined and simplified explanations have been attempted so as to make these comprehensible for investigators. This is considered an important feature of this study as TBML is a complex subject and lawmakers and investigators alike find it difficult to understand the terms and processes of international trade and its financing arrangements. In this regard the Project Team interacted with the private sector.

d) A brief review of some of the literature on the subject has been made. Existing studies on the subject made by the FATF, FSRBs and other organizations have been examined in an attempt to take this body of research forward.

FRAMEWORK

38. Chapter II of this paper considers issues categorized into four areas of concern.

(i) What is the extent of TBML in specific jurisdictions, regions and across the globe?
(ii) What should be the roles, responsibilities of investigating agencies and other allied agencies to tackle TBML?
(iii) What are the best practices (preventative measures) to effectively deal with TBML? and
(iv) What are those features of TBML which can make it possible to discern it from other forms of ML?

39. The inferences drawn from the statistical analysis of the responses received to the Questionnaire attempt to provide answers to these concerns. The statistical analysis made in Chapter-II has also looked at the extent of the prevalence of TBML.

40. Chapter III of this Paper aims to develop a simplified explanation of terms and processes of trade finance so as to make these comprehensible for investigators. Improved understanding of concepts, terms and processes of trade finance should assist AML investigators to detect TBML cases by cross-referencing the leads from trade transactions with those of trade finance.

41. Chapter IV of this Paper illustrates the techniques of TBML through case studies. The Chapter elucidates how the abuse of trade system combines with that of trade finance for TBML to occur. Techniques of Trade Finance abuse have been identified. Chapter-V of this Paper is devoted to drawing of conclusions and suggesting way forward.

REVIEW OF EXISTING STUDIES

42. In order to better understand the complex subject of TBML, this Paper seeks to review the existing literature on TBML. This includes studies by published by the FATF, FATF-style regional bodies (FSRBs) and a range of studies from intergovernmental organisations, jurisdictions, the academic sector and other bodies.

Financial Action Task Force (FATF) Studies

Trade Based Money Laundering (2006)[2]

43. The FATF TBML study of 2006 set out a number of key findings and recommendations:-

a) TBML is a complex and increasingly important channel of ML.

b) Techniques of TBML adopted by criminals vary from simple to complex. Simple techniques include ‘over/under invoicing’ of goods, multiple invoicing of goods, ‘over/under shipments’ of goods and falsely described goods. Combinations of several simple techniques have been regarded as complex.

c) Analysis of trade data and its international sharing are useful tools for identifying trade anomalies and detection of TBML. Since international trade leaves behind documentation, the anomalies noticed during data analysis may lead the investigator to documentary evidence. Lack of structured and regular exchange of information related to trade and trade finance among relevant agencies.

d) The lack of resources and training further constrain Customs, LEA, FIU and Tax Authorities to develop effective AML methodologies against TBML.

[2] http://www.fatf-gafi.org/dataoecd/60/25/37038272.pdf

44. The FATF 2006 study identified and recommended three main areas to be focused by Authorities to increase effectiveness in combating TBML:

i) Building better awareness among the agencies responsible for detection, investigation and prosecution of offenders involved in TBML. These agencies have expressed strong need for training.

ii) Strengthening current measures so that there is extensive use of the available material in the form of case studies and red flag indicators of TBML. The aspects of effective domestic cooperation and sharing of information among Law Enforcement Agencies and Regulators have also been impressed upon.

iii) Improving international cooperation so that it can act as a trigger for detection of TBML cases. In this regard the setting up of physical and legal infrastructure has been emphasized.

Best Practices Paper on Trade Based Money Laundering (2008)[3]

45. The FATF Best Practices Paper on TBML (2008) has provided important guidelines for detection and investigation of cases of TBML. The objective of the Best Practices Paper was to improve the ability of competent authorities to collect and effectively utilise trade data, both domestically and internationally, for the purpose of detecting and investigating ML and TF through the trade system. It was also aimed at FATF continuing to explore vulnerabilities in the trade system, including those related to trade finance, with a view to identifying other measures that could be considered in combating illicit use of the trade system.

46. The best practices described include:

a) Capacity building and increased awareness of TBML to be achieved by enhancing the focus on TBML in training programs. Developing capacity to identify anomalies in data collected for trade transactions and in trade finance.

b) Familiarize staff of competent authorities with typologies & 'red flags' and include these in their training materials & internal guidance manuals. A Risk based approach with target orientation has been strongly recommended.

c) Cooperation among domestic competent authorities to be developed so as to facilitate coordination between authorities responsible for collecting and analysing trade data and the authorities responsible for investigating ML and TF. For this purpose, jurisdictions should identify where trade data and trade finance data are being stored and managed. Often such data is dispersed over more than one agency.

[3] http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based %20Money%20 Laundering %202012%20COVER.pdf

d) Investigation Agencies should have timely and clear access to trade data and trade finance databases, through secure networks and Memoranda of Understanding.

e) Practical obstacles in the area of domestic cooperation and information sharing to combat TBML/FT need to be identified and addressed. Specific best practices involving information sharing between domestic agencies and FIU were also suggested. It has been recommended that FIU should be able to obtain information from agencies collecting trade data viz. Customs and Trade Authorities.

f) Encourage international cooperation to provide the widest possible range of mutual legal assistance in TBML/FT investigations and prosecutions. Clear and effective mechanisms and gateways need to be established to facilitate trade data.

47. The Best Practices Paper has recommended safeguards relating to maintenance of data protection and privacy as well as to ensure competitive neutrality for legitimate trading activities which is also supported by the project team.

Money Laundering Vulnerabilities of Free Trade Zones (2010)[4]

48. The 2010 FATF study on Free Trade Zones (FTZs) has significant cross-over with earlier studies on TBML and includes three case studies of TBML. One of these cases relates to TBML for terrorist financing (Hezbollah).

49. Businesses located in FTZs utilise international trade for a majority of transactions. FTZs are designated areas within jurisdictions in which incentives are offered to support the development of exports, foreign direct investment (FDI), and local employment. These incentives include exemptions from duty and taxes, simplified administrative procedures, and the duty free importation of raw materials, machinery, parts and equipment. In addition to boosting economic opportunity, these incentives can result in a reduction in finance and trade controls and enforcement, creating opportunities for ML and TF.

50. The lack of AML/CFT safeguards poses a particular vulnerability in FTZs. Cases in the FATF report highlight systematic weaknesses that make FTZs vulnerable to abuse including relaxed oversight, lack of transparency, absence of trade data and systems integration.

51. The study finds that FTZs may facilitate the TBML and related illicit activity. The misuse of FTZs impacts every jurisdiction in the world, regardless of whether or not a jurisdiction has FTZs.

FATF Typologies on Proliferation Financing (2008)

52. The June 2008 FATF Typologies Paper on Financing the Proliferation of Weapons of Mass Destruction[5] did not address TBML directly, but did include an annex on trade

[4] http://www.fatf-afi.org/media/fatf/documents/reports/ML%20vulnerabilities %20of%20Free%20 Trade% 20Zones .pdf

documentation, including those relevant to trade finance. These descriptions have been included as part of the Chapter on Trade Finance.

EAG

53. The Eurasian Group (EAG) on Combating ML and TF has published two reports relating to TBML. These are as follows:

(i) EAG Working Group on Typologies Study Report on "International Trade Based Money Laundering" (December, 2009)[6]

54. The EAG Study Report on International TBML was based on the generalized findings of national studies conducted by select EAG members. The study considered the use of foreign trade transactions to launder proceeds and instruments of crime. The EAG study focused on identifying the legal aspects of business regulation that affect the development of various mechanisms using both international economic and especially, trade-based, activities for ML. An attempt was made to analyse the legal standards of national legislations governing the conduct and control of foreign trade-based transactions.

55. This Study highlighted instruments, mechanisms and corporate structures, used for TBML. Instruments such as fictitious export/import transactions and false contracts were identified. Common mechanisms used for the purpose have been found as non-declaration / mis-declaration of goods and false certificate of origin. Corporate structures involved in the process comprise three groups of entities viz. transient firms, off-shore companies and illegal financial services providers.

(ii) EAG Typology Report on Risks of Money Laundering in Foreign Trade Transactions (December, 2010)[7]

56. The EAG Report on the Risks of Money Laundering in Foreign Trade Transactions aimed to develop a risk assessment methodology to prevent and combat use of foreign trade transactions in ML schemes.

57. The main features of the study were: the identification of legal aspects in Foreign Trade Regulation; efficient assessment of the risk based approach in national AML strategies; and, the analysis of monitoring mechanisms adopted by financial institutions. The study attempted to classify ML risks in foreign trade transactions by determining the share therein of risk companies, risk countries and risk commodities. All competent authorities, including, policy makers, customs, taxation authorities, central bank and financial institutions were called to adopt risk assessment approach.

---

[5] http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

[6] http://www.eurasiangroup.org/typology_reports.php

[7] http://www.eurasiangroup.org/ru/news/WGTYP_2010_6_eng.pdf

APG

58. The 2008 APG Typologies Report[8] collected case studies from across the Asia/Pacific region and included case studies on TBML and related cases. Case studies on alternative remittance services, shell companies, off-shore banks and promissory notes are of significance to the current research.

59. The 2012 APG Typologies Report includes a number of TBML case studies from across the Asia/Pacific region.

The Wolfsberg Group

60. The Wolfsberg Group is an association of eleven global banks formed in 2000 to develop financial services industry standards. In 2009 the Wolfsberg Group published a paper entitled The Wolfsberg Trade Finance Principles[9], which aimed to contribute to industry efforts to define standards for the control of the AML/CFT risks associated with trade finance activities. The Wolfsberg Group published these Principles on the role of Financial Institutions (FIs) in relation to the management of processes: 1) To address the risks of ML and terrorist financing through certain trade finance products, and 2) To aid compliance with international and national sanctions, including the Non Proliferation of Weapons of Mass Destruction requirements of the United Nations.

61. The paper addresses the mechanisms used for the finance of the movement of goods or services across international boundaries. In particular, the paper provides detailed, practical guidance on the types of controls that may be applied to letters of credit (LCs); documentary bills for collection (BCs); and sanctions, including non proliferation, weapons of mass destruction and dual use goods (NP WMD)

62. In 2011 an expanded version of the paper was published[10]. This version provides additional AML guidance in relation to guarantees (Gtees); standby letters of credit (SBLCs); and open account trade transactions. it is noted:

> "Despite the fact that historically trade finance has not been viewed as high risk it has always been recognised that international trade and the processes and systems that support it are vulnerable to abuse for the purposes of ML and terrorist financing. In recent years, however, the focus on these risks has increased for a variety of reasons, including the dramatic growth in world trade. In addition, the fact that controls introduced by FIs in response to the more traditional ML techniques have become more robust means that other methods to transmit funds, including the use of trade finance products, may become more attractive to criminals." (2011: 3)

63. The Wolfsberg Group noted that it is committed to the application of appropriate systems and controls in respect of trade finance products to mitigate these risks. It does not however

[8] http://www.apgml.org/documents/docs/6/APG_2008_Typologies_Rpt_July08.pdf
[9] http://www.wolfsberg-principles.com/pdf/Wolfsberg_Trade_Principles_Paper_I_(2009).pdf
[10] http://www.wolfsberg-principles.com/pdf/Wolfsberg_Trade_Principles_Paper_II_(2011).pdf

believe that currently there is sufficient evidence to support an assessment of this area as high risk for AML/Sanctions purposes. Despite this, the Wolfsberg Group calls for on-going cooperation between stakeholders to counter the threat of ML in the trade finance area.

United Nations Office of Drugs and Crime (UNODC)

***Risk of Money Laundering through Financial Instruments, Users and Employees of Financial Institutions* (2010)**[11]

64. The UNODC Risk of Money Laundering through Financial Instruments, Users and Employees of Financial Institutions (2010 English version) was produced to address the need of the justice sector to improve their economic, financial and accounting preparation in order to investigate, prosecute and adjudicate ML cases. The report does not specifically address TBML, but contains a brief description of various financial instruments, including a number of trade instruments, as well as their underlying documentation and red flags (451 in total).

65. Chapter 8 deals with Foreign Trade Business. It is noted that "Payments resulting from foreign trade business, understood to be the export or import of goods or services, can be one of the financial instruments at the highest risk for ML operations." (2010: 113). Documents of interest (e.g. the import or export declaration or form, the interbank transfer of funds, and the declaration or form for registering the exchange operation) are identified. Warning signs regarding the transfer of funds resulting from foreign trade are also listed.

United States

66. The Financial Crimes Enforcement Network (FinCEN) issued an advisory in 201012 to inform and assist the financial industry in reporting suspected instances of TBML. This advisory contained examples of 'red flags' based on activity observed in Suspicious Activity Reports (SARs) that may indicate TBML. Financial institutions were advised to take appropriate measures to mitigate the risks of analogous activity occurring globally.

67. It was concluded in that advisory that no one activity by itself is a clear indication of TBML. Due to some similarities with legitimate financial activities, financial institutions should evaluate indicators of potential trade-based money laundering in combination with other 'red flags' and expected transaction activity for its customer before making determinations of suspicion. Additional investigation and analysis may be necessary to determine if the activity is suspicious, based on information available to the financial institution.

[11] http://www.unrol.org/doc.aspx?d=3041
[12] http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-a001.pdf

Journal Articles

Delston R S & Walls SC (2009) Reaching Beyond Banks: How to Target Trade-Based Money Laundering and Terrorist Financing Outside The Financial Sector.

68. Delston and Walls in their publication (Delston R S & Walls SC 2009) Reaching Beyond Banks: How to Target Trade-Based Money Laundering and Terrorist Financing Outside The Financial Sector. Case Western Reserve Journal of International Law 41 (8): 85–118) have stated that AML/CFT measures have succeeded in restricting the two traditional avenues of ML, namely, the abuse of financial intermediaries and the physical movement of money across borders. Consequently, international criminal and terrorist organizations have turned to TBML to conceal and legitimize their funds, as this is a channel that remains relatively untouched by AML/CFT efforts internationally.

69. The authors noted the FATF's focus on TBML due to ML and TF risks as well as financing of the proliferation of weapons of mass destruction (WMDs). The paper proposed a far-reaching solution—that those in the international supply chain be required by law to adopt AML/CFT safeguards to protect their businesses, including filing suspicious activity reports, identifying their customers, and designating an AML/CFT compliance officer.

70. Delston and Walls (2009), argued that there needs to be greater harmonisation between the FATF Best Practices Paper for combating TBML and the 2003 FATF Recommendations calling for traders to adopt CDD, KYC and STR reporting protocols in line with obligations on financial institutions and DNFBPs. Their proposals appear to be at odds with the recommendations put forward in the FATF *Best Practices Paper*, which cautioned against undue regulatory burdens upon legitimate trading activities. However, Delston & Walls warn that 'companies may ignore their TBML risk only at their peril' (Delston & Walls 2009: 118) and suggest that businesses may voluntarily go beyond FATF's Best Practices to safeguard themselves against TBML threats.

Zdanowicz JS 2009, Trade-Based Money Laundering and Terrorist Financing

71. Zdanowicz (Zdanowicz JS 2009, Trade-Based Money Laundering and Terrorist Financing. Review of Law and Economics 5(2): 858–878) contributes to the literature on TBML and terrorist financing by providing an analysis of previously unused statistical techniques and methodologies as a means of monitoring, detecting and prosecuting ML activities. Zdanowicz describes how new statistical profiling methodologies that evaluate transactions contained in a jurisdiction's international trade database can mitigate the risks associated with TBML.

72. Zdanowicz discusses the application of four new TBML profiling techniques which focus on jurisdiction, customs district, product, and transaction price risk characteristics. The paper highlights recent developments which reveal a new focus on TBML and TF.

    1. Trade Transparency Units:
    2. FATF: Trade-Based Money Laundering Report: In June 2006

3. FFIEC Bank Secrecy Act Anti-Money Laundering Examination Manual

Brown HA 2009, Free Trade Zones: Haven for Money Laundering and Terrorist Financing?

73. Brown has raised several possible vulnerabilities associated with the area of FTZs (Brown HA 2009, Free Trade Zones: Haven for Money Laundering and Terrorist Financing? ACAMS Today January: 10–12) that include:

i) Possible lack of regulations or lack of enforcement of regulations within free trade zones;
ii) use of cash or nonfinancial instruments, which are usually high risk, as the primary forms of payment that occur within these zones;
iii) lack of means to implement, enforce or create regulations needed within free trade zones;
iv) difficulties in determining the primary owner of the goods or the point of origin of the shipments due to the transference of many shipments into and out of multiple free trade zones around the world;
v) due to the beneficial tax incentives offered within these areas, and the decrease or lack of tax revenue gathered by customs officials, there is little incentive to enforce or implement regulations and oversee trade;
vi) the lack of automation and an accurate method of recording shipments and items manufactured or received within many free trade zones, causing the loss of a paper trail that can accurately verify the true owner of the goods;
vii) possible zone manipulation to aid in trade-based money laundering, including over-and-under invoicing, *hawalas* and Black Market Peso Exchange, among other trade based schemes.

74. Various best practices and recommendations, as mentioned in this paper could increase the security, regulations and enforcement within these areas that currently do not have the measures in place to monitor or detect illegal activities.

McSkimming S 2010, Trade Based Money Laundering: Responding to an Emerging Threat.

75. McSkimming (McSkimming S 2010, Trade Based Money Laundering: Responding to an Emerging Threat. Deakin Law Review 15(1): 37–63) observes that while little has been done to prevent trade-based financial crime, there is also little empirical evidence of its ill effect. Further, there has been little consideration as to whether systematic monitoring of the trade system would be cost-effective, relative to the number of offenders detected and the harm prevented. Without such analysis, it is almost impossible to reach a measured and balanced view on appropriate policy settings.

76. When considering typologies of over and under invoicing, McSkimming briefly considers issues of transfer pricing manipulation. A transfer price is the price paid for an exchange of goods and services between related affiliates of the same transnational corporation. This may be a parent firm trading with subsidiaries or between subsidiaries of the same firm. Transfer pricing refers to the method transnational corporations adopt for the setting and adjusting prices of goods or services from one associate of the entity to another associate within that same entity. Corporate subsidiaries in different countries must adjust prices

when one subsidiary transfers goods or services to a subsidiary operating in a different country. It is estimated that trade between related transnational corporations affiliates account for 60% cent of global trade, which represents significant risks for transfer mispricing.[13] Tax authorities require that an 'arm's length principle' should be followed in determining the open-market price. Many markets are thin and often dominated by the same multinationals and market prices are hard to determine. Transfer pricing frauds ignore the arm's length principle and misprice transactions to allow companies to move profits to low tax jurisdictions to minimise or avoid tax.

77. McSkimming proposes that even if monitoring were to be implemented, the analytical methodologies that are currently used have major flaws. They not only rely on data that is often of poor quality, but may also be worryingly easy to circumvent. This too, raises serious questions about the effectiveness of the proposed policy responses to TBML. The difficulties associated with data monitoring also raise the spectre of a significant increase in the number of physical, and therefore costly, inspections of trade goods. Preventing TBML/TF will take more than importing AML/CFT strategies from the financial sector to the trade sector. Instead, a robust new approach to AML/CFT in the trade sector will be required.

78. The author highlights that the absence of data on TBML/TF is particularly concerning in light of the fact that TBML/TF is a credible substitute for traditional, financial system ML typologies. If offenders are able to avoid AML/CFT controls by abusing the trade system in substantial numbers, then costly regulation of the financial sector may be pointless. McSkimming notes that the larger, organised crime syndicates most able to take advantage of TBML/TF, which makes the lack of effective AML/CFT responses even more concerning.

Liao J & Acharya A 2011. Trans-shipment and Trade-Based Money Laundering

79. Liao and Acharya (Liao J & Acharya A 2011. Trans-shipment and Trade-Based Money Laundering. Journal of Money Laundering Control 14(1): 79–92) analyse reports made by international organizations and government bodies, particularly, the US, dealing with various aspects of financial crime, import/export activity, and world trade statistics, in order to identify major challenges and possible solutions to the problem.

80. The paper finds that efforts to monitor and staunch the flow of illicit money through trade would be enhanced through more widespread coverage of customs cooperation and standardization of information sharing procedures between national customs agencies. Also, measures should be taken to make free trade areas (FTZs) more transparent to regulatory scrutiny.

[13] Prem Sikka, 'Enterprise, culture and accountancy firms; new masters of the universe', *Accounting, Auditing and Accountability Journal*, vol 21, no 2, 2008, p 268-295, www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=CD97B03F94E6B0C92BDA1B4D3D

Australian Institute of Criminology

81. Sullivan and Smith (Paper: 2011 by Claire Sullivan and Evan Smith, Trade-Based Money laundering: Risks and Regulating Responses Published as Australian Institute of Criminology Reports -Research and Public Policy Series 115) contend that the formation of a regulatory framework to deal with TBML would be premature and unnecessary at this stage, as more research needs to be conducted to ascertain with greater precision the nature, risks and prevalence of TBML in Australia.

82. The Report identifies additional TBML methods besides those identified in the FATF Study 2006. The two other techniques involve:
    (i) related party transactions; and
    (ii) acquisition and sale of intangibles.

83. The Report further holds that the specific areas of risks increase the vulnerability of international trade to TBML. These risks are:
    - Barter trade
    - use of shell and front companies
    - trade with and through high risk jurisdictions; and
    - trade with and through free trade zones.

84. The Report recommends that future education and awareness-raising programs should usefully incorporate training materials on TBML.

CHAPTER II - STATISTICAL ANALYSIS

85. An important objective of this Paper is to build on the existing studies, particularly those of the FATF. The past studies have raised issues in four key areas:

(i) What is the extent of TBML in specific jurisdictions, regions and across the globe?
(ii) What should be the roles, responsibilities of investigating agencies and other allied agencies to tackle TBML;
(iii) What are the best practices (preventative measures) to effectively deal with TBML ; and,
(iv) What are those features of TBML which can make it possible to discern it from other forms of ML?

86. To look at these four primary areas of concern, this Chapter presents a Statistical Analysis. The statistical analysis is based upon the responses received from 19 Jurisdictions and 1 Organization, to a Questionnaire circulated by the APG Secretariat. Due to the limited number of responses received from jurisdictions & organizations the sample size is not large enough to lead to any statistically significant inferences. However, these responses do add to the understanding of the issues involved in each of the four primary areas of concern and can help crystallize work done in the future on TBML.

87. The Questionnaire, comprising six parts, was designed in such a way that each part could be answered by the Agency in the best position to furnish answers in any given jurisdiction. In all, 64 questions were circulated in the Questionnaire. The Six classes of agencies which have combined to answer the Questionnaire can be classified as follows:-

(A) Coordinating Agency; (8 questions)
(B) Customs; (19 questions)
(C) ML Investigating Law Enforcement Agency (LEA); (17 questions)
(D) Financial Intelligence Unit; (7 questions)
(E) Tax Authority; (7 questions)
(F) Anti Money Laundering Regulator; (6 questions)

EXTENT AND PREVALENCE OF TBML PROBLEM

88. The concern about the extent and prevalence of TBML across the globe has confronted investigators and policy-makers, as there are inherent difficulties in gauging the extent and magnitude of the problem. This Paper has highlighted a few of the difficulties which became obvious during the analysis of questionnaire responses. These difficulties may also go some way to explain why only a few cases of TBML have been reported.

89. In fact getting a sense of the magnitude of the problem has been the most challenging for this Paper. Walker J and Unger B in their Paper "*Measuring Global Money Laundering: The Walker Gravity Model*" (published in 2009 in Review of Law and Economics 5(2):821-853) have acknowledged that measuring global ML is still in its infancy. In most jurisdictions,

when data about ML is captured, there is no distinction made in the data with respect to cases of TBML.

90. Further, since in most jurisdictions the same investigating agencies investigate TBML cases and other ML cases, there is no distinction between the methods of detection, investigation and prosecution of the cases of TBML and of other forms of ML. Therefore, no separate statistics of TBML are available among most of the jurisdictions. Suspicious Transaction Report (STR) database of FIUs also generally do not distinguish between TBML STR and other STRs.

91. A general lack of awareness about the red flags of TBML and the multiplicity of authorities which deal with elements of international trade transaction increases the challenges with the detection and investigation of TBML cases. Resultantly fewer cases are being reported, thereby making estimation of the correct size of TBML almost impossible.

92. Responses which have been received from 20 jurisdictions/organizations indicate the following:

a) 45% of the respondents have attributed the reason for so few cases of TBML being reported is the lack of training / awareness and limited resources being allocated for the purpose. Most of the jurisdictions have responded that they have not undertaken sufficient studies and/or risk assessments on TBML; abuse of trade finance; transfer pricing, and alternative remittance systems.

b) 40% of the respondents have attributed the reason for low reporting of TBML cases as their law and current policy. It is interesting to note that such law and policy relate to trade policy and to Customs law. For instance, in a few jurisdictions, violations of Customs law have not been included as a predicate offence under their national AML Law. Consequently, a lower number of cases of TBML have been detected, reported or investigated. A few jurisdictions stated in the questionnaire that low rates of Customs duties / taxes effectively lower the incentive of 'over and-under invoicing' of shipped goods. Since the aim of criminals using TBML is to earn ineligible export incentives and evade customs duty there have been few TBML cases recognized. Others have responded that Customs officers are primarily required to detect and investigate cases of undervaluation / overvaluation of export / import of goods / services, and are not primarily responsible for enforcing the national AML/CFT laws therefore, a limited number of TBML cases are detected. Among other policy/law issues highlighted in the questionnaire were, the absence of proper categorization of TBML cases and hence the nonexistence of separate data for TBML cases. This was explained by the observation that the priority of the authorities, till recent times, has been to prevent ML by the other two significant methods of ML, namely, cash remittance and bulk cash smuggling, rather than through TBML.

c) Only 20% of respondents indicated that TBML was not an issue despite the low recording rates. Reports received from respondents reveal that for a few jurisdictions, international trade is an insignificant percentage of their GDP, hence possibility for TBML is also limited.

93. It appears from the analysis that the low level of cases that have been reported on TBML are largely due to a lack of awareness and training about TBML among the jurisdictions. It follows then that any available statistics will be an underestimate of the true extent of the TBML problem.

94. To ascertain the extent of TBML an attempt has been made in this Paper to see whether all known forms of TBML have been covered by the past studies or whether there is scope for further expansion.

95. Analysis indicates that 55% of the respondents have stated that the FATF studies of the past have covered all known types of TBML. Whilst this leaves scope to explore other types of TBML a few jurisdictions have also reported that the following aspects of TBML call for sharper focus than what has been achieved in the past:

i. 'Under /over pricing' of **services** need to be targeted separately due to its peculiar nature
ii. **Terrorist financing** and its linkage to TBML
iii. Misuse of **Trade Finance**.

96. The most challenging aspect relating to the extent of TBML given the current sample size, has been to arrive at any conclusion about the magnitude of the TBML problem. Perhaps one way of such estimation may be by looking at the number of TBML investigations which have been carried-out; the average size of TBML offence; and, the number of STRs generated in this regard, over the last five years. Even this methodology is flawed by the fact that most of the jurisdictions do not maintain separate statistics for TBML as a distinct from other ML offences and therefore no meaningful inferences can be drawn. However, for the sake of completeness and record, this report will present the few statistics provided, though the results are unlikely to be representative of regional or global patterns.

97. Five jurisdictions reported on the numbers of TBML investigations in the TBML questionnaires. Between 2007 and 2011 investigating authorities in the jurisdictions reported 289 investigations. The number of identifiable TBML STRs generated between 2007 & 2011 has been 1994. The average size of a TBML offence is USD 1.93 million (USD 557.32 million involved in 289 cases), based upon the responses received. The total value of assets forfeited by two of these jurisdictions between 2007 and 2011 on account of TBML was USD 144.35 million.

CONCLUSION ON THE EXTENT AND PREVALENCE OF TBML

98. This study has not been able to draw definitive conclusions on the extent and prevalence of TBML. The few cases reported by the limited number of jurisdictions undermine estimation of the size of TBML. To what extent TBML is in use remains a concern as a straight answer is not available due to the lack of awareness and paucity of training on TBML among the jurisdictions. All the aspects of TBML are not even covered by those jurisdictions which have reported TBML statistics. There is no standardization with regard to the practice of collection and maintenance of data on TBML. Even then, it is obvious that TBML is a

problem for many of the jurisdictions and has tremendous potential as an avenue to launder money.

99. Despite the findings in this Paper in relation to lack of awareness; in tandem with the limited number of TBML studies that have been done by jurisdictions; and, the lack of separate statistics for TBML, it is still asserted by the project team, with some measure of confidence, that these statistics, although underestimating the problem, do go some way to corroborate the significance of TBML as an increasingly important avenue for laundering of proceeds of crime.

ROLE OF AGENCIES RESPONSIBLE FOR TACKLING TBML

100. The 2006 FATF Paper on TBML pointed out that trade data analysis is a useful tool to discover trade anomalies,, which in turn can lead to detection, investigation and prosecution of cases of TBML. The questionnaire sought to consider which agencies are responsible for collecting and managing trade data; what risk management analysis is undertaken for such data; and, whether it is the same agency or some other agency which undertake TBML investigation. The study has sought to determine the role of other allied agencies including the regulators in this regard.

101. Almost all the jurisdictions reported that at least one department within Government records and manages information on goods imported and exported into the jurisdiction. In most of the jurisdictions, it is the Customs Department that does this. In a few jurisdictions, other agencies like the Economic Services Bureau, Free Zone Authorities, Census and Statistics Department, Port Terminal Operators also record and manage information on goods imported / exported. In most of the jurisdictions, information databases are maintained by Customs and these databases record all relevant information both on imported and exported goods. In response to questions on whether information is collected on: the type of goods; value of goods; importer details; exporter details; owner details; receiver details; and, shipping company details etc, almost all the jurisdictions have reported that all this information is collected. Generally, a Customs Declaration Form is used to obtain this information, which besides being used for tax / duty purposes, can also be used for the purpose of detecting or investigating TBML cases. The Questionnaire circulated among jurisdictions also sought to ascertain whether the jurisdictions collected information to identify the true value of goods, i.e. whether there is under/overpricing. 60 %of the jurisdictions have advised that they are using data within the various databases to help identify the true value of goods, i.e whether goods have been under/overpriced, by attempting to ‘normalise, Trade Pricing.

102. 75% of the jurisdictions have indicated that the relevant Customs agencies are also maintaining an intelligence database on import and export of goods; however, 30% reported that Customs also cross reference this information with other government databases, i.e. companies registry, tax records, criminal records etc. Only 20% of the respondents indicated that Customs conduct ML investigations. In most of the jurisdictions, ML investigations were done by a separate ML investigating agency. In these jurisdictions Customs generally referred the potential TBML cases to an investigating agency mandated to investigate ML cases.

103. Only 25% of respondents have reported that Customs have dedicated financial investigators with experience in trade related offences and/or ML investigations. Thus in most of the jurisdictions, although Customs capture and manage the information on goods imported and exported into the jurisdiction, they have either no authority to investigate ML cases or even where they have such authority, they don't have dedicated financial investigators with experience in trade related offences and/or ML investigations.

104. About 50% of the respondents have indicated that Customs personnel are part of joint financial investigation/ML task forces in those jurisdictions. In a few jurisdictions, Customs officers are members of Anti-Money Laundering Working Groups. The working groups do not conduct investigations; however their members do share information, typologies, and emerging trends on ML.

105. 45% of the respondents have reported that the law enforcement agency mandated to investigate ML cases is part of a joint financial investigation/ML task force that conducts investigations into TBML offences. The same percentage of respondents have reported that ML investigating agency have specialist financial investigators to conduct the TBML investigations.

106. Only 15% of the jurisdictions have reported that their FIU form part of any joint financial investigation/ML task forces that conduct investigations into these offences. In the majority of jurisdictions, the relevant FIU is not part of any joint financial investigation/ML task forces that conduct investigations into TBML offences and is designated as the agency responsible for carrying out day to day functions of the ML Reporting Authority only i.e. functioning as an administrative FIU.

107. Only 15% of the jurisdictions have reported that their relevant Tax Authority conduct investigations/audits into TBML. Most responses indicated that the main aim of tax authorities in their jurisdiction was to ensure tax compliance and not to focus on detecting suspected criminal activity of ML. In most of these jurisdictions, there was no detection of any link between TBML and transfer pricing and no case of TBML was detected out of tax compliance audits.

108. Only 25% of the jurisdictions reported that members of the relevant Tax Authority were part of any joint financial investigations/ML Task Force that investigates TBML.

109. More than 50% of the jurisdictions have indicated that the relevant regulator or supervisor are providing guidance to reporting entities regarding TBML vulnerabilities and red flags. Such guidance includes dissemination of examples of suspicious transactions (red flags in relation to trade finance, typologies report and papers issued by either FATF or APG) so as to enhance awareness. Some responses indicate that although no specific guidance was provided in relation to TBML, more general guidelines about AML/CFT were issued to the banking and financial institutions. One jurisdiction indicated that they had established specific examination procedures relating to a range of banking activities, products, and services, including trade finance activities, in the form of an AML Examination Manual. Feedback also indicated that supervisors regularly participated in industry forums, regulator

panels, and other outreach activities so as to provide financial institutions with guidance relating to TBML risks.

110. 50% of the jurisdictions indicated that their AML supervision regime include trade finance aspects of compliance. Response received from one jurisdiction also indicated that in its jurisdiction, AML supervision applied a risk-based approach to scoping and planning its AML supervisory functions.

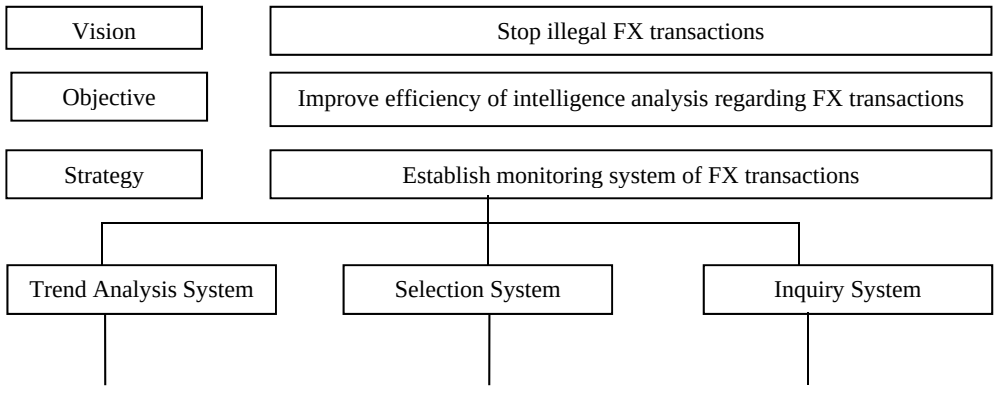
111. Only 40% of jurisdictions indicated that the regulator or supervisor was providing training to reporting entities and to its own staff. Further, only 25% of jurisdictions have reported that regulators have experts in the area of Trade Finance. However, jurisdictions were unanimous that there is a need for training to be provided to regulators about AML risks and vulnerabilities associated with trade finance activities as they, the regulators, would benefit from better training and awareness.

112. 55% of the jurisdictions indicated that their jurisdictions had in place foreign currency controls. However, 25% of jurisdictions reported that in their opinion, such "foreign currency control" had a role in identifying abuse of trade finance or TBML. Thus, it may be extrapolated that in these 25% of jurisdictions the aim and objective of foreign currency controls, are not specifically to target abuse of trade finance or TBML. However, the significance of foreign exchange manipulation in adding to the vulnerability from TBML in international trade and the necessity to monitor foreign exchange data to reduce such vulnerabilities are demonstrated by the contribution from South Korea in the box item placed below.

FX MONITORING SYSTEM

The volume of Foreign Exchange (FX) data received in the course of cross border economic transactions has skyrocketed largely due to increase in international trade. There was no satisfactory system in South Korea which would allow effective monitoring of overall FX data, which limited the capacity for quick response to changes in the foreign exchange market. It became imperative that an Effective Risk Management System is developed to deal with the voluminous data. FX Transaction Monitoring System has been developed in South Korea which aims at (1) effective monitoring of FX data, (2) selection of suspicious companies based on logical criteria, and (3) swift intelligence analysis.

System Structure



(1) Time series information on trend of changes in FX data (2) Information on abnormal FX transactions.	(1) Selection model utilizing statistical method. (2) User-oriented selection model.	(1) Detailed analysis on FX Balance Sheet (B/S). (2) One-click inquiry about detailed transaction records.

The Trend Analysis System monitors all FX data (including inward /outward remittances and purchase of bill of exchange) collected by Korean Customs for working out trends of changes. The System categorizes FX data by industry or jurisdiction month-wise so as to provide inquiry service about time series information. Users can take a look at trend of changes in industry-/jurisdiction-specific FX data. The System brings out changes considered abnormal with regard to overall FX data; or FX data by major industry or jurisdiction. Transactions are regarded as abnormal which show abrupt changes compared to average value of the recent three years. Once abnormal transaction is spotted, the system provides relevant information to experts in charge of intelligence analysis. The experts would compare such abnormal inflow or outflow of FX for that industry or jurisdiction with data of exports or imports made from/to that industry/jurisdiction.

The Selection System calculates scores of all exports/imports by taking advantage of statistical method (data mining). Based on the scores, the System helps users to select suspicious companies. Crimes related to FX transactions are categorized into four categories based on applicable legislations and violation types viz. (1) Violations in terms of payment method, (2) Violations in terms of the report of capital transaction, (3) illegally moving property abroad, and (4) ML (which include trade abuse through mispricing etc.) For example ML may occur through inward remittances to multiple bank accounts disguising wire transfers as being related to trade activities. On analysing past crimes of four types of violations, risk profiles of companies are drawn. The System also provides a user-oriented selection model whereby experts in charge of intelligence analysis choose risk factors; and adjust value or ratio depending on their analysis purpose to select suspicious companies. One-click inquiries about suspicious companies regarding their records of export/import clearance and foreign exchange transactions are made possible.

The Inquiry System provides refined FX Balance Sheet (B/S), which reflects position of individual companies and jurisdiction-specific FX B/S of trading partners. Foreign exchange B/S is basic data for intelligence analysis on FX transactions. The B/S allows comparison between export/import amount and receipt/payment of FX money during certain period. The System builds jurisdiction-specific B/S by linking export/import data and FX data of each trading partner jurisdiction; and provides visualized results such as tables and graphs. The System enables one-click inquiry about general information of export /import and FX data of individual companies. The System is equipped with user interface which not only allows selection of suspicious companies but also enables search for raw data of transaction records of each company. Such a System can shorten inquiry time.

113. Only 15% of the jurisdictions have reported that during investigations of Alternative Remitters, they have identified instances of TBML. Further only 10% of the respondents reported that during such investigations of Alternative Remitters, they have identified instances of abuse of trade finance. 40% of the respondents did not submit any response in respect to questions concerning alternative remittance systems.

CONCLUSIONS ON ROLES OF AGENCIES

114. The statistical analysis reveals that 'trade data' is collected and managed by at least one of the Government Department in each jurisdiction. In most of the jurisdictions that Department is the Customs Department which not only collects and manages 'trade data' but also uses the data to detect and investigate violations of Customs Law relating to evasion of Customs duty. However, in most of the jurisdictions, the Customs Department does not have the authority to conduct any ML investigation including TBML investigation. It appears that the agency responsible for ML investigations in those jurisdictions conduct all ML investigations including TBML investigations.

115. The Tax authorities in a large number of jurisdictions also have a limited role to play in investigation of TBML cases. While regulators in most jurisdictions do sensitize their reporting units about the abuse of finance products emphasis on the significance and relevance of these products in detecting TBML does not appear to be high. The lack of trade finance investigators and absence of 'systems' capable of cross-referencing trade data with that of trade finance are important limitations.

DOMESTIC & INTERNATIONAL COOPERATION AND TRAINING

116. Professional specialization of any agency makes it more proficient to carry-out its mandated work. However, a complex problem like TBML which cuts across more than one sector of an economy and goes beyond the national borders require considerable cooperation among agencies both domestically and internationally in order to provide solutions. To address this, a set of questions were incorporated in the Questionnaire so as to determine the extent and manner of cooperation among agencies both at the domestic and international levels. The FATF Paper on Best Practices published in 2008, has recommended having joint task forces among domestic agencies to ensure domestic inter-agency cooperation.

117. This Paper suggests strengthening the arrangements concerning exchange of information by fortifying mutual legal assistance agreements to support more meaningful international cooperation. One significant method of building such best practices has been the suggestion to include TBML orientation in ML training programs. Another set of questions in the Questionnaire relate to the exposure to TBML training for the agencies concerned.

118. The project team has categorized that there are three broad phases of domestic cooperation among the competent authorities namely: sharing of intelligence; coordination in investigation; and, support in prosecution.

119. The statistical analysis reveals that only 55% of the jurisdictions have submitted a response to the question of how the TBML investigations were initiated. 30% of the jurisdictions reported that the inputs for TBML investigations came from intelligence and STRs. 45% of jurisdictions reported that inputs for TBML investigation came from law enforcement agencies whereas only 25% of jurisdictions reported that the source for initiating TBML investigations was "Trade Data". For almost 35% of the respondents, suspicious transactions related to TBML were first reported to FIU, which conducted analysis before reporting it to the relevant investigating authority.

120. 35% of jurisdictions reported that TBML investigations by ML investigating agency are initiated from 'internal intelligence' whereas 55% of respondents reported the source of intelligence for ML investigating agency as 'referrals from other agencies'. Jurisdictions reporting 'internal intelligence' as the source for initiation have also reported that 'referrals from other agencies' are another source for initiating TBML investigations. A few jurisdictions have also reported referrals from the 'private sector'. 60% of responses received indicate that they receive information from the relevant Customs agency. However, 35% of the jurisdictions stated that though their ML investigating agency receives information from Customs there are restrictions on the use of that information.

121. In response to the question on the types of impediments faced in use of information received from other agencies, 25% of the jurisdictions have reported that there are impediments which have been identified as: resource constraints; lack of training; delay in release of further information; and, the inability to justify an inquiry. It is interesting to note that limited capacity to match trade data with financial transaction information also hinders the capability of the FIU to proactively assess possible TBML-related transactions.

122. 30% of the jurisdictions have reported that there are impediments encountered in the extending of cooperation while conducting investigations. According to the survey the main impediments encountered during the course of investigations were maintaining confidentiality; inhibited from using such information in prosecution / legal proceedings; non-disclosure to third parties without consent; and, use of juridical information only with the authorization of a magistrate (or judicial authority).

123. 90% of the jurisdictions submitting response to the Questionnaire reported that Customs agencies receive financial information from the FIU. According to the responses the FIU generally provided such information spontaneously or upon request. However, responses received also revealed that in some countries, there is requirement to sign a Memorandum of Understanding before sharing of information can take place. In one jurisdiction, the FIU has a Memorandum of Understanding (MOU) with several partner agencies/departments. These Partner Agencies according to the response have on-line access which allows them to ask for financial information relevant to all investigations. According to the response, the MOU framework accounts for objectives of each agency and is aligned with national interests.

124. 30% of the respondents have indicated that the Tax Authority receives FIU data for the purpose of investigation of administrative issues. However, to what extent such data relate to TBML has not been indicated.

125. Since TBML occurs across national borders, the best practices for strengthening international cooperation recommended by the FATF in 2008 and supported by the project team needs to be emphasized. Mutual Legal Frameworks with effective gateways must be capable of facilitating prompt exchange of information and trade data.

126. 55% of the jurisdictions have indicated that they seek information from their international counterparts during ML investigations. Responses received indicate that jurisdictions

provide and share intelligence with the Regional Intelligence Liaison Office and World Customs Organization. Some share 'trade data' with their partner countries in terms of specific information sharing agreements to exchange trade data. 40% of the respondents have indicated that they seek information from FIUs and LEAs in other countries. 40% of the respondents have advised however that there are impediments to the receipt or dissemination of this information. The most common impediments identified in the survey are: "supply and use of information under the secrecy clauses"; signing of relevant MoUs: lack of a clear document of mutual administrative assistance in areas that are not under the control of Customs; delay in response; and, use of financial information obtained from the FIUs being limited to intelligence purposes only etc. Further, it was identified that restrictions occur without the existence of a multilateral trade agreement for the use and sharing of information with other foreign partners.

127. About 30% of the jurisdictions indicated that they have shared TBML related intelligence with foreign counterparts. However, 15% jurisdictions have reported that they were not made aware of the results of that dissemination.

128. 70% of the respondents advised that international requests have been made for sharing financial intelligence. Responses also indicate that in some jurisdictions, trade-related information can be shared with other FIUs within the framework of MOUs. Operationalising international cooperation by developing a common platform to share and analyse trade data of trading partners so as to combat TBML is demonstrated by forming Trade Transparency Units (TTU). The challenges met by formation of a TTU and its basic features have been explained in the contribution made by the USA in the box placed below:

TRADE TRANSPARENCY UNITs (TTU)

TBML schemes are often accomplished through customs fraud violations such as over & under-valuation, over & under-shipment, false invoicing, double invoicing, and the Black Market Peso Exchange. Due to the complex nature of international trade systems, law enforcement agencies are only able to see one side of the trade transactions. Criminal investigators might have expertise and experience investigating either financial or customs fraud crimes, but do not have the full financial and trade data that would give them a complete picture of the scheme. This lack of transparency often catalyzes the use of TBML by Transnational Criminal Organisations (TCOs).

Furthermore, as international trade has expanded, so also has the range of activities that TCOs are involved in. This has led to TCOs evolving into loose networks who work together in order to exploit new market opportunities. Such rapid evolution calls for international law enforcement agencies to take a more integrated approach to address this threat. However, many challenges on integration, such as communication and cooperation, still present themselves. Law enforcement agencies are often hamstrung when it comes to sharing information with international partners, relying on traditional diplomatic channels such as Mutual Legal Assistance Treaties (MLATS) or Customs Mutual Assistance Agreements (CMAAs), in order to gather or exchange information on criminal or terrorist threats. These agreements are often lacking in scope and can take considerable time to execute the exchange of information. Additionally, International trade transactions inherently occur behind multiple sides of international borders involving multiple parties and many layers of documentation and paperwork. This complexity and lack of transparency make these transactions highly susceptible to fraud and exploitation.

Another core issue is the disparity of the capacity and capabilities between different international law enforcement agencies. A uniform understanding of the threat and threat space is a key starting point

amongst partnered countries, followed up by in-depth co-sponsored training that will eventually close the knowledge gap on TBML. Law enforcement agencies must follow a uniform methodology in attacking TBML if they are to be successful. Agencies must have adequate strategic, operational, and tactical intelligence capabilities. Also, agencies must have a platform to share trade data across borders with partner countries. Finally, countries must have adequate prosecutorial authorities and arrest powers for their agencies to attack the threat.

In 2004, United States Homeland Security Investigations (HSI) initiated the Trade Transparency Unit (TTU) to prevent, combat, and dismantle TCOs that engage in TBML. TTU develops partnerships with customs and financial agencies around the world to detect trade discrepancies and to investigate criminal violations including TBML. TTU focuses on the sharing of trade information with international partners allowing each TTU to compare values reported on U.S. import/export declarations against the corresponding values reported on foreign counterpart import/export declarations. Investigators are thus able to see both sides of the trade transaction, thereby adding a level of transparency.

The process starts when HSI reaches out to jurisdiction representatives, to further discuss a potential partnership under the TTU umbrella. Thereafter trade data of the partner jurisdiction is formatted. Agreements are signed and guidelines are established for the sharing of trade information. The access to the shared TTU trade software system is the key component that allows the TTUs to operate. TTU has developed a proprietary computer-based system called "Data Analysis & Research for Trade Transparency System" (DARTTS) to host and analyse the combined international trade data, which allows the user to identify abnormal trade transactions that may indicate TBML, customs duty evasion, and other related customs and financial crimes.

Direct communication amongst international partners is highly encouraged. Personnel assigned to the TTUs meet regularly to exchange ideas, discuss emerging trends and to provide each other support, guidance, training, and tools to combat TBML.

129. The FATF Best Practices Paper 2008 urged for a stronger focus on training programmes for competent authorities to enhance their ability to identify TBML techniques which is also supported by the project team. Such programmes, particularly those directed towards investigating and other allied agencies, must highlight the relevance of both financial and trade data to assist programme participants in detection of TBML cases.

130. 40% of the jurisdictions indicated that Customs have received training on TBML. Further, only 10% indicated that they provided training to others. Most of the jurisdictions have agreed on the need for better training and understanding of the techniques of TBML. Even on the question of 'challenges and obstacles for the Customs agency', a common response was that besides the 'lack of authority for Customs to investigate TBML cases' (legal issue), 'lack of training and resource' was indicated as a major challenge for Customs to identify or investigate TBML.

131. 35% of the jurisdictions indicated that relevant ML enforcement agencies had received training on TBML. Further, only 15% of the jurisdictions reported that they provide training to other agencies on TBML issues. The main methods of training have been stated as, 'attending local and overseas training and seminars'. Most of the jurisdictions agreed on the need for better training and awareness of the techniques of TBML.

132. Only 35% of the jurisdictions have indicated that the FIU has received training on TBML. Equal numbers of jurisdictions have indicated that FIU is also providing training to other agencies on TBML issues. The mode / method of training are through the participation in international conferences, seminars and overseas training. Material relied upon in the training include annual reports of FIUs, typologies, sanitised cases and indicators linked to TBML latest studies & papers etc. 20% of the jurisdictions have informed that their Tax Authority received training on TBML. Further only 5% have indicated that their Tax Authority provides training to others on TBML issues. Responses received from jurisdictions indicate that officers of Tax Authority are trained to conduct tax audits and no training with specific reference to audit in TBML cases has been received by the said officers.

133. Training to those responsible for detection and investigation of TBML as well as to those who collect trade data and handle trade finance is critical to raise their awareness about TBML and build capacity to identify TBML. Since in majority of jurisdictions those who handle trade data, who deal with trade finance and who investigate TBML belong to separate agencies the significance of building mechanisms for domestic cooperation cannot but be emphasized. Sharing of trade data across trading countries supported by prompt exchange of information during investigation and for prosecution can be very important for preventing and curbing TBML. However, there are impediments in exchange of information both domestically and internationally.

PATTERNS OF FINANCIAL PRODUCTS USED

134. On the issue of financial or banking products used for TBML, responses received from the jurisdictions indicated that formal banking channels as well as alternative remittance system are being used. Normal banking channels that have been used to finance trade are open accounting system and letter of credit mechanisms. The gaps between declared trade transaction value and the true value of goods have often been filled-up through alternative remittance.

RED FLAGS AND PATTERNS

135. The last set of questions in the Questionnaire relate to eliciting responses from the jurisdictions about the indicators which can help discern the patterns of TBML. The FATF Best Practice Paper 2006 has regarded making case studies and red flags available to competent authorities and financial institutions as a basic principle of guidance to foster the capacity to combat TBML. The patterns and red flags help in identifying the occurrence of ML in trade and trade finance transactions. The jurisdictions which responded to the Questionnaire have listed a large number of patterns and red flags which this Paper has categorised in five broad groups: i) Trade Finance; ii) Jurisdictions; iii) Goods; iv) Corporate Structures; and v) Predicate Offences. The last four categories have been dealt with in the past papers under the broad category of trade.

136. TBML can take many forms and the distinction between it and other forms of ML which use the financial system is often blurred. Efforts have been made in the present section of this Chapter to identify and describe specific characteristics of TBML and hence this

Section has examined and analysed trade characteristics as patterns of jurisdictions, goods, corporate structures and predicate offences. Red flags identify only possible signs of illicit activity and have to be considered in conjunction with the normal transaction activity expected.

137. Based on the responses received from jurisdictions, red flags relating to financial & banking products may be categorized as follows:

a) Use of **letters of credit** to move money between those countries, where such trade would not normally occur and / or is **not consistent with the customer's usual business activity**. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.

b) The **method of payment** requested by the client appears **inconsistent with the risk characteristics of the transaction**. For example receipt of an advance payment, for a shipment, from a new seller in a high-risk jurisdiction.

c) The transaction involves the receipt of cash (or by other payment methods) **from third party entities** that have no apparent connection with the transaction or which involve front or shell companies or wire instructions / payment from parties which were not identified in the original letter of credit or other documentation. The transactions that involve payments for goods through cheques, bank drafts, or money orders not drawn on the account of the entity that purchased the items also need further verification.

d) The transaction involves the use of repeatedly **amended or frequently extended letters of credit** without reasonable justification or that includes changes in regard to the beneficiary or location of payment without any apparent reason.

e) **Unusual deposits** i.e. use of cash or negotiable instruments (such as traveller's cheques, cashier's cheques and money orders) in **round denominations** (to keep below reporting threshold limit) to fund bank accounts and to pay for goods and services. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information. Further, cash payments for high-value orders are also indication of TBML activity.

f) Inward remittances in **multiple accounts** and payments made from multiple accounts for trade transaction of same business entity are indicators for TBML. In this regard the study of foreign exchange remittances may help detect the offence.

g) In the case of **merchanting trade**, the trade finance mechanism should be in place for both export leg as well as import leg of transaction. If the Trade Finance mechanism, for example, Letters of Credit, have been provided for only the import leg of the transaction and not for export leg, it also indicates the possibility of TBML.

PATTERNs OF JURISDICTION (FROM WHERE OR TO WHOM, GOODS ARE USUALLY SHIPPED/TRANSHIPPED)

138. The Questionnaire also intended to ascertain patterns from jurisdictions as to or from where goods usually shipped. Responses received indicated that in 90% of jurisdictions, no such patterns had been identified to date, either because of the low numbers of TBML cases or due to other reasons such as a study of this type had not been carried out. Responses indicated that existence of duty free zones or jurisdictions having high import tax / export tax rebate are most likely to be used for TBML. Volume of trade, value of trade, type of commodity or service traded and/or the domestic regulatory environment are the factors which determine the sensitiveness of a jurisdiction for TBML. Generally, all the factors combine to make a jurisdiction prone to high risk of TBML.

RED FLAGS WITH REGARD TO JURISDICTIONS

a) The commodity is shipped to or from a jurisdiction designated as '**high risk'** for ML activities or sensitive / non co-operative jurisdictions.

b) The commodity is **transhipped** through one or more such high risk / sensitive jurisdictions for no apparent economic reason.

c) Presence of **Free Trade Zones / Special Economic Zones** also affects the sensitiveness of a jurisdiction as far as TBML is concerned. FTZs are also emerging as being especially vulnerable to TBML. FATF (2010: 4) defines FTZs as 'designated areas within countries that offer a free trade environment with a minimum level of regulation'. In the said report, FATF noted that most zone authorities operate separate company formation services from those that exist in the rest of the jurisdiction and market the ease of setting up a legal entity in an FTZ to attract business. Many zone authorities request little or no ownership information of the companies interested in setting up in the zone. As a result, it is simpler for legal entities to set up the firms/companies in FTZs and hide the name(s) of the true beneficial owners. This lack of transparency has allowed companies located in FTZs to create layers of transactions that are difficult (if not impossible) for law enforcement agencies to follow (FATF 2010). It also reported that 'goods introduced in a FTZ' are generally not subject to the usual customs controls, with goods undergoing 'various economic operations, such as transhipment, assembly, manufacturing, processing, warehousing'. FinCEN has identified TBML red flags that are specific to FTZs. In its 2010 report, FinCEN (2010: 4) signalled that a number of red flags seen in conjunction with shipments of high dollar merchandise (such as electronics, auto parts and precious metals and gems) to duty free trade zones could be an indication of a trade-based money laundering activity.

   These include:

   i. third-party payments for goods or services made by an intermediary (either an individual or an entity) apparently unrelated to the seller or purchaser of goods. This may be done to obscure the true origin of the funds;
   ii. amended letters of credit without reasonable justification;

iii. a customer's inability to produce appropriate documentation (ie invoices) to support a requested transaction; and
iv. significant discrepancies between the descriptions of the goods on the transport document (ie bill of lading), the invoice, or other documents (ie certificate of origin, packing list etc) (FinCEN 2010).

d) **Circuitous route of shipment** and/or **circuitous route of financial transaction** or **Order for the goods** is placed by firms or individuals from foreign countries other than the jurisdiction of the stated end-user.

e) Transaction involves **shipment of goods inconsistent with normal geographic trade patterns** of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense e.g. Semi-conductor manufacturing equipment being shipped to a jurisdiction that has no electronics industry.

PATTERNS OF GOODS INVOLVED IN TBML

139. Most of the jurisdictions have responded to state that no definite pattern of goods involved in TBML is identifiable. This is probably due to the vulnerability of almost all trade transactions for TBML, irrespective of the goods involved. A few studies including that of Clare Sullivan and Evan Smith cited earlier, have emphasized the vulnerability of trade in services for TBML. Global trade in services provide greater opportunities for ML than trade in merchandise because fraud particularly in regard to valuation of services is more difficult to detect and prove. The intangible nature of services makes even facts of supply / delivery / provisioning difficult to determine. Unlike merchandise, services are also less likely to be standard, so anomalies in value and price are less apparent and more difficult to substantiate. However responses do indicate that goods involved in TBML will be usually those goods, where it is rather difficult to identify true value, due to the nature of these goods. Further responses also indicate that vulnerable goods are those which are subjected to higher taxes/ duties or are high turnover goods or are high valued goods. Examples of such goods are consumer goods, textiles, garments, engineering goods, electronics goods, illicit tobacco products, leather goods, luxury cars, precious metals, counterfeit products, diamonds, metal scraps. Illicit trade in tobacco has been identified as prone to ML as such trade is cash intensive, profitable with low levels of risk, and the possibility of intermingling of illicitly generated funds with legitimate forms of business is high.

RED FLAGS WITH REGARD TO GOODS

a) Where significant discrepancies appear between the **description, quality and quantity** of the goods on the documents such as bills of lading, invoices etc and the actual goods shipped. The misrepresentation may also be in relation to or type / grade of goods. For example, a relatively inexpensive good is supplied but it is invoiced as being more expensive, of different quality or even as an entirely different item so the documentation does not accurately record what is actually supplied. This technique is particularly useful in TBML. Cheap cloth items / waste thereof are declared as premium quality garments to launder the criminal money.

b) Significant discrepancies appear between the **value** of the commodity reported on the invoice and the commodity's fair market value. This is done either in conjunction with mis-declaration of the description / quality / grade of goods or without it. This is also often associated with mis-declaration of the jurisdiction of origin.

c) **Consignment size or type of commodity** being shipped appears **inconsistent with the scale or capacity of the exporter or importer having regard to their regular business activities** or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.

PATTERN OF CORPORATE STRUCTURES

140. To adduce information about the types of corporate structures i.e. Companies, Partnership Firms, Proprietorship, Offshore Companies etc. used by criminal syndicates in TBML, relevant questions were included in the Questionnaire. Responses indicate that both domestic companies as well as overseas companies are used by criminal syndicates. Bogus registered companies (behave like true consignor / consignees of goods) and offshore companies located in tax havens have been reported as corporate structure misused by criminal syndicates. The use of offshore companies is also associated with complex schemes and methodologies utilized by established criminal enterprises.

RED FLAGS WITH REGARD TO CORPORATE STRUCTURES

a) The transaction involves the use of **front or shell companies**. Both shell and front companies can be used to facilitate TBML but in different ways. A shell company has no real operating activity and is used to hide ML activity and the identities of individuals involved so as to obscure the money trail. If activity is traced to the company it is literally an empty shell. As FATF (2010: 20) explained TBML and other ML schemes rely on the ability of the perpetrator of the crime to distance themselves from the illicit proceeds. Shell companies enable illicit actors to create a network of legal entities around the world. By contrast, a front company has real business whose legitimate operations are used as a cover for ML and other criminal activity. In many ways, front companies present a much more significant TBML threat than shell companies. The characteristics of offshore companies, for example, convenient formation, free operation, tax exemption and financial secrecy, all provide rather good veneer to disguise ML

b) Numerous **sole proprietorship businesses/private limited companies** set up by seemingly unrelated people (proxies) are found to be controlled by the same group of people. For the setting up of such businesses false addresses are registered.

c) Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management. TBML requires collusion between traders at both ends of the import/export chain. **Related party transactions** (ie transactions between entities that are part of the same corporate or business group) can possibly make TBML easier and more difficult to detect. Related party transactions, including transfer pricing, rely on mutual agreements between the parties, rather than free market forces. As the FATF (2006: 5) pointed out, over-

or under-invoicing of goods and services requires collusion between the exporter and importer. Although there is a higher risk of related party transactions being used for fraud and for TBML, dealings between related parties are not necessarily illegal.

d) **Transfer pricing** is a related party transaction that is commonly used by transnational corporation as part of their financial and tax planning strategy. Multinational organisations use transfer pricing to shift taxable income from jurisdictions with relatively high tax rates to jurisdictions with relatively low tax rates to minimise income tax. Similar strategies are also employed in relation to import duties and value added tax. FATF (2006: 3) made it clear though that in the case of transfer pricing, the reference to over- and under-invoicing relates to the legitimate allocation of income between related parties, rather than customs fraud. However possibility of TBML originating in transfer pricing cannot be ruled-out.

PREDICATE OFFENCES OF TBML

141. 15% of the jurisdictions have reported that **tax evasion** is the predominant predicate offence in TBML cases whereas 10% of the jurisdictions have reported **customs offences** as the main predicate offence. Other responses indicate that predicate offences are often related to commercial fraud, IPR, Narcotics, human trafficking, terrorist financing, embezzlement, corruption, organized crime (racketeering), dealing in banned goods, conducting illegal business, speculation etc. One Reporting jurisdiction indicated that ML is considered to be an autonomous offence and there is no need to prove the existence or nature of the predicate offence in order to prosecute hence as a consequence, there is no systemic link between ML cases and other crimes.

CONCLUSION ON RED FLAGS

142. The attempt here to segregate Red Flags for different segments of TBML is to simplify the process of understanding the complex problem of TBML. In real life situations the occurrence of more than one red flag is likely for trade transactions involving ML. The red flags enumerated in this Chapter are by no means exhaustive. Annexure A to this Paper has enlisted ‘red flags’ from a number of sources. The process of developing red flags is continuous and requires more and more jurisdictions to contribute towards a common pool of knowledge.

CHAPTER III - TRADE FINANCE

SIGNIFICANCE OF TBML

143. TBML provides an important avenue for disguising funds of illicit origin and for moving value to finance illegal activities. Chapter II on Statistical Analysis may have failed to show the extent and prevalence of TBML in terms of statistical results. However, the significance of TBML as a means of moving illicit value across the globe cannot be denied.

144. Baker (2005: 25) has argued that because 'anything that can be priced can be mispriced' and 'false pricing is done every day, in every jurisdiction, on a large percentage of import and export transactions' that TBML 'is the most commonly used technique for generating and transferring dirty money—money that breaks laws in its origin, movement and use'.

145. Preliminary examination of this statement would invoke acceptance by most AML practitioners as anecdotal evidence indicates that false pricing (under and over invoicing) is considerably widespread. It is considered by the project team to be particularly prevalent in trade within jurisdiction as a means of generating criminal wealth through deliberate avoidance of taxation commitments. This is one of the reasons why domestic trade is not within scope of this paper.

146. The project team believe that the geneses of TBML was to defeat the ability of jurisdictions to collect appropriate revenue as espoused by Baker but in more modern times, under and over invoicing has in fact become a 'by-product' of what has been identified as professional ML schemes involving very complex international TBML structures capable of moving billions of dollars of value with impunity. In these instances, the commodity is as good as cash without the governance currently imposed on cash transactions around the world. Why this can be achieved is also because of the fundamental lack of regulation of Trade internationally which provides the money launderer with ample vulnerabilities to exploit.

147. Using the cover of Trade is the most logical next step as it further frustrates the activities of regulators and investigators due to the sheer size of the trade mechanisms worldwide and the continuing introduction of new products to reduce supply line costs. The vast number of trade transactions produces a high level of 'noise' about the level of legitimate trade and increased flexibility of the processes masks the criminal ML activity. Without specific information to help focus investigations, automatic monitoring becomes relatively ineffective. Legitimate Trade structures have a significant number of benefits to professional ML syndicates namely:

- The large amount of value that is moved internationally in the guise of Trade;
- The appetite of jurisdictions especially those that are developing economies to promote trade which in turn reduces red tape to create corporate entities;
- The ability to mask true activity of corporate entities and ability to disburse concentrations of illegal currency through corporate entities disguised as 'business as usual';
- The ability to engage in corrupt practices on the pretense of trade and trade negotiation;

- The existing trade based mechanism including 'Trade financing', International trade payments in foreign exchange; trade liberalisation, electronic commerce and other financial markets are susceptible to abuse;
- Lack of international regulatory coordination;
- Lack of data matching across sovereign states;
- Inconsistent legal frameworks; and
- Enhanced electronic communication.

148. Unlike alternate remitters systems that are very mobile and operate on very small overheads, TBML structures, especially those that move large amounts of value, are expensive to create, expensive to maintain, leave a considerable evidentiary trail and are difficult to dismantle. It is for these reasons that those responsible for their creation leverage as much criminal profits as they can. These same structures can be used to:

- Launder criminal profits and instruments of crime from criminal activity other than tax evasion and fraud;
- Undertake large fraud;
- Facilitate confidence and other financial scams;
- Facilitate corruption payments; and,
- Siphon money from aid and other Government assistance programs.

149. Each can be undertaken as an individual activity or simultaneously if necessary. For this reason the project team see TBML as the most difficult activity to detect and in turn successfully disrupt and dismantle.

150. Further, professional money launderers do not need to utilise the traditional financing mechanisms used in International trade (for example credit documentation) as they are moving excess value (profit) or financing ongoing criminal activity (instrument of crime) and credit is not essential. They do so however, to further disguise their activity. The application of credit facilities also assist the criminals to defray their risk if it happens that their activities are detected as the credit partner has a legal right to at least some share of the funds that might be restrained for possible forfeiture.

THE TRADE FINANCE ENVIRONMENT

151. In order to better understand how TBML operates it is necessary to understand the environment in which it operates. By understanding this environment, the ML investigator can better recognise the 'red flags' that help peel away the veneer considered paramount by money launderers in achieving their goals. With this veneer in place, an investigator is unlikely to recognise TBML as a result of all the 'noise' of legitimate trade. As stated, this paper attempts to provide investigators and in turn regulators with the insight to enable them to 'crack' that veneer.

152. Occurrence of trade in a Cash Based Economy can also open up possibilities for TBML which may throw up challenges of its own kind. The contribution by Nepal in the box item placed below give succinct description of such challenges.

CASH BASED ECONOMIES

Less developed countries have economies which are largely cash based. These countries also usually have manual system of records. Such records lying with different entities are in a fragmented state and are usually un-reconciled. Discreet access to such records becomes impossible. These two features viz. Pre-dominance of cash transaction and manual record keeping pose many challenges in combating financial crimes as it is difficult to follow the paper trail. Cash based economies flourish in an economic environment which has a limited number of financial institutions in the formal financial sector. This situation makes the economy vulnerable to a number of financial crimes, including TBML.

Predominance of cash transactions builds uncertainty in the financial system. Transactions in cash allow for concealment of the true value of a transactions and/or the misrepresentation of true records. Cash transactions may even facilitate cash smuggling. Such transactions also fuel the underground economy and tax evasion.

The manual system of records engenders its own set of problems. There is difficulty in data collection. The data cannot be easily cross-checked, timely review of information is not possible and identification of any ultimate beneficiaries or ultimate suppliers and recipients becomes rather difficult. Without a proper database, the customs authorities in these countries also have a major handicap in detecting and investigating TBML cases.

The economic scenario is further compounded by the use of Alternate Remittance Systems (hawala / hundi) by workers of such countries who are located abroad and need to send their savings back home. Such an environment is quite conducive to TBML where proceeds of crime can be very easily structured as remittance for import/export and presented as legitimate funds.

153. It has been said that *trade finance* can be seen as the precise science of managing the capital required for Trade to flow. This chapter describes the most common of the Trade Financing Instruments used today in legitimate trade transactions and then attempt to identify the vulnerabilities of each of these.

154. In its simplest form, an exporter and importer enter into an agreement to Trade. This may be done in some developing regions by way of 'countertrade' but more often than not, it is achieved by way of a cash payment or some more complex form of financing.

155. Traders require working capital (i.e., short-term financing) to support their trading activities. Exporters will usually require financing to process or manufacture products for the export market before receiving payment. Such financing is known as *pre-shipping finance*. Conversely, importers will need a line of credit to buy goods overseas and sell them in the domestic market before paying for imports. In most cases, foreign buyers expect to pay only when goods arrive, or later still if possible, but certainly not in advance. They prefer an open account, or at least a delayed payment arrangement. Being able to offer attractive payments term to buyers is often crucial in getting a contract and requires access to financing for exporters.[14]

[14] Trade Facilitation Handbook for the Greater Mekong Subregion – Chapter 8: An introduction to Trade Finance

156. The absence of an adequate trade finance infrastructure is, in effect, equivalent to a barrier to trade. Limited access to financing, high costs, and lack of insurance or guarantees are likely to hinder the trade and export potential of an economy, and particularly that of small and medium sized enterprises. Trade facilitation aims at reducing transaction cost and time by streamlining trade procedures and processes. One of the most important challenges for traders involved in a transaction is to secure financing so that the transaction may actually take place. The faster and easier the process of financing an international transaction, the more trade will be facilitated.[15]

157. Financial institutions play the critical role in trade finance. The trade finance products elaborated in this chapter are all derived from financial institutions. Financial institutions have a role to play in efforts to prevent ML activity, holding a large amount of intelligence and information critical for TBML investigators. Often however, these institutions are not aware of how critical the information they hold may be to an investigator. Close interaction with financial institutions is seen by the project team as fundamental to success in dismantling TBML structures.

158. The role of Government in *trade financing* is crucial especially in emerging economies. In the presence of underdeveloped financial and money markets, traders have restricted access to financing. Governments can either play a direct role like direct provision of trade finance or credit guarantees; or indirectly by facilitating the formation of trade financing enterprises.

INSTRUMENTS OF TRADE FINANCE & THEIR VULNERABILITIES

Bills of Exchange

159. The drawing of a 'bill of exchange' (also referred to as a 'draft') is commonly used by exporters as a means of obtaining payment from buyers for goods shipped. Bills of exchange protects (reduces transactional risk) of both parties. Documentary credits (discussed later) issued for buyers by banks usually require bills of exchange to be drawn, and frequently bills of exchange are drawn by the seller in terms of the commercial contract of sale with the buyer.

160. The relevant financial institution has a vested interest in this transaction, as they are advancing credit to the buyer; and, given this advanced credit may be considerable in monetary terms, the due diligence by the institution is usually as comprehensive as is possible given the circumstances.

161. The Draft or Bill of Exchange (not always required) provides formal evidence of debt under a letter of credit and is presented with all other documents unless stipulated otherwise. A Draft may contain information on:

- Value of Draft, date of payment and payment terms e.g. "at sight", "30 days after sight", "60 days after Bill of Lading Date".

[15] (http://www.unescap.org/tid/publication/chap8_2224.pdf

- Date Exporter presents documents to the "available with" Bank (not normally required).
- Letter of credit reference number assigned by the Issuing Bank (if required by credit).
- Date the letter of credit was issued (not normally found on a draft).
- Name and address of the Issuing Bank (if the drafts are drawn on the issuing bank).
- Name and address of the bank on which the Drafts are to be drawn.
- Signature of an authorised signing officer of the Company and the Beneficiary's name as shown on the letter of credit.

162. The *Commercial Invoice* is the accounting document through which the exporter charges the importer for goods and services purchased. The Invoice gives details about:

- Merchandise weight, quantity and price and currency.
- The name and address of Exporter and the Importer.
- The number of copies presented and signed if required.
- The trade term listed, e.g. C.I.F., F.O.B etc.

163. The *Transport Document* (or Bill of Lading, Airway Bill, Railway Consignment Note) is a document issued by the carrier that describes the goods that have been accepted for carriage. In some forms, the Bill of Lading may also act as a document of title to the goods and should include information that is consistent with the letter of credit:

- Information on the merchandise (usually a general description).
- The points of loading and discharge.
- To whom the Bill of Lading is consigned.
- The date of shipment.

164. The *Insurance Document* is a guarantee in part or in whole (depending on the terms and conditions) by an insurance company, specifying the goods shipped on a named vessel, indicating the applicable coverage, and showing to whom loss is payable.

165. The *Certificate of Origin* notes the country where the goods were produced. The *Certificate of Inspection* offers an opinion that the specified quality and quantity related conditions have been met. These documents should be dated on or before the Bill of Lading date.

166. A *Packing List* is usually supplied by the exporting shipper in cases where a diversified shipment is packed in several packages or containers. The list will show the contents of each box or case identified by a specific number. A *Weight Certificate* is supplied by the Exporter, at the request of the Importer. It certifies the weight of each large unit in a shipment or the net and gross weights of packages containing smaller units. It is of

particular value when the price of the goods is based on weight and, also, is often used by the carrier in arriving at the weight to be recorded on the Bill of Lading as a basis for the freight charges.

167. The quantity of units/weights should match the Commercial Invoice (this may or may not agree based on how the weights are calculated by the various parties involved). The breakdown of merchandise/weight per carton, package or container should be shown if requested in the letter of credit.

Vulnerabilities:

- Undertaken and paid for without any form of due diligence by an intermediary in the supply chain because the parties are complicit.
- Phantom trades maybe the cause of unrealistic timeframes or unrealistically short supply chains.

Countertrade

168. Countertrade exists where economies face the problem of limited foreign exchange holdings. That is, they do not hold enough currency of the jurisdiction they are trading with to pay the outstanding debt and the cost of buying more foreign currency to service that debt makes the trade uneconomical.

169. One way to overcome this constraint is to promote and encourage countertrade. It generally encompasses the idea of subjecting the agreement to purchase goods or services to an undertaking by the supplier to take on a compensating obligation in lieu of a cash settlement. The seller is required to accept goods or other instruments of trade in partial or whole payment for its products. Some of the forms of counter trade include:

- Barter – This traditional type of countertrade involving the exchange of goods and services against other goods and services of equivalent value, with no monetary exchange between exporter and importer.
- Counter purchase – The exporter undertakes to buy goods from the importer or from a company nominated by the importer, or agrees to arrange for the purchase by a third party. The value of the counter-purchased goods is an agreed percentage of the prices of the goods originally exported.
- Buy-back – The exporter of heavy equipment agrees to accept products manufactured by the importer of the equipment as payment.

Vulnerabilities

- The TBML vulnerabilities arise in determination of exchange ratios for the goods to be countertraded. Such ratios may often be determined as a process of negotiation rather than market determined, giving scope to TBML.

Documentary Credit (Letters of Credit, etc)

170. Generally the exporter requires an importer to prepay in cash for goods shipped. The importer naturally wants to reduce risk by asking the exporter to acknowledge through documents that the goods have been shipped. The importer's bank assists by providing a letter of Credit (Documentary credits) to the exporter (or the exporter's bank) providing for payment upon presentation of certain documents, such as a bill of lading, either immediately or at a prescribed date.

171. A letter of credit is a precise document whereby the importer's bank extends credit to the importer and assumes responsibility in paying the exporter. Aside from the letter of credit document, other documents used in legitimate Trade include shipping and insurance documents, and commercial invoices. The documentary credit arrangement offers an internationally recognised and used method of attaining a commercially acceptable undertaking by providing for payment to be made against presentation of documentation representing the goods, making possible the transfer of title to those goods.

172. Documentary credits (LCs, etc) are seen as a declining method of doing business, although small and medium enterprises often rely upon documentary credit basis for trade finance. Trade finance has been shifting away from this sometimes cumbersome and often expensive method of conducting business to that conducted on an open account basis.

Vulnerabilities

- Even in this simple form the true value of goods transferred between countries can be masked through misrepresentation of price, quantity and quality. Letters of Credit may be generated to create a veneer.
- The documentation generated in the process leaves a paper trail which money launderer may rely upon to disguise illegal proceeds.

Open Account Facilities

173. Open account transactions can be described as 'buy now, pay later' and are more like regular payments for a continuing flow of goods rather than specific transactions. The pursuit of 'supply chain efficiencies' among larger businesses has encouraged their preference for open account trading, even as small and medium enterprises still rely upon documentary credit basis to conduct business of international trade. Ultimately these results suggest that trade finance should be flexible and that financiers will benefit by adapting product and service offerings to the needs of customers in different segments.[16]

Vulnerabilities

- Open account facilities have caused a disconnect between the movement of the underlying trade and the money used to finance it.

[16] http://www.east.com.au/media/2009-09-16.pdf

- Payments against these facilities may or may not be undertaken through an international funds transfer instruction (IFTI) or SWIFT.

174. A range of Open Account Facilities are set out below.

Factoring

175. Factoring, also known as invoice discounting, receivables factoring or debtor financing, is where a third party company assumes a debt or invoice from another company. This involves either the sale at a discount of accounts receivable or other debt assets on a daily, weekly or monthly basis in exchange for immediate cash. It can also involve the charging of interest on the debt. The debt assets are sold by the exporter at a discount to a factoring house, which thereby assumes part of risks of the account receivable. Factoring in international trade is the discounting of a short-term receivable (up to 180 days). The exporter transfers title to its short-term foreign accounts receivable to a factoring house for cash at a discount from the face value. It allows an exporter to ship on open account as the factor assumes the financial liability of the importer to pay and handles collections on the receivables. The factoring house usually works with consumer goods.

176. Factoring therefore relieves the first party of a debt for less than the total amount providing them with working capital to continue trading, while the buyer, or factor, chases up the debt for the full amount and profits when it is paid. The factor is required to pay additional fees, typically a small percentage, once the debt has been settled. The factor may also offer a discount to the indebted party. Essentially factoring transfers the ownership of accounts to another party that then chases up the debt. In the absence of private sector players, Governments can facilitate the establishment of a state-owned factor; or a joint venture set-up with several banks and trading enterprises. The peak international body is Factors Chain International (FCI) which is a body that International Factors deal with[17].

177. Factoring is divided into import factoring and export factoring. Details of each are set out below.

Export factoring

178. In export factoring, the Factor deals directly with the seller of the goods. In this case the debt is a 'recourse' debt, and if the seller goes under, or the purchaser does not pay, the local Factor assumes the risk. In Export factoring the local Factor, deals with a counterparty Factor, who will check out the creditworthiness of the purchaser.

179. In this case the seller will provide documentation to show that the goods have been shipped prior to payment. Payment is usually made on an 80/20 split, 80% is paid to the seller at the time of the invoice/goods shipment. This amount is loaned to the seller by the Factor and interest charged until the purchaser pays. When the purchaser pays the 100% of the invoice

[17] http://www.fci.nl/about-factoring/how-does-it-work

the Factor pays the seller the other 20% of the invoice. There is usually a small activity fee (around 1% of the invoice that is also charged, so it is typically a 80/1/19 split!)

Import Factoring

180. Import factoring is a reverse of the scenario set out for export factoring, but differs slightly. The local Factor will insure the risk on a usually 80% basis, and will therefore carry a 20% risk. This is called a 'non-recourse debt'. The local Factor will check out the bona fide credit history etc. of the purchaser of the goods. Credit lines etc are usually established.

181. The foreign factor will examine the bills of lading shipping documents etc and confirm with the Local Factor. International factoring (as opposed to domestic factoring) have more to do with the counterpart abroad and with insuring risk.

Vulnerabilities

- Often the factor may be left with losses after the so-called traders disappear, after having indulged in TBML, by moving illicit funds through ‘sham trade’.

Forfaiting

182. Forfaiting is the purchase of an exporter's receivables (the amount importers owe the exporter) at a discount by paying cash. The purchaser of the receivables, or forfaiter, must now be paid by the importer to settle the debt. As the receivables are usually guaranteed by the importer's bank, the forfaiter frees the exporter from the risk of non-payment by the importer. The receivables have then become a form of debt instrument that can be sold on the secondary market as bills of exchange or promissory notes. Forfaiting is a method of trade financing that allows the exporter to sell its medium-term receivables (180 days to 7 years) to the forfaiter at a discount, in exchange for cash. With this method, the forfaiter assumes all the risks, enabling the exporter to extend open account terms and incorporate the discount into the selling price. Forfaiters usually work with capital goods, and large projects.

Vulnerabilities

- These instruments (exporter's receivables) are capable of being sold on the secondary market as ‘bills of exchange’ or ‘promissory notes’, provides a money launderer with an enhanced mechanism to move value.
- If the launderer, through collaboration inflates the value of receivables more value can be moved.

Pre-Shipment Finance

183. This is financing for the period prior to the shipment of goods, to support pre-export activities like wages and other costs. It is especially needed when inputs for production must be imported. It also provides additional working capital for the exporter. Pre-shipment financing is especially important to smaller enterprises because the international sales cycle

is usually longer than the domestic sales cycle. Pre-shipment financing can take the form of short-term loans, overdrafts and cash credits.

Vulnerabilities

- Pre-shipping finance especially its application to 'inputs for production that must be imported' provides the money launderer with an ability to engage a third party in another jurisdiction thus moving value to all venues in which the criminal syndicate are operating and thus widen the scope for TBML.
- Short-term loans, overdrafts and cash credits may allow launderers to make business claims on the relevant revenue agencies in those countries thus supplementing their reasons for the value they hold.

Post-Shipment Finance

184. This is financing for the period following shipment. The ability to be competitive often depends on the trader's credit term offered to buyers. Post-shipment financing ensures adequate liquidity until the purchaser receives the products and the exporter receives payment. Post-shipment financing is usually short-term.

Vulnerabilities

- Although this method of financing is short term by nature, cash is usually supplied at time of sale, hence such pretence would not raise suspicion unless intelligence arouse such suspicion.

Buyer's Credit

185. A financial arrangement whereby a financial institution in the exporting jurisdiction extends a loan directly or indirectly to a foreign buyer to finance the purchase of goods and services from the exporting jurisdiction. This arrangement enables the buyer to make payments due to the supplier under the contract.

Vulnerabilities

- Financing of the importer by an institution in the exporter's jurisdiction widen the scope for TBML, since to exercise due diligence in a foreign jurisdiction may be more difficult.
- The money launderers seek this credit to help minimise risk of confiscation.
- If a financial institution has a stake in the trade, law enforcement has to account for that stake in any ensuing action unless the law enforcement action can demonstrate that the financial institution in complicit.

Supplier's Credit

186. A financing arrangement under which an exporter extends credit to the buyer in the importing jurisdiction to finance the buyer's purchases.

Vulnerabilities

- The utilisation of *Supplier's Credit* arrangements provide a mechanism to move significant amounts of value in most forms irrespective of whether or not the trade is legitimate, inflated or phantom.
- This financing arrangement need not involve a financial institution, although to reinforce the veneer, engaging the third party may be undertaken in ML schemes.
- If the buyer and seller are in collusion, this mechanism is a channel for TBML.

Structured Commodity Finance

187. Structured commodity finance (SCF) focuses on three main commodity groups: metals & mining, energy, and soft commodities (agricultural crops). It is a financing technique utilised by commodity producers and trading companies conducting business in the emerging markets. SCF provides liquidity management and risk mitigation for the production, purchase and sale of commodities and materials. This is done by isolating assets, which have relatively predictable cash flow attached to them so as to estimate their present value. The corporate borrowers use such assets to mitigate risk and secure credit from a lender. A corporate therefore borrows against a commodity's expected worth.

188. If all processes go to plan, then the lender is reimbursed through the sale of the assets. If not then the lender has recourse to some or all of the assets. Lenders charge interest on any funds disbursed as well as fees for arranging the transaction. SCF funding techniques include those techniques previously mentioned, namely, pre-export finance, countertrade, barter, and inventory finance. These solutions can be applied across part or all of the commodity trade value chain: from producer to distributor to processor, and the physical traders who buy and deliver commodities.

189. As a financing technique based on performance risk, it is particularly well-suited for emerging markets considered as higher risk environments.[18]

USEFUL TIPS FOR TBML INVESTIGATORS

190. Whilst it is suggested that trade financing and especially open account facilities can provide a reasonable veneer for the activities of the money launderer, it is still costly to set up and maintain. It is important to emphasise that if the veneer protecting the criminal mischief is cracked the trail is relatively easy to follow. In conducting Trade business, legitimate companies also require mechanisms to track their activity and example of this include:

Export Credit Insurance

191. In addition to financing issues, traders are also subject to risks, which can be either commercial or political. Commercial risk arises from factors like the non-acceptance of goods by buyer, the failure of buyer to pay debt, and the failure of foreign banks to honour

[18] http://www.tradefinancemagazine.com/boutUs/tub/WhatIsTradeFinance.html

documentary credits. Political risk arises from factors like war, riots and civil commotion, blockage of foreign exchange transfers and currency devaluation. Export credit insurance involves insuring exporters against such risks. Export Credit Insurance is not likely to be something of interest to either the professional or novice money launderer as it adds additional costs seen as unnecessary and therefore should be something actively examined by the TBML investigator.

Trade Services Utility

192. In response to the development of open account trading, the organisation SWIFT launched the TSU (trade services utility), a collaborative centralised data matching utility, which allows banks to build products around its core functionality to improve the speed and flow of open account trade. This is helping banks re-intermediate themselves into these trade flows.

193. This development may in fact be of assistance to TBML investigators as it can help identify 'red flags' discussed in this paper. There are a number of other mechanisms capable of collecting data including revenue departments, customs departments, accountancy data, general financial data, market data, topography data and social media data. The issue to date when it comes to investigating and prosecuting TBML is that this data is still stored in a dispersed way.

194. TBML investigator will need to devise ways in which to gather this data, have it integrated and then analysed against the concept of time and distance and normality. It is only then will enough criminal activity will be identified and actioned to cause a change in general attitude which is all that can be expected.

195. The project team believes that two critical elements that might be used to crack the veneer created by the ML syndicates is for investigators to consider the concepts of time and distance in ML schemes. Investigators need to commence building a time line of all known events surrounding the activities of the syndicates being investigated. Information and intelligence gathering is paramount to this endeavour and interaction with the financial institution is essential. These institutions have a vested interest in ensuring the trade in which they are engaged is legitimate. These discussions may be hampered by domestic privacy restrictions so legislative change may be necessary before significant headway can be made.

196. Distance is the other key concept. Inconsistencies in documentation, excessive complication and unrealistic time frames all contradict that path of least resistance and should therefore raise suspicion.

Partnership with Private Sector

197. An outreach programme can help create awareness about the TBML vulnerabilities to which private business are exposed. Not only the private sector can install preventative measures but in turn disseminate useful information for the ML investigators. U.S. Immigration and Customs Enforcement (ICE) have introduced many new initiatives aimed

at analysing and combating the movement of illicit funds by bulk cash smuggling, TBML, courier hubs, money services businesses (MSBs), charities, and alternative remittance systems. These initiatives include:

- Operation Cornerstone, (founded in 2003 – a private industry partnership and aggressive outreach program) (http://www.ice.gov/cornerstone/).
- Operation Cornerstone detects and closes down weaknesses within U.S. financial, trade and transportation sectors that can be exploited by criminal networks. Law enforcement entities share criminal typologies and methods with businesses and industries that manage the very systems that terrorists and criminal organizations seek to exploit. This sharing of information allows the financial and trade community to take precautions to protect itself from exploitation. In return, ICE receives information to more thoroughly investigate these complex and sophisticated criminal schemes.

Inter-sectoral & cross border transaction data analysis

198. Cross referencing of trade data with that of trade finance is useful to discover trade anomalies which can in turn lead to TBML investigations. It is important that such anomalies are investigated in the light of information obtained from international trading partners. In 2004, the US ICE established a number of Trade Transparency Units (http://www.ice.gov/trade-transparency/) to combat TBML and other import–export crimes. These TTUs rely on data analysis of international trade patterns to identify potential TBML activities. The TTUs in the United States use the 'Data Analysis and Research for Trade Transparency Systems' (DARTTS), which allows investigators to view totals for merchandise imports and then sort on any number of variables, such as jurisdiction of origin, importer name, manufacturer name, and total value (US DHS 2010: 3). Through this, DARTTS identifies trade and financial transactions that are 'statistically anomalous based on known facts and user queries', rather than being used to 'predict future behaviour' or to 'profile' traders (US DHS 2010: 3) The data that DARTTS uses is collected from US Customs, the US Bureau of Census (where historical trade data is held), FinCEN and foreign government bodies, and consists of information gathered from those required to complete import–export forms (US DHS 2010). From this collection of data, three types of analysis are conducted by DARTTS:

- *International Trade Discrepancy Analysis* — US and foreign import/export data are compared to identify anomalies and discrepancies that warrant further investigation for potential fraud or other illegal activity.
- *Unit Price Analysis* — trade pricing data are analysed to identify over- or under-valuation of goods, which may be an indicator of TBML or other import–export crimes.
- *Financial Data Analysis* — financial reporting data (the import/ export of currency, deposits of currency in financial institutions, reports of suspicious financial activities and the identities of parties to these transactions) are analysed to identify patterns of activity that may indicate illegal ML schemes (US DHS 2010: 110).

199. When conducting this analysis, the TTU in the United States relies heavily upon information gathered from other countries.

CHAPTER IV - CASE STUDIES

200. Case studies best illustrate the complex and simple forms of TBML. The cases studies set out below, while being based upon the experience of various jurisdictions, present the facts in simplified manner, through narration and diagram, highlighting the modus operandi and red flags.

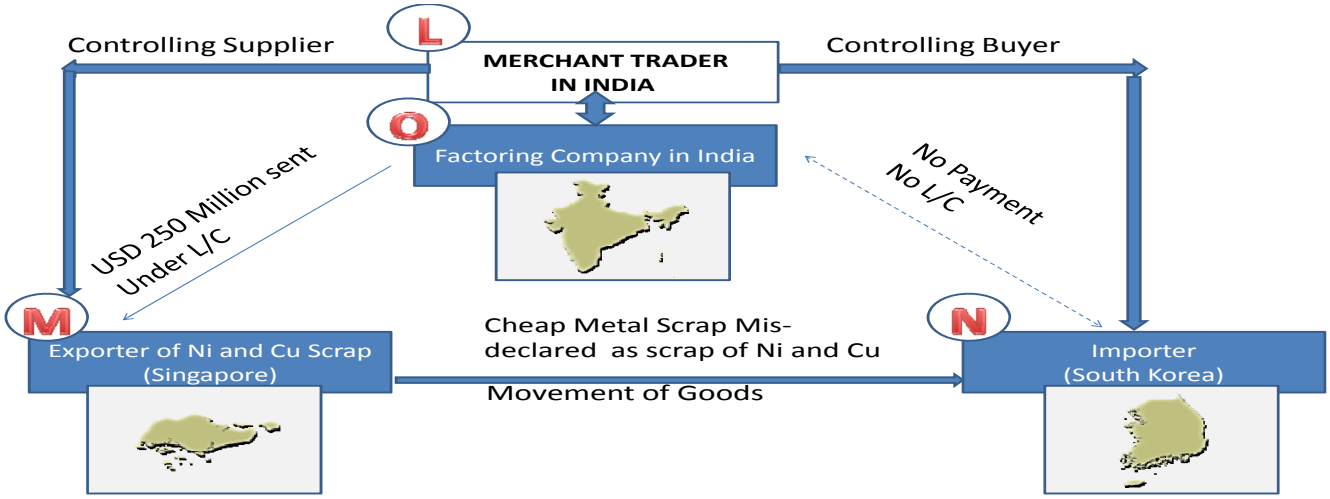
201. The FATF Paper 2006 on the TBML focused on trade based techniques used in TBML. The techniques which have been mentioned are over/under invoicing of goods, multiple invoicing of goods, over/under shipments of goods and false description of goods. Besides identifying these elements of trade that facilitate TBML, the seven case studies presented in this Chapter also bring-out the mechanisms of trade finance used in TBML.

202. The cases studies have been presented in four parts. The first part comprises the modus operandi in several simple steps. The second part demonstrates the essence of modus operandi though a diagram. The third part relates to giving comments on the case study so as to highlight the essential features. Finally, a list of red flags which can be inferred from the case study is included.

CASE STUDY 1 (Information provided by India)

- Company L located in India entered into a trade arrangement called merchanting trade with Company M located in Singapore and Company N located in South Korea.
- Trade arrangement required that Company L act as an intermediary between Company M and Company N.
- Trade finance arrangements required Company L to make payments to Company M and receive payments from Company N.
- Goods involved in the transaction i.e. “Nickel & Copper Scrap” were to be directly shipped from Company M to Company N.
- To secure payment for Company M, Company L got Letters of Credit (L/C) issued in favour of Company M (import leg).
- Company L entered into an agreement with Company O in India to get such Letters of Credit issued by Company O in favour of Company M for a charge of commission by Company O (for the import leg of the transaction).
- Company O secured receipt of payments for the export leg of the transaction (payment from company N) by obtaining bonds and guarantees furnished by Company L.
- On the advice of Company L, Company O opened L/Cs in favour of Company M as & when Company M directly shipped scrap consignments to Company N.
- Company M on shipment of the goods to Company N, got such Letters of Credit discounted with the bank.

- For the initial shipments, Company N accepted the goods and made payments to Company L. For payments made through Letters of Credit by Company O to Company M, Company L compensated Company O through payments received from Company N.
- After the successful completion of the initial rounds of transactions, Company N defaulted on payments to Company L even though the Letters of Credit opened by Company O at the behest of Company L in favour of Company M had already been discounted by Company M.
- The trade finance arrangement for the import leg of the transaction was completed between Company M & Company O by way of payment to beneficiary (Company M) but for the export leg of the transaction, due to non-acceptance of goods by Company N, no payment was received from Company N to Company O through Company L.
- On investigations it was found that Company L was in league with Company M & Company N. Company O was left with heavy losses.
- Predicate offences of cheating and criminal conspiracy were involved and merchanting trade and its finance arrangements were used to launder the criminal proceeds.



Commentary:

203. This case study reveals the misuse of trade and trade finance to generate proceeds of crime and to launder funds. Unlike conventional methods of laundering the money in which generally, the proceeds of crime is structured into the financial system, in this case proceeds of crime were generated through mis-declaration of the goods, forgery of trade documents and the introduction of a third party in a jurisdiction other than the two trading countries. The techniques deployed to indulge in TBML were mis-declaration of goods and related party transactions which were not independent corporate structures.

204. In this case study, Letters of Credit (trade finance) were arranged only for the import leg of the transaction and not for the export leg. Thus trade finance mechanisms became

vulnerable to laundering the criminal proceeds. The lack of proper due diligence by the factoring company in assessing and acknowledging the risks and the lack of duty of care by banks in undertaking the proper scrutiny of the documents facilitated the commission of crime and TBML.

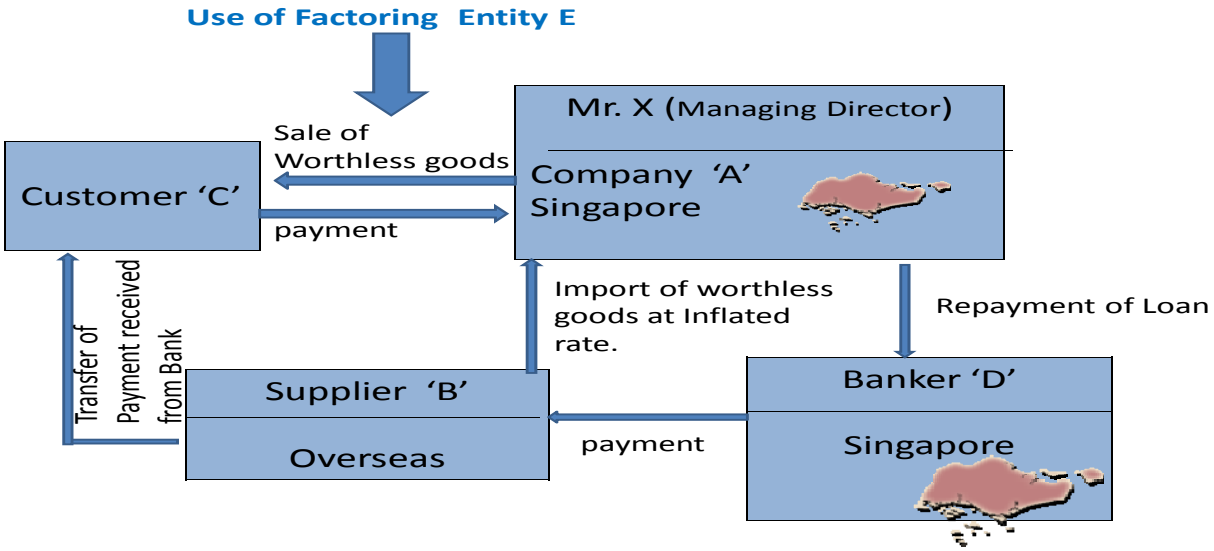
Red Flags

1. Mis-declaration of the goods - both of quality and type.
2. The third party located in a third jurisdiction acted as an intermediary, even though goods were in fact capable of being supplied from one jurisdiction to another jurisdiction directly.
3. Both supplier and buyer of the goods are related to the intermediary or the buyer and /or the seller all belong to the same group of companies.
4. Risk exposure of the factoring company was not commensurate with expected norms.
5. Intermingling of different types of trade finance arrangements for different segments of trade transactions.

CASE STUDY 2 (Information provided by Singapore)

- Mr X was the managing director of a Company A listed on a stock exchange outside Singapore. Company A indulged in trade of integrated circuit chips.
- In 2001, Company A began experiencing cash flow problems due to an industry downturn.
- Mr. X tied up with Supplier B located abroad and Customer C to collude in a fraudulent scheme.
- Overseas Supplier B supplied worthless goods to Company A and raised grossly inflated invoices.
- Company A submitted trade credit applications to Banker D for disbursing invoiced value to Supplier B.
- Supplier B then transferred the funds corresponding to the inflated value to Customer C.
- Company A then “sold” these worthless goods to Customer C again at inflated value.
- In order to realise the invoiced value of the goods “sold” to its accomplice Customer C before the expiry of the credit period, Company A discounted the invoices raised to Customer C with Factoring Entity E.
- The payment received by Company A was then used to repay the trade credit which it had obtained from its Banker D.
- The Customer C paid the factoring company when the credit term was due.
- Through this scheme, Company A and its accomplice suppliers and customers defrauded various banks and a factoring company into disbursing funds.
- Mr X was charged with cheating offences for his role in defrauding bankers and the factoring company.

- Mr. X had also exploited the international trade system to channelize the disbursements from Singapore back to Company A after a series of cross border sham purchases / sales involving the same worthless goods.



Commentary:

205. In this case study, international trade was mis-used to fraudulently obtain funds from banks and from a factoring company and launder proceeds through trade channels. By resorting to cross-border transactions, it became easy to deceive the banks and the factoring company as it is generally difficult to verify the genuineness of the other end of the international trade transactions pipeline. Further, by using accomplice suppliers and accomplice customers, the entire movement of mis-declared goods was fully controlled by the main person Mr. X and thereby it escaped detection for six years. The trade finance channels of the bank, trade credit, open accounting and factoring were all used to circulate the funds.

Red Flags

1. Mis-declaration of value (over-valuation) of goods.
2. Series of cross border transactions in the same goods between related companies.
3. Use of factoring companies to finance trade transactions between related companies.
4. Despite an industry-wide recession, the ability of a company to generate large funds from trade.
5. Direct payment through open accounting from banks to overseas suppliers on trade credit application of the domestic trader.

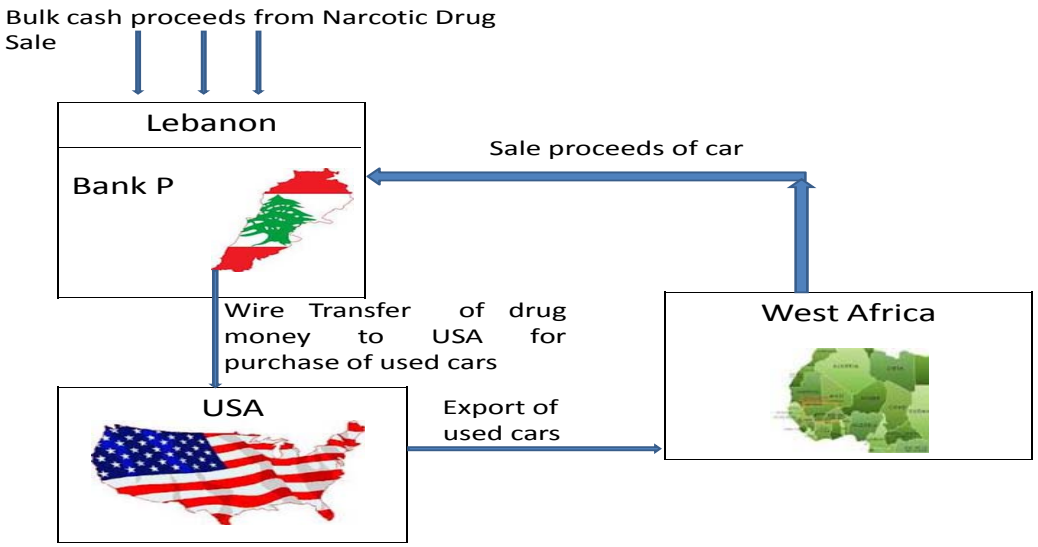
CASE STUDY 3 (Information provided by USA)

206. Authorities in US had information that Bank P in Lebanon had been extensively used by an international drug trafficking syndicate controlled by individual Q for moving the proceeds of narcotics sales through TBML across the globe.

- The syndicate smuggled narcotics from South America to Europe and to the Middle East through West Africa.
- The kingpin Q of the syndicate organised shipments of 100 Tonnes of Cocaine from South America and laundered the proceeds of up to US $ 200 Million per month, obtained from the sale of cocaine in Europe and Middle East.
- Proceeds of drug trafficking were moved and laundered through-
    1. bulk cash smuggling (cash couriers) ;
    2. use of exchange houses including one owned by Q.
    3. use of accounts of family members of "Q" in several branches of Bank P ;
- Bulk cash deposits were made by Q and his associates into exchange houses which in turn deposited the money into several accounts maintained in Bank P.
- In fact Q owned and controlled one of the exchange houses located in the same building as a branch of Bank P. Certain employees of Bank P were in league with Q.
- Two distinct TBML schemes were used by the syndicate to move and launder illicit funds through trade.

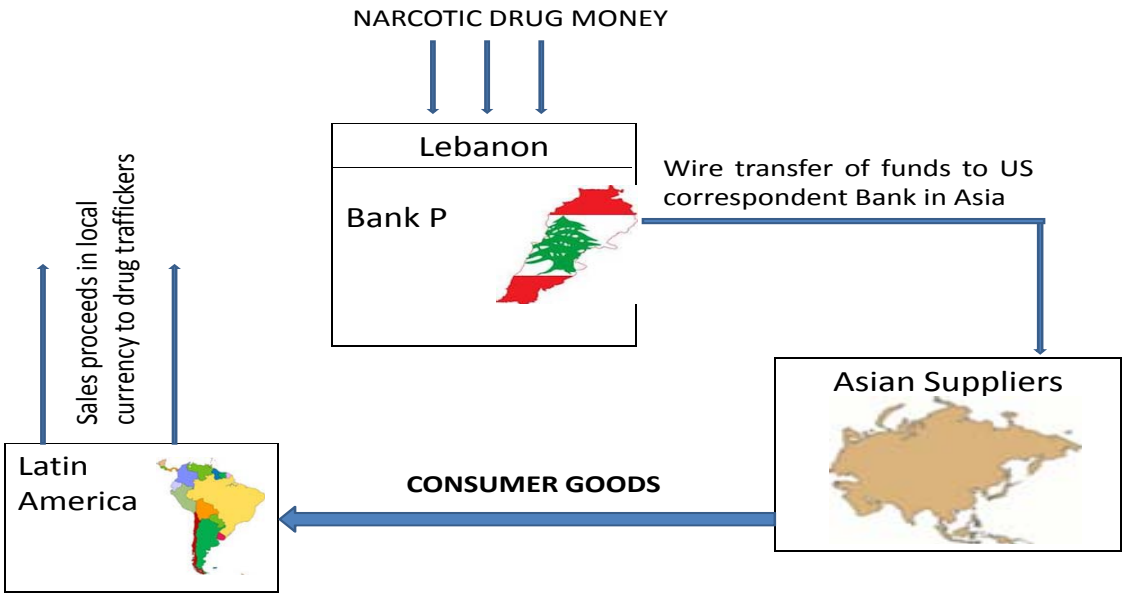
SCHEME A

- In the first scheme, wire transfers from Bank P were sent to banks in U.S. for the purchase of used cars in the U.S.
- The car dealerships were operated by individuals who had been separately identified in drug-related investigations.
- The recipients of these funds purchased vehicles in the United States, which were then shipped to countries in West Africa and elsewhere.
- The proceeds generated from sale of used cars were ultimately repatriated back to Lebanon.
- The money generated from illicit drug trade was thus fully integrated into the financial system through TBML scheme involving trade in used cars.



SCHEME B

- In the second scheme, Individual R, who owned a wide network of companies which were dealing in consumer goods in Asia and in other regions provided consumer goods for TBML.
- Although based in Asia, individual R had centralized his banking operations in Lebanon, particularly through the use of over 30 accounts at Bank P.
- Individual R received funds in his accounts from the kingpin Q and R also exchanged funds with the Latin American members of the drug syndicate.
- In the TBML scheme used by them, the proceeds generated in local currency from the sale of imported consumer goods were deposited in individuals' accounts in the local banks.
- This completed the Latin America-based Black Market Peso Exchange ML cycle, and allowed for the repatriation of proceeds for the Latin American drug producers.



Commentary:

207. The proceeds of narcotics drug money were first placed into the financial system of a jurisdiction where the AML regime was not adequately strong. The syndicate targeted jurisdictions where the AML regime may not have been as strong as Europe. The criminal syndicate was able to influence individuals on the operations of its bank as well as those of the exchange houses. The proceeds of drugs was layered and moved through the use of international trade. Round tripping of the money and its laundering occurred through abuse of trade and trade finance (open accounting system). Interestingly, both the TBML schemes were being operated concurrently and funds were moving between the two schemes, by use of the Money Exchange House established by Q.

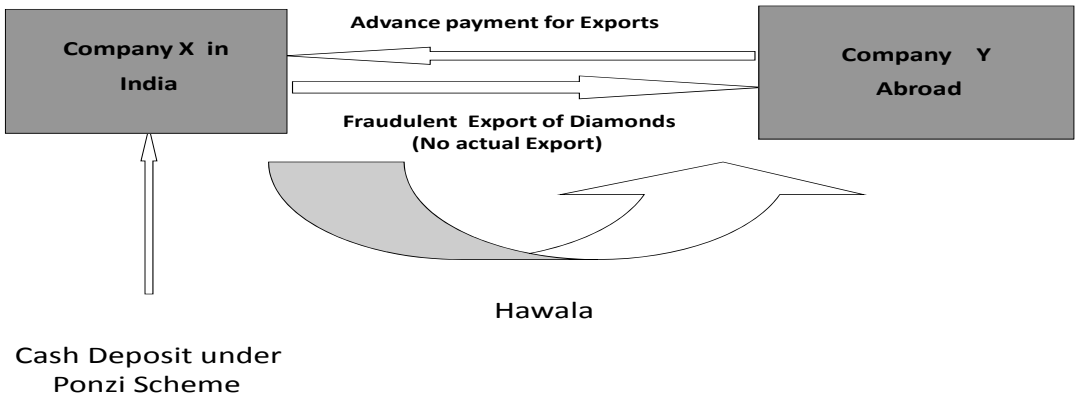
Red flags

1. Trade in commodities like used cars and consumer goods for which valuation can be manipulated.
2. Payment for imports received from banks located in a third jurisdiction, whereas goods are traded between two other countries.
3. Cash deposits made in bulk in certain bank accounts from high risk customers like exchange houses.
4. Cross border wire transfers from sensitive jurisdictions without adequate explanation of the considerations involved for such transfers.

CASE STUDY 4 (Information provided by India)

208. Company X located in India received advance remittance from Company Y located in foreign jurisdiction for a promise to export consignments of diamonds.

- Company X filed falsely declared and forged documents with the bank to show the overvalued exports of diamond without having made any shipment.
- To give a colour of authenticity, Company X also fabricated purchase invoices to show local purchases of diamonds, whereas no purchases of diamonds had actually ever taken place.
- Company X received export payments through trade finance arrangements via an open accounting system from Company Y.
- Company X had received substantial cash deposits in India from the public on the promise of high returns via a fraudulent Ponzi Scheme.
- Company X transferred large amounts of public deposits to company Y through hawala (Alternative Remittance System).
- Company X indulged in round tripping by receiving back as export earnings the financial value which it had transferred abroad as hawala.
- Predicate offences of cheating, criminal conspiracy and forgery of documents occurred.



Commentary:

209. In this case, the proceeds of crime were generated through the fraud perpetrated on general public under a Ponzi scheme which was then laundered through fraudulent and bogus exports. Such proceeds of crime were transferred abroad through alternative remittance system. Money was received back from abroad through banking channels as export

remittance. Round tripping of money and its laundering occurred through TBML. Company X had a network of associate companies established in many jurisdictions abroad. In this case, on the trade side, overvaluation of export goods and under shipment (no shipment) of goods was done. Proceeds of Crime were moved abroad by using alternative remittance system (hawala) and then round tripping occurred through open accounting system.

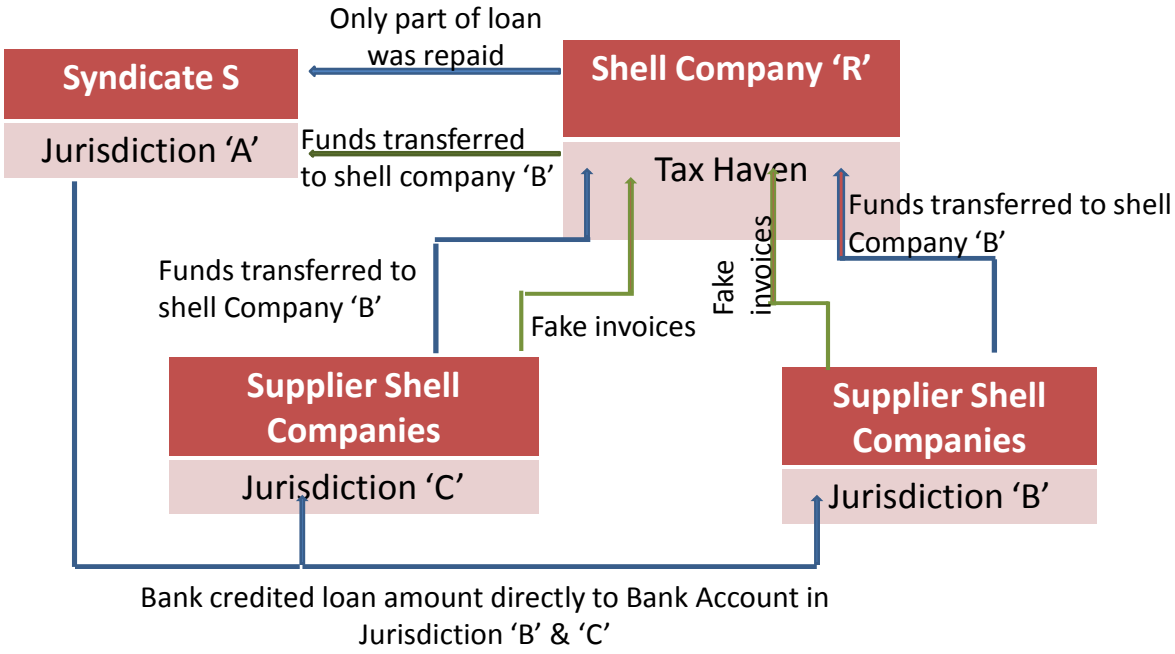
Red flags

1. Export of goods without any corresponding purchase of raw materials or finished goods.
2. Sudden increase in volume of exports by a new exporter.
3. Advance inward remittance against exports without justifiable reasons.
4. Export documents which are not duly authenticated by export regulating agency were accepted by the bank.

CASE STUDY 5 (Information provided by Macao, China)

210. Criminal Syndicate S had a regional base in Jurisdiction A.

- Syndicate S registered a Shell Company R in a tax haven jurisdiction.
- Syndicate S set up a number of "supplier" shell companies in Jurisdiction B and Jurisdiction C.
- Syndicate S opened accounts in more than 10 banks in Jurisdiction A and applied for high value loans.
- Shell Company R claimed that the company dealt with cross-border trading activities, and thus purchased goods from Supplier Companies in Jurisdiction B and in Jurisdiction C.
- Shell Company R obtained trade credit from the banks in Jurisdiction A on the strength of invoices for the purchases made from Jurisdictions B & C.
- The banks in Jurisdiction A directly credited loan amounts at the behest of Company R into the bank accounts of the "supplier" shell companies in Jurisdiction B and in Jurisdiction C.
- On receipt of funds the "supplier" shell companies immediately transferred the funds through a circuitous route to Shell Company R and to other accounts controlled by Syndicate S.
- Shell Company R used the funds for part repayment of loans.
- The fake transaction cycle engendered outstanding non-performing loans for banks in Jurisdiction A.



211. **Commentary**: In this case study, it is observed that cross border trade was mis-used by a criminal syndicate to move value between shell companies located in different jurisdictions. There was use of a Tax Haven jurisdiction to take advantage of relaxed AML regime and to avoid detection. The veneer of international trade was created to conceal collusion among related companies located in different jurisdictions. The trade finance mechanism of raising bank loans (trade credit) against fake invoices could occur due to limitations to verify the credibility of overseas suppliers. Wire transfers made to such related suppliers resulted in losses to banks. Thus a Criminal Syndicate could indulge in TBML in the absence of cross-verification of trade data and financial data.

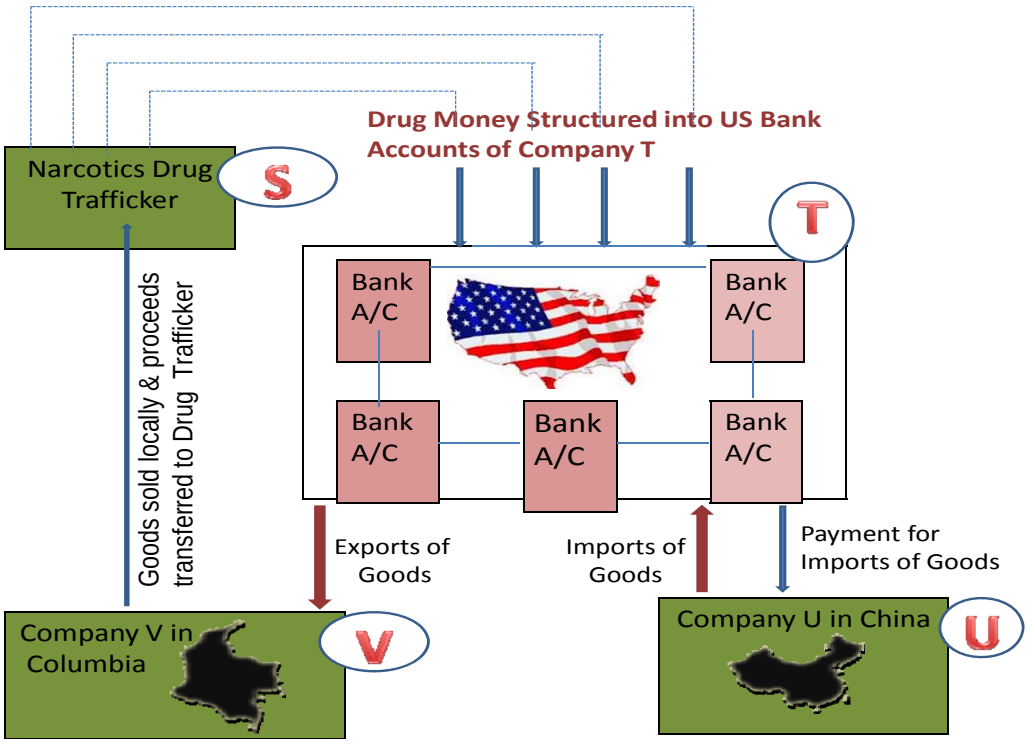
Red Flags

1. Use of corporate structure of shell companies located across the jurisdictions.
2. Registration of a trading company in a tax haven even though its business relates to another jurisdiction.
3. Mismatch between trade documents like bill of lading, import bill, invoices and trade finance documents (trade credit applications).
4. Direct payments by banks to overseas suppliers who are related parties without adequate verification of the authenticity of such suppliers and without verifying trade transactions.

CASE STUDY 6 (Information provided by USA)

212. Toy Company T of Los Angeles, USA was receiving cash generated from trafficking of narcotics by Columbian drug cartel S.

- Company T received such cash by two methods - in some cases, people affiliated with drug traffickers simply dropped cash at the company offices in downtown Los Angeles; the second method involved cash deposits made directly into Company's bank account, sometimes by individuals located as far away as New York.
- During the four-year period, the investigation tracked more than $ 8 million in cash deposits into the accounts of the Company T, and not a single transaction was for more than $ 10,000.
- The bank accounts of Company T, were used to pay for import of toys into USA.
- The toys, viz. stuffed animals, including teddy bears and Topo Gigio dolls, were imported from Company U in China.
- The toys imported into US from China were again exported from the U.S. to Company V in Colombia.
- The Colombian pesos generated by the sales of toys by Company V were then used to reimburse the Colombian drug trafficker.
- TTU Colombia was deployed to investigate shipments of toys.
- The TBML investigation brought out structuring transactions to avoid reporting requirements, bulk cash smuggling and intimidation of witnesses. In addition, the toy Company T was charged with conspiracy to launder money.
- Five persons, including two owners of the Company T and a Columbia-based businessman were convicted and fined.



Commentary:

213. Cash obtained from the trafficking of narcotics was first structured into financial system through smurfing. Money was then used to import toys, thereby converting the proceeds of narcotics trafficking into goods. The imported toys were then re-exported to move that value to the desired jurisdiction, in lieu of the value of narcotic drugs. Thus international trade was used for layering and integrating the crime money and to disguise its illicit origin.

Red Flags

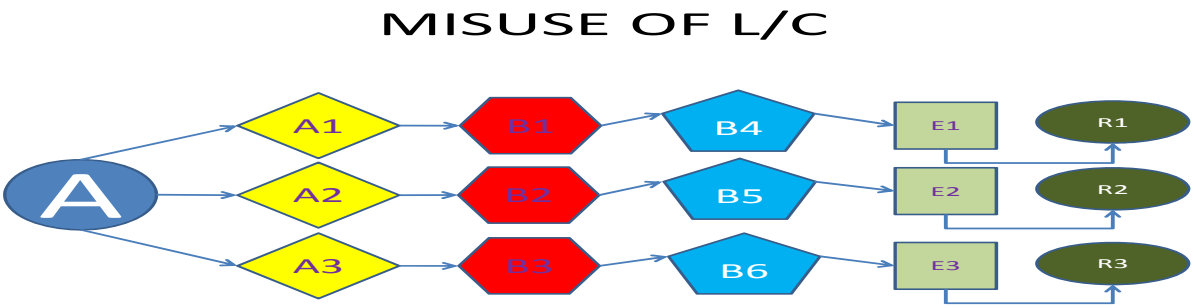
1. Payment for import is made through multiple accounts.
2. Credits into such accounts were made mostly through structured cash deposits, i.e. through smurfing.
3. Re-export of goods to sensitive jurisdictions.
4. Inadequate consideration received for re-exported goods.

CASE STUDY 7 (Information provided by India)

214. This is a complex case which involves multiple techniques of ML by misuse of trade as well as trade finance mechanisms. The kingpin of this ML racket, called "A" in this case study, was laundering funds for Narcotic Drug cartels in Asia and South America using various techniques including cash couriers, money service bureaus, alternate remittance system (hawala) as well as through formal mechanisms of trade finance.

A. MISUSE OF LETTERS OF CREDIT (DOCUMENTARY CREDIT)

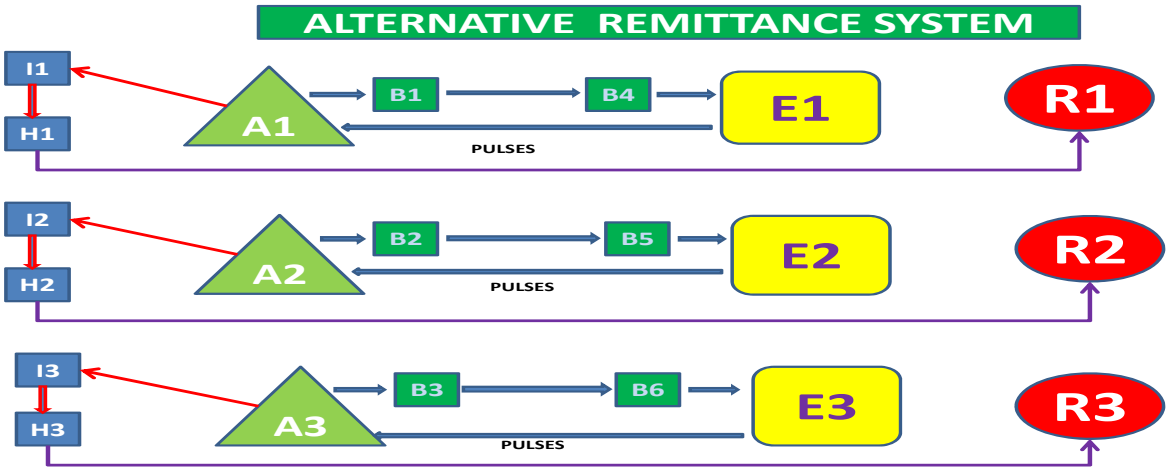
- An Indian national "A" was based in Dubai and had established a number of companies there, say A1, A2, A3.
- He also had a network which spread across many countries in Europe, Asia, Africa and USA.
- In Dubai, he got Letters of Credit (L/Cs) opened by various companies A1, A2 & A3, which were controlled by him, for Importers I1, I2 & I3 in Dubai.
- Exporters E1, E2 & E3 in India, as well as in other parts of the world, were the beneficiary parties for these L/Cs.
- For opening of L/Cs, "A" used his networking with Issuing Banks (B1, B2 & B3), who tied up with the Advising Banks (B4, B5 & B6). Advising Banks were responsible for transmission of funds into accounts of Exporters E1, E2 & E3.
- L/Cs were opened for amounts substantially higher than the real value of the actual consignments being traded.
- "A" arranged for trade documents to be prepared so as to make such documents acceptable to the Issuing Banks B1, B2 & B3 and Beneficiary/Advising Banks B4, B5 & B6.
- "A" in turn remitted the inflated value of exports to Exporters E1, E2 & E3 in India, as per the terms of L/Cs, after adding the drug money lying with him. Funds remitted to India were as per the terms of the L/C.
- After receiving the higher remittances, the Exporters E1, E2 & E3 retained the actual price of the goods exported and transferred the additional amount to the family members (R1, R2 & R3) of "A" in India and to his associates in other parts of the world.
- In a slight variation of this technique of misuse of L/Cs, "A" facilitated opening of L/Cs for importers (I1, I2 & I3), for commission. The L/Cs were opened at inflated values. He collected fair value of imports from the importers but remitted the inflated L/C amount of higher value to the Exporters E1, E2 & E3. The additional funds thus transferred were collected from Exporters, by associates of "A"
- Thus, by misuse of Letters of Credit, funds were moved across countries, in the guise of trade finance, after intermingling of drug money of criminal origin.



B. USE OF ALTERNATIVE REMITTANCE SYSTEM

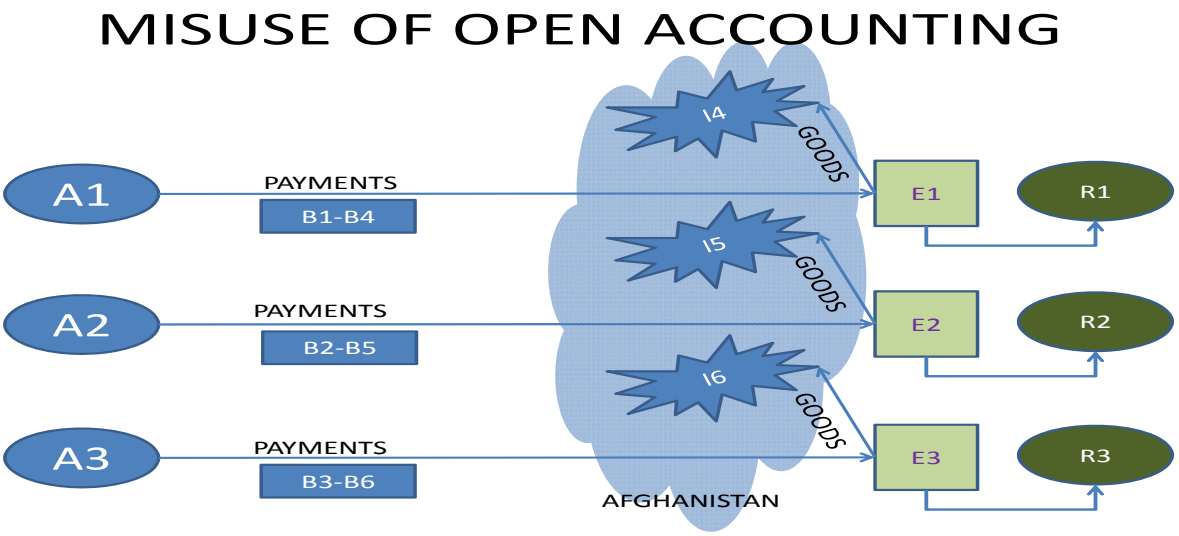
- "A" also utilised the services of alternative remitters (hawala operators) to move funds offshore.
- The legal framework in Dubai allows hawala to operate after registration with the UAE Central Bank.
- One way of use of Alternate Remitters by "A" was by funding those individuals who were visiting Dubai and were in need of funds in local currency, which he provided.
- The flush of money arising from the narcotics trade was enough to cater to large demands of individuals as well as of companies.
- On return to their home jurisdiction, these individuals made compensatory payments to the assigned agents of "A" located in their home jurisdiction, in currency of their home jurisdiction, thereby completing the clandestine movement of funds from Dubai to the home jurisdiction of these individuals.
- In another technique of use of Alternate Remitters, "A" facilitated trade in prohibited / restricted goods by falsifying trade documents by using his network of associates in India. Fake documents were prepared to fraudulently export pulses from India, when such exports were banned.
- To circumvent the restriction, the goods were mis-described in trade documents, which also enabled mis-declaration of value and thereby also enabled movement of excess funds to the exporting jurisdiction.
- He used alternative remitters (Hawala operators) H1, H2 & H3 to settle differential payments arising out of such trade in prohibited / restricted goods.
- Through the companies A1, A2 & A3 controlled by him, "A" first imported pulses into Dubai and made payments of contractual price to Exporters E1, E2 & E3, through banking channels / through L/C.
- Through his companies A1, A2 & A3, he resold the imported pulses at higher prices to the real importers I1, I2 & I3, who were in fact the genuine buyers of pulses in Dubai and elsewhere.

- Since A had pre-dated the contracts to allow for export of pulses from India after ban, he earned huge profits on resale in foreign market facing shortage of pulses.
- Profits earned on resale of pulses were also remitted to his agents R1, R2 & R3 through Alternate Remitters (Hawala operators) H1, H2 & H3.



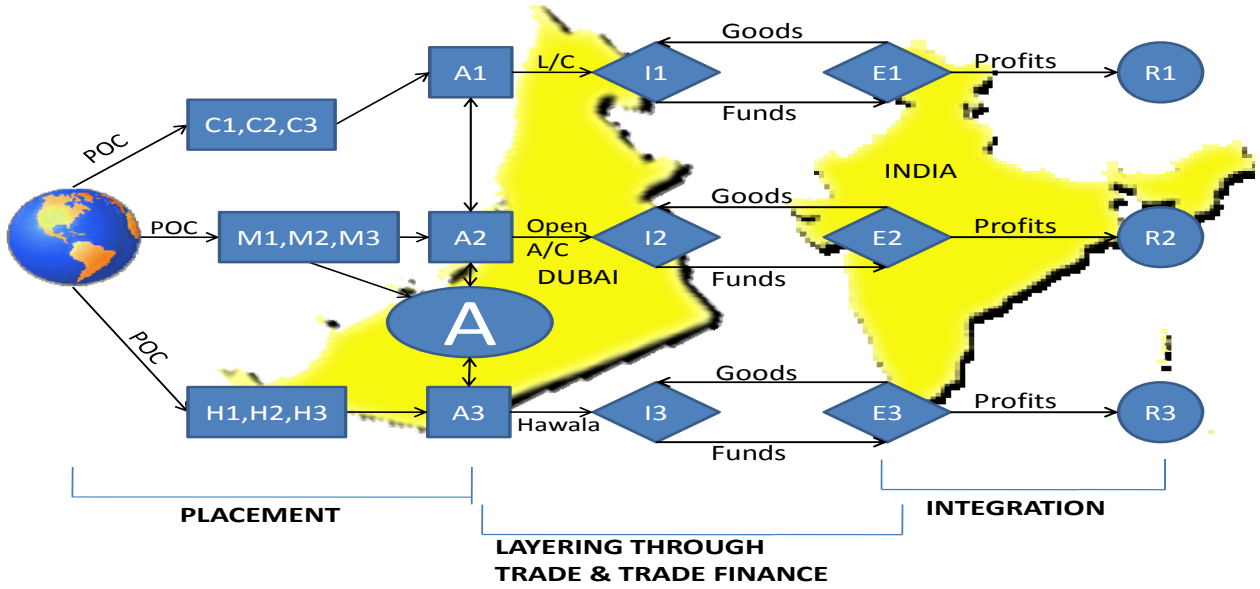
C. USE OF OPEN ACCOUNT

- "A" organised exports of artificial jewellery from India to various importers (I4, I5 & I6) in Afghanistan.
- Companies A1, A2 & A3 established in Dubai by "A" were declared as 'Notifying Parties' in trade documents for exports from India to Afghanistan.
- Payment was sent by A1, A2 & A3 through banks B1, B2 & B3 in Dubai to the accounts of Indian exporters E1, E2 & E3 in banks B4, B5 & B6 in India.
- The Indian exporters having received payments through open accounting paid the commission in cash for such exports to the agents of "A" in India, viz. R1, R2 & R3.
- Thus, in exchange for drugs originating from Afghanistan, "A" arranged for delivery of goods in that jurisdiction, by indulging in countertrade through trade manipulation.
- "A" used his companies A1, A2 & A3, by declaring them as 'Notifying Parties' in the trade documents to facilitate misuse of the trade finance mechanism of open account trading.



215. As stated at the outset, "A" was operating a very complex scheme of TBML, which can be summed up as follows:

- "A" indulged in laundering of proceeds from Narcotics trafficking and was based in Dubai. He opened a number of associate companies (A1, A2 & A3) to place money into the financial system by using the services of Cash Couriers (C1, C2,& C3) or Money Service Bureaus (M1, M2 & M3) or Alternative Remitters or Hawala Agents (H1, H2 & H3).
- To remit part of the proceeds of crime to his home in India, he tied up with Indian exporters (E1, E2 & E3).
- The Indian exporters (E1, E2 & E3) overvalued the exports to earn export incentives. The individual "A" used letters of credit, open accounting as well as alternative remittance system for movement of money between importers (I1, I2 & I3) and the Indian exporters E1, E2 & E3.
- The actual importers / users situated in the same jurisdiction as "A", collected the goods exported from India and paid to "A", the actual cost (true value) of the goods so imported.
- "A" in turn remitted the inflated proceeds of exports either against the L/Cs opened in the names of Importers (I1, I2 & I3) OR through open account OR through alternative remittance system to Indian Exporters (E1, E2 & E3).
- After receiving the higher remittances, the Exporters (E1, E2 & E3) retained the actual costs and conveyed the additional amounts to the associates (R1, R2 & R3) of "A" in India or elsewhere.
- The Exporters (E1, E2 & E3) gained from excess export incentives on overvalued exports and from being able to export banned goods and to inaccessible destination. The importers gained by acquiring goods which were not available through normal trade channel.
- "A" succeeded to launder criminal proceeds through trade finance.



Commentary:

216. In this complex case study, the funds originated from narcotic drug sales and fraudulent export incentives. The proceeds of crime were laundered by mis-declaration of description of goods and forgery of documents.

217. In the first illustration, the misuse of Letter of Credit mechanism of trade finance to disguise the movement of criminal funds in conjunction with overvaluation of goods, where both exporter as well as importers were in league, has been depicted.

218. In the second illustration, use of alternative remittance system (Hawala) has been explained, wherein funds were moved in connection with trade in prohibited / restricted goods. Using the international trade system, the criminal organisation was able to transfer illegal funds by using trade transactions to justify payment through the financial system.

219. In the third illustration, criminals have mis-used the open account trade finance system to launder the crime money. Movements of funds were disguised by using the third party remittance system. Mis-declaration of goods, over-valuation of goods and barter of goods were deployed, coupled with misuse of trade finance mechanisms of L/Cs and open account trading. Extensive use of Alternate Remitters was also resorted to move funds illegally across countries, at will.

Red Flags

1. Trade in banned/prohibited/restricted goods.
2. Overvaluation of export goods.

3. Exports to sensitive destinations of a new commodity by a regular exporter of some other commodity.
4. Introduction of notifying parties in trade documents without adequate explanation.
5. Export Remittances received from third parties.
6. Settlement of accounts for trade between two countries through a third jurisdiction.
7. Movement of abnormally large sums of money in various accounts of the individuals and companies which are not related to the nature of their business.

ALTERNATIVE REMITTANCE SYSTEMs:

220. Some of the case studies have referred to Alternate Remittance System. Therefore a brief write-up on Alternative Remittance System by Bangladesh in the box placed below explain the basic features of such a system whereby accounts are settled across the nations through compensatory payments made in local currency of trading partners for differentials arising between true value of goods involved in trade and formal means of trade finance.

ALTERNATIVE REMITTANCE SYSTEM

Alternative Remittance System i.e. "Hundi" or "Hawala" is a way to transfer funds through informal channels. Hundi means "trust" and hawala means "transfer related to money". These are also often referred to as "underground banking system" or "parallel banking system" or "informal money transfer system". Alternative remittance systems are financial services, traditionally operating outside the conventional financial sector, where value or funds are moved from one geographic location to another. (FATF Best Practice Paper 2006: Combating the abuse of Alternative Remittance System http://www.fatf-afi.org/media/fatf/documents/recommendations.)

Under-invoicing / over invoicing of goods and services are used in TBML to move funds across the borders not only to disguise its illicit origin but also to evade taxes and duties as well as get undue export incentives. To settle such over or under payments in international trade transactions, Hundi or Hawala mechanisms are used.

Hawala Operators (Hawaldars) or Hundi Dealers operate their business under a global network which helps them to do their business worldwide. Generally Hawala Operators or Hundi Dealers have other formal businesses, like exchange houses, travel agencies, import/export or shipping companies, grocery stores, gold and jewellery shops, textile or apparel shops and many other business establishments. Often these operators arrange fund transfers for a large number of migrant workers and immigrants, who send back their savings to the home jurisdiction. The popularity of their business lies in 3 C's viz. certainty, convenience and cheap. The transactions ensure that remittance reaches the beneficiary at an assigned address in definite time period, for a charge which is less than the transfer charges of formal system. Moreover the accounts among the Alternative Remittance System operators are settled by making compensatory payments in local currency to persons in the home jurisdiction who have been assigned by the partner hawala operator located abroad.

Since such hawala transactions remain largely unreported, there is no reliable data available on the magnitude of hawala / hundi / other alternative remittance systems. The significance of this trade finance mechanism as means to fill up the gap arising out of difference in actual trade value being exchanged and the amount transferred through formal mechanisms call-for larger awareness and focused training on the subject of Alternative Remittance System.

CONCLUSIONS

221. The first case study relating to 'merchanting trade' reveals how a third party located in a third jurisdiction ostensibly to facilitate trade between two other countries introduces TBML vulnerability in such trade transactions. The financing of different segments of trade through diverse mechanisms of trade finance can introduce risks in the trade transactions which are difficult to assess by financial institutions.

222. The second case study brings-out how the 'carousel trade' with the circulation of the same goods across the countries, call for close scrutiny of such transactions, for TBML. The mechanisms of financing trade through factoring and through disbursement of trade credit to overseas suppliers are fraught with risks for financial institutions unless due diligence is exercised about the overseas trading partner.

223. The third case study reveals how proceeds of crime can move to a jurisdiction where the AML regime may have weaknesses. It also shows the vulnerability arising from trade finance mechanisms in a system wherein the integrity of financial institutions has been undermined by weak application of fit and proper controls. The operations of 'exchange houses' owned and controlled by criminals coupled with 'compromised' working of a bank make trade finance mechanisms means for indulging in TBML.

224. The fourth case study demonstrates how proceeds of crime generated out of a 'ponzi scheme' were moved abroad though a variant of alternative remittance system viz. hawala. The TBML allowed for integration of proceeds as legal remittance.

225. The fifth case study reveals how the creation of veneer of international trade can help conceal the identity of true beneficiary from the financial institutions. The use of a corporate structure of shell companies located in sensitive jurisdictions of a tax haven can hoodwink the institutions of trade finance.

226. The sixth case study demonstrates yet another variant of alternative remittance system viz. Black Market Peso Exchange. The use of international trade acts as a lubricant to facilitate the cycle of laundering of narcotic drugs funds.

227. The seventh case study shows multiple forms of international trade and various mechanisms of trade finance which give inherent flexibility to criminals to adopt those forms and types which suit the demands of a situation. Such adaptability of these forms makes the detection and prevention of TBML a very challenging task.

228. The FATF Paper 2006 highlighted four basic techniques of TBML. These basic techniques relate to abuse of trade transactions and combine with techniques which abuse trade finance mechanisms for TBML to occur. Four of the trade finance techniques which can be inferred from the analysis in this Paper are following:

    a) **Cash Inflow Based Payment:** Cash is structured into formal financial system through smurfing and other processes so as to make payments for international trade transactions. Trade finance payments are funded out of cash receipts of the financial institutions.

Normally cash will be received in one jurisdiction and payment through trade finance mechanisms will be made in the jurisdiction of trading partner. Thus the veneer of international trade is used to obliterate the signs of illicit origin of the payments.

b) **Third Party Payment:** A third party is introduced preferably in a third jurisdiction, in the payment channel between two trading partners. Such third party may be a notifying party between consignor and consignee. It can also be a facilitator who acts as an intermediary for trade transaction as well as for trade finance mechanism. In still other situations such third party may either be a factoring or forfaiting entity. The technique involves making the process of due diligence to be conducted by domestic financial institutions more difficult to succeed.

c) **Segmental Modes of Payment:** Instead of opting to finance single trade transaction as a whole, the trade transaction is split into parts so that each part is financed through different modes of trade finance. The segmental modes of trade finance are used to fund the trade transaction. This technique is normally used wherein a third party is brought in between the exporter and the importer. For imports of goods, letters of credit mechanisms may be used and on the re-export of such goods to other jurisdictions wire transfers may be opted. The technique introduces different levels of risks for different segments of trade so that financial institutions are unable to make correct risk assessment of the trade finance payments.

d) **Alternative Remittance Payment:** Trade transactions which are vulnerable to TBML involve transfer of goods of which the true value does not correspond to the amount of payment transferred through formal mechanisms of trade finance. To finance such gap the alternative remittance mechanisms are utilized. The technique involves 'squaring-off' the 'differential gaps' by making compensatory payments in local currency to domestic persons assigned by the trading partner located abroad.

229. The techniques of trade finance abuse succeed only when they work in conjunction with the techniques of abuse of trade transaction. The segregation of sectors of finance and of trade prevents investigators from having an integrated approach. Isolated sectoral outlooks fail to raise 'alerts' about the TBML.

CHAPTER V - CONCLUSIONS

CHALLENGES

Growing Concerns

230. This study on TBML, done six years after the landmark FATF Study of 2006, has reaffirmed the conclusion of the earlier study that TBML is an important channel for criminal organizations and terrorist financiers to move money or value to disguise its illicit origin and to integrate it into the formal economy. The rapid growth in the global economy has made international trade an increasingly attractive avenue to move funds through goods and services. There are instances brought out in this Paper where the veil of international trade was deliberately created so as to launder the proceeds of crime. A number of publications on TBML during the intervening period of six years, as reviewed in Chapter-I, reflect the growing concern about its potential as a form of ML.

231. While various jurisdictions may have different levels of preparedness for identifying and investigating TBML, the general recognition of its existence and of its future potential underscore its significance. In fact, international trade remains a viable option for movement of value even in those jurisdictions that do not have a well-developed financial or banking sector. Thus, TBML is a concern for the international community even though it may presently impinge upon various jurisdictions without the same impact.

Complex Phenomenon

232. TBML is a complex phenomenon since its constituent elements cut across not only sectoral boundaries but also national borders. The dynamic environment of international trade imparts inherent flexibility for TBML to take multiple forms. To discern TBML from among the legitimate activities of international trade has become a daunting task. The features of the dynamic environment that also distinguish TBML from other forms of ML were identified in Chapter I. Such features include occurrence of TBML through intermingling of the trade sector with the trade finance sector in cross-border transactions. The foreign exchange market and the long supply chain make international trade more vulnerable to TBML.

233. To assist in recognizing the multiple forms of TBML, Chapter II of this Paper has enumerated specific characteristics of TBML. These attributes of TBML have been categorized into those relating to trade finance and to trade. For further simplification trade characteristics have been classified into four groups, namely: jurisdictions; goods; corporate structures; and, predicate offences. This methodology has allowed the Project Team to identify some ‘Red Flags’ which relate to specific characteristic of TBML.

Statistics and Data

234. Very few cases of trade base ML were reported. Thus statistics on detection of TBML and on TBML related STRs were also very limited. One of the major obstacles in devising future strategy to tackle TBML has been the lack of reliable statistics relating to it. Most jurisdictions do not distinguish TBML from other forms of ML. Hence they have reported that they do not maintain separate statistics for TBML. Moreover, the data on trade which

is largely collected by the Customs Department in most of the jurisdictions are oriented to serve purposes other than those of TBML. While the trade data is collected, maintained and analysed by the Customs they neither have a legal mandate to undertake TBML investigations nor do they have training and competence to utilize such data to combat TBML. Merely 25% of the jurisdictions have reported that TBML investigations were initiated on the basis of trade data.

235. As already pointed out in this Paper any strategy that focuses only on the trade sector leaving-out the corresponding elements of the trade finance sector would be inadequate to tackle TBML. Having a warehouse of trade finance data within financial institutions without correlating such data to that of the trade sector will not allow effective targeting of TBML. The Project Team holds that an isolated sectoral approach has not worked. An integrated holistic strategy to fight TBML is needed.

Sharing of Information

236. It is evident from the feedback from most of the jurisdictions that sharing of the information obtained domestically and internationally, has impediments. These impediments relate to inadequate and delayed response, restrictions on the use of the information furnished and insistence on confidentiality or secrecy clause which hamstring its evidential value. More than 50% of the jurisdictions reported having initiated TBML investigations on referrals from other agencies. Again, more than 50% of the jurisdictions reported seeking information from foreign jurisdictions. Laying platforms for effective and prompt sharing of information domestically and internationally can go a long way to combat TBML.

Trade Finance Vulnerabilities

237. Investigators in many jurisdictions face major challenges comprehending trade finance products and the implications of the use of trade finance in TBML. Chapter-III of this Paper attempts to be a ready reckoner for investigators to assist them to better understand trade finance products. This should assist investigators to begin to incorporate trade finance analysis in their investigations.

238. The trade finance products set out in Chapter III reveal a menu of choices that are available to genuine traders to facilitate trade. While the various trade finance products reduce trade transaction costs, their accessibility have also made them vulnerable to abuse.

239. Information relating to the trade finance products remain concentrated within the financial sector. Often the financial institutions are not aware of the significance of the information held by them to TBML investigators. A TBML investigator would need to obtain crucial data from financial institutions and correlate that with the information available in the trade sector so as to sieve ‘TBML-laced’ transactions from the predominantly genuine trade flows, the ‘noise’.

240. Chapter II of this Paper finds that jurisdictions were unanimous in highlighting a need for training to be provided to regulators regarding TBML vulnerabilities and risks associated with trade finance activities.

TBML Techniques of Trade Finance

241. The selection of Case Studies in Chapter IV has the intention of expounding the 'modus operandi' involved in TBML not only to throw light on the abuses in the trade sector but also to bring home the contributory anomalies of the trade finance sector. Several of these Case Studies reflect the confidence of the criminal syndicates in the impregnability of the veneer of the international trade they have created to move illicit funds and indulge-in TBML. The syndicates have not merely taken advantage of existing trade structures but have gone on to create new and additional structures for TBML.

242. A number of 'Red Flags' have been enumerated from each of the 7 Case Studies. The 'Red Flags' relate to trade as well as to trade finance. These red flags also corroborate the patterns identified for TBML in Chapter-II.

243. On the basis of the analysis of patterns, modus operandi and red flags, four techniques of TBML relating to trade finance have been formulated. The four techniques are: cash inflow payments; third party payments: segmental modes of payment; and, alternative remittance payments. These four techniques are those which have been more commonly used by criminal syndicates to support the practice of abusing the trade sector.

THE WAY FORWARD

244. Any strategy to prevent and combat TBML needs to be based on dismantling TBML structures, while allowing genuine trade to occur unfettered. A holistic approach, with emphasis on inter-agency coordination and international cooperation, needs to be universally adopted by the policy-makers. A comprehensive strategy which takes into account sectoral peculiarities, agency specialization and jurisdictional frameworks can only address the challenges in tackling TBML. Some of the steps that can form part of the way forward are discussed ad seriatim.

Standardization of Data and Statistics

245. Presently, statistics relating to TBML are not distinguished from those of other forms of ML. Data needed to combat TBML remain dispersed over various domestic sectors. Practices to compile and collate the statistics and data relevant to TBML vary among jurisdictions. There is a need to have common formatting of how TBML statistics are to be recorded and maintained so that trends are more easily identifiable.

246. If centralization of data and statistics is not presently possible then access of competent authorities to such statistics and data should be ensured. Cross-referencing data relating to trade and trade finance can be the starting point for adopting a risk based approach. Such an approach will not only lead to prioritization of limited resources but will also facilitate genuine trade without compromising the necessary governance over TBML. A risk based approach will help capture crucial trade data along with providing an ability to keep track of its corresponding payments data. To ensure efficient real time delivery of analysis the adopting of an electronic platform may be essential.

247. Monitoring foreign exchange may be an option for some jurisdiction in identifying anomalies to detect TBML. one of the finding of the project team is there exists an acute need to correlate trade data with the foreign exchange data of a jurisdiction so as to detect TBML and in particular identify cases wherein value is moved across countries in the form of goods without corresponding outgo of foreign exchange as its payment.

248. As an example, the development of a foreign exchange monitoring system by South Korea endeavours to cross-reference trade related data based on an electronic platform. By working out trends and past performances the system conducts some risk analysis to select risk-prone foreign exchange transactions for more specific scrutiny. There is a capacity to systematically target TBML.

249. Capturing data on trade and trade finance in standard format across the jurisdictions will ease cross-referencing for discovering trade anomalies leading to detection of TBML. Correlating such findings with systematic compilation of foreign exchange data can foster efficient strategies to prevent and combat TBML.

Domestic Task Forces

250. Multiple agencies are associated either directly or indirectly in fighting TBML. One way-forward to combine the respective competencies of relevant authorities for combating TBML is to form domestic task-forces. Task-forces focused on TBML investigations will need to have the ability to utilize the expertise of each agency without comprising its functional skills. It is suggested that to be successful the task-force must set its modes of communication and interaction. The operating platform should be electronic which allows for virtual exchange and management of large quantities of information. If a manual operating platform is adopted then task-force members must ensure regular interaction. The coordination achieved through a TBML task-force should go some way in providing effective support in intelligence, investigation and prosecution work relating to TBML.

251. Customs agencies hold trade data in most of the jurisdictions surveyed. Traditionally such data is used to detect and investigate Customs offences relating to smuggling and duty evasion. The regulators in the trade finance sector issue alerts on the basis of the data available within the sector for the use of financial institutions.

252. Law enforcement agencies responsible for investigating ML use the same tools to investigate TBML without any specialized training to undertake such investigations. These agencies work in isolation without the necessary inputs from Customs and Regulators. FIUs in most jurisdictions analyse and disseminate suspicious transaction reports on the information furnished by the financial sector without corresponding inflow from trade sector and foreign exchange control agencies (in those jurisdictions with such controls). Tax authorities exclusively focus on investigation relating to tax evasion. Transfer pricing audits conducted by such authorities do not identify implications for TBML.

253. The competent authorities tasked with tackling TBML are more often than not focused on work mandated by the legislation as it relates to them. They may have even achieved professional specialization and competence in such mandated work. However, the strategy

to prevent and combat TBML requires expertise created through the combination of all such authorities. It is recognized however that any necessary amendment in the given legal framework may not be easy and in some cases may impact on the respective professional efficiency that exists.

International Cooperation

254. International cooperation to combat TBML is difficult to achieve. The formal and informal means of international cooperation used include treaties and agreements. The Mutual Legal Assistance Treaty (MLAT) and the Customs Mutual Assistance Agreement (CMAA) are bilateral arrangements for exchange of information and are often deployed for combating TBML. However, exchanges made through formal channels often result in delayed responses, inadequate information and limited or no further feedback.

255. Informal channels include interaction with the representatives of foreign jurisdictions assigned for the purpose in the domestic jurisdiction. Informal channels which exist as part of bilateral diplomatic arrangements can also be used to tackle TBML.

256. The Project Team believes that there is an urgent need to strengthen the existing bilateral arrangements and to build multilateral mechanisms for international cooperation. The bilateral arrangements must ensure prompt exchange of information with regular follow-ups which should result in more efficient delivery. The multilateral mechanisms may entail equal commitment of all trading jurisdictions for coordination in matters relating to TBML. Technological innovations for effective communication across jurisdictions can provide permanency to multilateral arrangements. In this regard an initiative by the World Customs Organisation (WCO) to develop the concept of Globally Networked Customs (GNC) for exchange of information may turn-out to have significant strategic value.

TBML Focused Training

257. TBML focused training is an absolute necessity for the anti-TBML strategy to succeed. Customs, ML investigating LEA, FIU, Tax Authorities and Regulators have all identified a pressing need for more focused training so that their personnel can have an adequate knowledge base to detect, prevent and combat TBML. Many of the jurisdictions have reported limitations with regard to resources which they can spare to provide training capable of mitigating TBML activities. This study reiterates the findings of the FATF Best Practices Paper 2008 to incorporate a TBML focus in the existing AML training programmes.

258. The sharper focus on TBML in existing training programs can be brought about by incorporating specific topics which relate to TBML. The case studies, the red flags and typology papers on TBML may be disseminated during such programs. As trade essentially involves multiple jurisdictions, there is a need for Law Enforcement Officers to understand the legal and procedural aspects of other jurisdictions. Training should be aimed at making use of trade data analysis as well as cross referencing trade data with trade finance data and understanding any useful tools developed to identify trade anomalies which may lead to investigation and prosecution of TBML cases. Inter-linkages of tax frauds and customs violations with TBML also need to be explained.

259. The significance of domestic coordination and of international cooperation to tackle TBML must be conveyed during training programs. Further, as a large number of private players are involved in international trade they need to be apprised of concealed TBML threats in any outreach programs that are conducted. Thus, capacity building among all competent authorities and private industry is an important component of any successful strategy to prevent and combat TBML.

Further Research

260. The ongoing fight against TBML through the comprehensive strategy discussed in this Chapter should spur further research so as to meet emergent challenges. The possible areas of such research may be briefly delineated as follows:

a) Services: Treatment with regard to TBML vulnerabilities in trade of services shall require specialized tools. Services more than goods, give wide scope for manipulation in pricing, quantification and delivery time-schedule. It may therefore be imperative to undertake further research to develop case-studies and identify red-flags.

b) Terrorist Financing: Moving of funds through trade to fund illicit activity of terrorism in an important issue confronting the global security. Further research to look into aspects of such illicit fund movement through trade is called for.

c) Financing the proliferation of WMD: Building on work undertaken by the FATF, there is a need to further consider vulnerabilities of trade finance to the financing of the proliferation of WMD.

d) Risk Based Approaches: Adoption of risk based approaches in the strategy to combat TBML is essential not only to maximise resources but to target TBML without inhibiting genuine trade flows. Research should be undertaken to work-out models which could be practically adopted by various jurisdictions.

e) Tax evasion: The work done by international bodies such as OECD, Global Financial Integrity, have brought into focus trade-mispricing and transfer pricing as well as their correlation with poverty. With continued enhanced focus on tax evasion, or use of tax havens and on evasion of customs duty, it is essential to do research to explore their inter-linkages with TBML.

261. A comprehensive strategy to meet the growing concern about TBML has been recommended in this Chapter. Challenges in formulating such a strategy have been identified. Ways forward for addressing some of these challenges have been suggested. International trade needs to be kept free of TBML so that the full benefit from effective and efficient global trade can be realised by the community of nations.

ANNEX A - TBML RED FLAGS FROM CURRENT & EXISTING STUDIES

262. The Red Flags which have been mentioned in the existing studies have been categorized as per the scheme adopted in Chapter II of this Paper. Annex A sets out red flags gleaned from existing studies, as well as those identified in the current study. In many cases there is a correlation between previous studies and the present study.

263. The Red Flags set out in this section of Annex A are derived from studies by the FATF, US (FINCEN & ICE), Australia (AIC) the Wolfsberg Group and studies by BRANNIGAN (2010) and Brown (2009).

Red Flags relating to Trade Finance:

- The transaction involves receipt of cash (or other payments like wire transfers, checks, bank drafts or postal money orders) from unrelated third party entities or an intermediary (either an individual or an entity) apparently unrelated to the seller or purchaser of goods. This may be done to obscure the true origin of the funds (e.g. Wires where no apparent business relationship appears to exist between the originator and the beneficiary) ;

- The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or for reasons like changes of the beneficiary or location of payment ;

- A customer's inability to produce appropriate documentation (e.g. invoice or any other document) to support a requested financial transaction or bank finds double invoicing or a Customer fails to provide adequate information about the originator, beneficiary, and purpose of the wire transfer;

- The method of payment appears inconsistent with the risk characteristics of the transaction; (For example, the use of an advance payment for a shipment from a new supplier in a high-risk country or Frequent transactions involving rounding or whole dollar amounts).

- Phantom shipping – no goods are shipped and all documentation is completely falsified to move funds in the guise of trade

- Negotiable instruments (such as traveller's checks, cashier's checks and money orders) in round denominations under $3,000 used to fund domestic accounts or, alternatively, smuggled from a jurisdiction for placement into accounts at foreign financial institutions. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information or contain visible broker markings or symbols. These negotiable instruments may also be used to pay for goods and services.

- International wire transfers received as payment for goods into bank accounts or processed through correspondent or intermediary accounts in a particular country, especially where the ordering party (importer of goods) of the wire does not live in the country from which the wire originated. (e.g. Wires originating from jurisdictions which have been highlighted in relation to black market peso exchange activities),

- Sudden onset and equally sudden cessation of payments – typically wire transfers – within a short duration. This could be an indication that the account is temporarily being used to launder illicit proceeds.

- A foreign based importing entity with accounts in exporting country receiving payments from locations outside the areas of their customer base.

- Unusual deposits occurring in combination with one or more of the following indicators:

    - Multiple deposits occurring in various locations when the account owner resides elsewhere, for example, deposits made in various cities when the account owner resides in a different city.
    - Multiple bank accounts held by a customer individually or along with closely related family members. These accounts may be held at one or more financial institutions. Such accounts may be used to facilitate the placement and layering of illicit funds.
    - Checking accounts receiving cash deposits in amounts under $1,000 as frequently as several times per month. These deposits may be followed by ATM withdrawals in foreign countries. This method, sometimes referred to as micro-structuring, is used by “smurfs” to deposit cash which may then be used to purchase goods.

- Foreign visitors opening multiple bank accounts at one or more financial institutions. Individuals may travel to a foreign jurisdiction with instructions to establish multiple bank accounts as a straw party. Upon return to their home country the straw account owner signs all of the blank checks and relinquishes control of the checkbooks and ATM cards tied to the accounts to the beneficial owner who now has control of the accounts. The following are examples of activity common to these accounts:

    - Cash deposits received using over-the-counter deposit slips since the checkbooks containing the pre-printed deposit slips as well as ATM cards are located out of that country;
    - Deposits which are frequently made in multiple cities / jurisdictions;
    - Withdrawals made via foreign ATM transactions; or
    - Withdrawals via check transactions that exhibit a difference between the handwriting for the signature and the payee portions of the check.

- Unusual activity in established bank accounts for non-resident aliens, such as structured cash and monetary instrument deposits; checks written from the domestic account to foreign businesses with no apparent relationship to the account holder; and international wire transfers to entities that do not appear to have any relationship with the originator.

- Sequentially numbered checks drawn on domestic bank accounts negotiated through foreign money services businesses.

264. It is important to remember that no one activity by itself is a clear indication of trade-based ML. Due to some similarities with legitimate financial activities, financial institutions should evaluate indicators of potential trade-based ML in combination with other red flags and expected transaction activity for its customer before making determinations of suspiciousness. Additional investigation and analysis may be necessary to determine if the activity is suspicious, based on information available to the financial institution.

Red Flags relating to Jurisdictions:

- The commodity is shipped to (or from) a jurisdiction designated as "high risk" for ML activities;
- The commodity is transhipped through one or more jurisdictions for no apparent economic reason;
- Customers conducting business in high-risk jurisdictions. Although not specifically identified by the authority handling AML work or FATF ; FTZs may be added to the list of high-risk jurisdictions given that there is an argument that FTZs exacerbate the risk
- Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries
- Unusual shipping routes or trans-shipment points
- Funds transferred into a country's domestic accounts that are subsequently transferred out of the account in the same or nearly the same amounts. Origination and destination locations are frequently high risk jurisdictions.

Red Flags relating to Goods:

- Significant discrepancies between the descriptions of the goods on the transport document (i.e., bill of lading), the invoice, or other documents (i.e., certificate of origin, packing list, etc.).
- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped;
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value;
- The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities;
- The type of commodity being shipped is designated as "high risk" for ML activities; [e.g. high-value, low-volume goods (e.g. consumer electronics, diamonds), which have high turnover rates and which present valuation difficulties].
- Shipment locations or description of goods that are inconsistent with the letter of credit

- Documentation showing a higher or lower value or cost of merchandise than that which was declared to Customs or paid by the importer (i.e. commodity over-valuation or under-valuation)
- Customers involved in potentially high-risk activities, including those subject to export/import restrictions such as equipment for military or police organisations of foreign governments, weapons, ammunition, chemical mixtures, classified defence articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore and crude oil
- Obvious misrepresentation of quantity or type of goods imported or exported
- A shipment that does not make economic sense (e.g. the use of a forty-foot container to transport a small amount of relatively low value merchandise)
- The type of commodity being traded appears inconsistent with the exporter or importer's usual business activities (e.g. a steel company that starts dealing in paper products, or an information technology company that suddenly starts dealing in bulk pharmaceuticals)
- Carousel transactions: the repeated importation and exportation of the same high-value commodity
- Packaging inconsistent with commodity or shipping method

Red Flags relating to Corporate Structures used:

- A transaction involves the use of front (or shell) companies.
- Companies or Money Exchange Bureaus located in third countries used as intermediaries for transfer of goods or money.
- A transaction structure that appears unnecessarily complex through introduction of corporate entities so that it obscures the true nature of the transaction.
- Companies operating out of foreign countries, especially when it is difficult or impossible to determine ownership or controlling persons of the company, or when the business purpose is not fully apparent.

RED FLAGS CONFIRMED IN THE APG TBML PAPER

265. The present paper has categorized the Red Flags received from various jurisdictions in response to the questionnaire into following five broad categories.

TRADE FINANCE

266. Based on the responses received from jurisdictions, red flags relating to financial & banking products may be categorized as follows:

a) Use of **letters of credit** to move money between those countries, where such trade would not normally occur and / or is **not consistent with the customer's usual business activity**. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.

b) The **method of payment** requested by the client appears **inconsistent with the risk characteristics of the transaction**. For example receipt of an advance payment for a shipment from a new seller in a high-risk jurisdiction.

c) The transaction involves the receipt of cash (or by other payment methods) **from third party entities** that have no apparent connection with the transaction or which involve front or shell companies or wire instructions / payment from parties which were not identified in the original letter of credit or other documentation. The transactions that involve payments for goods through cheques, bank drafts, or money orders not drawn on the account of the entity that purchased the items also need further verification.

d) The transaction involves the use of repeatedly **amended or frequently extended letters of credit** without reasonable justification or that includes changes in regard to the beneficiary or location of payment without any apparent reason.

e) **Unusual deposits** i.e. use of cash or negotiable instruments (such as traveller's cheques, cashier's cheques and money orders) in **round denominations** (to keep below reporting threshold limit) to fund bank accounts and to pay for goods and services. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information. Further, cash payments for high-value orders are also indication of TBML activity.

f) Inward remittances in **multiple accounts** and payments made from multiple accounts for trade transaction of same business entity are indicators for TBML. In this regard the study of foreign exchange remittances may help detect the offence.

g) In the case of **merchanting trade**, the trade finance mechanism should be in place for both export leg as well as import leg of transaction. If the Trade Finance mechanism, for example, Letters of Credit, have been provided for only the import leg of the transaction and not for export leg, it also indicates the possibility of TBML.

JURISDICTIONS (ORIGIN OR DESTINATION OF GOODS)

a) The commodity is shipped to or from a jurisdiction designated as '**high risk'** for ML activities or sensitive / non co-operative jurisdictions.

b) The commodity is **transhipped** through one or more such high risk / sensitive jurisdictions for no apparent economic reason.

c) Presence of **Free Trade Zones / Special Economic Zones** also affects the sensitiveness of a jurisdiction as far as TBML is concerned. FTZs are also emerging as being especially vulnerable to TBML. FATF (2010: 4) defines FTZs as 'designated areas within countries that offer a free trade environment with a minimum level of regulation'. In the said report, FATF noted that most zone authorities operate separate company formation services from those that exist in the rest of the jurisdiction and market the ease of setting up a legal entity in an FTZ to attract business. Many zone authorities request little or no ownership information of the companies interested in setting up in the zone. As a result, it is simpler for legal entities to set up the firms/companies in FTZs and hide the name(s) of the true beneficial owners. This lack of transparency has allowed companies located in FTZs to create layers of transactions that are difficult (if not impossible) for law enforcement agencies to follow (FATF 2010). It also reported that 'goods introduced in a FTZ' are generally not subject to the usual customs controls, with goods undergoing 'various economic operations, such as transhipment, assembly, manufacturing, processing, warehousing'. FinCEN has identified TBML red flags that are specific to FTZs. In its 2010 report, FinCEN (2010: 4) signalled that a number of red flags seen in conjunction with shipments of high dollar merchandise (such as electronics, auto parts and precious metals and gems) to duty free trade zones could be an indication of a trade-based ML activity.

   These include:

   i. third-party payments for goods or services made by an intermediary (either an individual or an entity) apparently unrelated to the seller or purchaser of goods. This may be done to obscure the true origin of the funds;
   ii. amended letters of credit without reasonable justification;
   iii. a customer's inability to produce appropriate documentation (ie invoices) to support a requested transaction; and
   iv. significant discrepancies between the descriptions of the goods on the transport document (ie bill of lading), the invoice, or other documents (ie certificate of origin, packing list etc) (FinCEN 2010).

d) **Circuitous route of shipment** and/or **circuitous route of financial transaction** or **Order for the goods** is placed by firms or individuals from foreign countries other than the jurisdiction of the stated end-user.

e) Transaction involves **shipment of goods inconsistent with normal geographic trade patterns** of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense e.g.

Semi-conductor manufacturing equipment being shipped to a jurisdiction that has no electronics industry.

NATURE OF GOODS

a) Where significant discrepancies appear between the **description, quality and quantity** of the goods on the documents such as bills of lading, invoices etc and the actual goods shipped. The misrepresentation may also be in relation to or type / grade of goods. For example, a relatively inexpensive good is supplied but it is invoiced as being more expensive, of different quality or even as an entirely different item so the documentation does not accurately record what is actually supplied. This technique is particularly useful in TBML. Cheap cloth items / waste thereof are declared as premium quality garments to launder the criminal money.

b) Significant discrepancies appear between the **value** of the commodity reported on the invoice and the commodity's fair market value. This is done either in conjunction with mis-declaration of the description / quality / grade of goods or without it. This is also often associated with mis-declaration of the jurisdiction of origin.

c) **Consignment size or type of commodity** being shipped appears **inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities** or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.

COPRPORATE STRUCTURES

a) The transaction involves the use of **front or shell companies**. Both shell and front companies can be used to facilitate TBML but in different ways. A shell company has no real operating activity and is used to hide ML activity and the identities of individuals involved so as to obscure the money trail. If activity is traced to the company it is literally an empty shell. As FATF (2010: 20) explained TBML and other ML schemes rely on the ability of the perpetrator of the crime to distance themselves from the illicit proceeds. Shell companies enable illicit actors to create a network of legal entities around the world. By contrast, a front company has real business whose legitimate operations are used as a cover for ML and other criminal activity. In many ways, front companies present a much more significant TBML threat than shell companies. The characteristics of offshore companies, for example, convenient formation, free operation, tax exemption and financial secrecy, all provide rather good veneer to disguise ML

b) Numerous **sole proprietorship businesses/private limited companies** set up by seemingly unrelated people (proxies) are found to be controlled by the same group of people. For the setting up of such businesses false addresses are registered.

c) Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management. TBML requires collusion between traders at both ends of the import/export chain. **Related party transactions** (ie transactions between entities

that are part of the same corporate or business group) can possibly make TBML easier and more difficult to detect. Related party transactions, including transfer pricing, rely on mutual agreements between the parties, rather than free market forces. As the FATF (2006: 5) pointed out, over- or under-invoicing of goods and services requires collusion between the exporter and importer. Although there is a higher risk of related party transactions being used for fraud and for TBML, dealings between related parties are not necessarily illegal. d) Transfer pricing is a related party transaction that is commonly used by transnational corporation as part of their financial and tax planning strategy. Multinational organisations use transfer pricing to shift taxable income from jurisdictions with relatively high tax rates to jurisdictions with relatively low tax rates to minimise income tax. Similar strategies are also employed in relation to import duties and value added tax. FATF (2006: 3) made it clear though that in the case of transfer pricing, the reference to over- and under-invoicing relates to the legitimate allocation of income between related parties, rather than customs fraud.

PREDICATE OFFENCES OF TBML

267. 15% of the jurisdictions have reported that **tax evasion** is the predominant predicate offence in TBML cases whereas 10% of the jurisdictions have reported c**ustoms offences** as the main predicate offence. Other responses indicate that predicate offenses are often related to commercial fraud, IPR, Narcotics, human trafficking, terrorist financing, embezzlement, corruption, organized crime (racketeering), dealing in banned goods, conducting illegal business, speculation etc. One Reporting jurisdiction indicated that ML is considered to be an autonomous offence and there is no need to prove the existence or nature of the predicate offence in order to prosecute hence as a consequence, there is no systemic link between ML cases and other crimes.

ANNEX B - SUMMARY OF RESPONSES TO THE APG TBML QUESTIONNAIRE

268. 19 jurisdictions responded to the questionnaire: Anguilla, Australia, Belgium, Belize, Bhutan, Cambodia, Canada, Fiji, Hong Kong,China, India, Japan, Macao, Malaysia, Myanmar, Nepal, OCO, Pakistan, Singapore, Vietnam and USA. Oceania Customs Organisation also responded to the questionnaire.

SUMMARY OF RESPONSES

SECTION A. COORDINATING AGENCIES

	Yes	No
1A. Reason for very few cases of TBML reported up to 2011:		
i. It is not an issue;	**4**	**1**
ii. It is a policy/law, issue that results in no detection; or	**8**	
iii. Other Issues (Training, awareness / other)that results in no detection;	**9**	
No Report / Not Applicable etc: (**1)**		
2A. Did the FATF 2006 & 2008 papers describe all types of TBML?	**11**	**4**
No Report / Not Applicable etc: (**5)**		
3A. Whether any Government department records information on goods imported and exported into your jurisdiction?	**19**	**-**
No Report / Not Applicable etc: (**1)**		
4A. Does this agency, if Customs, has dedicated financial investigators with experience in trade related offences and or ML investigations?	**5**	**10**
Does this agency, if other than Customs, has dedicated financial investigators with experience in trade related offences and or ML investigations?		**5**
No Report / Not Applicable etc: (**2)**		
6A. Does your jurisdiction use any database to identify the value of goods, ie under/overpricing?	**12**	**5**
No Report / Not Applicable etc: (**3)**		
7A. If your jurisdiction has identified cases of TBML?	**9**	**8**
No Report / Not Applicable etc: (**3)**		
8A. Has your jurisdiction undertaken any of the following: **a.** A typologies study on TBML , or Abuse of the Trade Finance sector in the jurisdiction?	**2**	**14**
b. A risk assessment of TBML or Abuse of Trade Finance sector in the jurisdiction?	**2**	**14**
c. A risk assessment on Transfer Pricing.	**2**	**14**
d. A risk assessment of the use of Alternative Remittance Sectors in trade finance.	**2**	**14**
No Report / Not Applicable etc: (**4)**		

SECTION B. CUSTOMS AGENCIES

	Yes	No
1B. Does Customs conduct investigations into TBML or Transfer pricing?	**8**	**11**
If so, does the Customs agency also conduct the ML aspect of this investigation?	**4**	**4**
No Report / Not Applicable etc: (**1**)		

2B. Statistics on the number of TBML investigations in the past 5 years.

Details	**2007**	**2008**	**2009**	**2010**	**2011**
Nos of TBML investigations initiated / identified / referred	-	-	5	8	219
Amount involved in such offences	-	-	-	-	Not available
Result of investigations	-	-	-	-	-
Value of assets attached / frozen	-	-	-	$90 million#	Not available
Value of assets confiscated	-	-	-	-	-

Not Available/ Not Maintained separately / Nil: (**17**)

 # US reported TBML investigations completed in 2010 resulted in approx US$90 million in seizures.

	Yes	No
3B. Is Customs part of any joint financial investigation/ML task force that conducts investigations into these offences?	**9**	**9**
Not Available/ Not Maintained separately: (**2**)		
4B. Has Customs received training on TBML?	**8**	**10**
Does Customs provide training to other agencies on TBML issues?	**2**	**10**
No Report / Not Applicable etc**:** **(2)**		
	Yes	**No**
5B. Whether any impediments encountered when conducting investigations? Eg impediments regarding the release of FIU data to the agency or agency unable to share trade information etc.	**6**	**6**
No Report / Not Applicable etc: (**8**)		
	Yes	**No**
6B. Whether information is collected on type of goods, value of goods, importer, exporter, owner, receiver, shipping company etc?	**17**	
No Report / Not Applicable etc: (**3**)		
7B. Do you conduct analysis of trade information that could be used to identify, investigate or prosecute TBML?	**10**	**9**
No Report / Not Applicable etc: (**1**)		
8B. Has your jurisdiction identified patterns of goods that are involved in TBML?	**5**	**13**
No Report / Not Applicable etc: (**2**)		
9B. Are goods in TBML usually trans-shipped?	**1**	**5**
And is there any pattern of jurisdiction of origin (ie where are the goods usually shipped from, or are there some jurisdictions more prevalent than others as a point of origin)?	**2**	**2**
No Report / Not Applicable etc: (**14**)		

10B. How are the investigations into TBML usually initiated? ie information from intelligence, law enforcement, FIU data, STRs, trade data etc.

On the basis of inter-agency intelligence	**8**
On the basis of intra-agency intelligence	**8**

information from intelligence	information from law enforcement,	information from FIU data	information from STRs,	information from trade data	information from other sources
6	**9**	**7**	**6**	**5**	**3**
No Report / Not Applicable etc: (**9)**					

	Yes	**No**
11B. During your investigations do you seek information from your international counterparts?	**11**	**3**
During your investigations do you seek information from your WCO?	**10**	**3**
No Report / Not Applicable etc: (**6)**		
12B. During your investigations do you seek information from Domestic LEAs?	**10**	**3**
No Report / Not Applicable etc: (**7)**		
13B. During your investigations do you seek information from international LEAs ?	**8**	**4**
During your investigations do you seek information from FIUs?	**8**	**3**
No Report / Not Applicable etc: (**8)**		
14B. Is there any impediments to the receipt or dissemination of this information?	**8**	**5**
Is there any legal requirements for the dissemination of information related to trade (ie MoU)?	**4**	**4**
No Report / Not Applicable etc: (**7)**		
15B. Does your agency maintain an intelligence database on import and export of goods?	**15**	**4**
Do you cross reference this information with other government databases, i.e. companies registry, tax records, criminal records etc.?	**6**	**7**
No Report / Not Applicable etc: (**1)**		
16B. Whether any indicators and red flags of TBML identified?	**7**	**5**
No Report / Not Applicable etc: (**8)**		
17B. Have you shared any TBML related intelligence with your foreign counterparts?	**6**	**10**
If so are you aware of the results of that dissemination, i.e. aid in investigation, result in prosecution etc.	**3**	
No Report / Not Applicable etc: (**4)**		
18B. Are there any challenges and obstacles for your agency to identify or investigate TBML?	**8**	**3**
No Report / Not Applicable etc: (**9)**		

SECTION C. LAW ENFORCEMENT AGENCY MANDATED TO INVESTIGATE ML (MAY INCLUDE CUSTOMS / INVESTIGATIVE FIUS)

1C. Statistics on the number of TBML investigations in the past 5 years

Details	**2007**	**2008**	**2009**	**2010**	**2011**
No. of TBML investigations initiated / identified / referred from other agencies	1	18	27	20	**223**
Amount involved	USD 2.17 Million	USD 6.16 Million	USD 420.59 Million	USD 46.88 Million	USD 81.52Million

Result of investigations	-	-	Prosecution pending	Prosecution pending	Prosecution pending
Value of assets attached / frozen (US $)	USD 2.17 Million	USD 6.16 Million	USD 44.98 Million	USD 91.04 Million #	Under investigation
Value of assets confiscated	-	-	-	-	-
No Report / Not Applicable etc/ Nil : (**15)**					
#: *In addition to above as per report of USA: 208 investigations. TBML investigations completed during 2010 resulted in approximately $90 million dollars in seizures.*					

	Yes	**No**
2C. Does the law enforcement agency conduct investigations into TBML or Transfer pricing?	11	4
If so does the law enforcement agency also conduct the ML aspect of this investigation?	**11**	**3**
No Report / Not Applicable etc: (**5)**		
3C. Is the law enforcement agency part of a joint financial investigation/ML task force that conducts investigations into these offences?	**9**	**6**
No Report / Not Applicable etc: (**5)**		
4C. Has the law enforcement agency received training on TBML?	**7**	**10**
Does it provide training to other agencies on TBML issues?	**3**	**9**
No Report / Not Applicable etc: (**3)**		
5C. Are there any impediments encountered when conducting investigations?	**6**	**9**
No Report / Not Applicable etc: (**5)**		
6C. How are TBML investigations initiated? i.e. referrals from other agencies etc.? 1. From Internal intelligence: (**7)** **2.** Referrals from other agencies: (**11)**		
No Report / Not Applicable etc: (**7)**		
7C. Of the TBML matters investigated what is the average size, in dollar terms, of the offence?	USD 557.3 Million in 19 cases.	
No Report / Not Applicable etc: (**15)**		
8C. What are the predicate offences that have in the past been associated with TBML? **1.** Narcotics **2.** Domestic Crime / Organised Crime **3.** Corruption **4.** Customs Violations **5.** Tax Evasion **6.** Manufacturing, stockpiling, transporting and/or trading in banned goods **7.** Conducting business illegally **8.** Speculation **9.** Commercial fraud **10.** IPR **11.** Human Trafficking & Terrorist Financing **12.** Embezzlement **13.** Fraud		
No Report / Not Applicable etc: (**12)**		
9C. What types of goods are involved in TBML matters? **1.** Metal scrap.		

2. Textile materials. **3.** Zero duty goods like Diamonds. (**2)** **4.** Precious metals. **5.** Luxury watches **6.** Good where the taxes are high or which are heavily controlled **7.** Electronic goods **8.** Illicit tobacco products **9.** Counterfeit Products **10.** Bulk Commodities.
No Report / Not Applicable etc: (**14)**
10C. What types of corporate structures are used by criminal syndicates in TBML investigations? **1.** Companies: (**6**) **2.** Offshore Companies: (**5**) **3.** Others: joint-venture companies registered in developing countries **(1)** **4.** Criminals don't use Corporate Structure. **(1)**

	Yes	**No**
Where such offshore companies are registered? Is there any pattern to jurisdictions that they are registered?	**3**	
No Report / Not Applicable etc: **(16)**		
Yes **No**		
11C & 12C. Whether you receive information from the Customs agency?	**12**	**1**
Are there any restrictions on the use of this information?	**7**	**5**
No Report / Not Applicable etc: (**7)**		
14C. Does your agency have specialist financial investigators who conduct the TBML investigations?	**9**	**7**
No Report / Not Applicable etc: (**4)**		

	Value in USD
15C. What was the value of any assets forfeited as a result of the investigation?	USD 72.66 Million
No Report / Not Applicable etc: **(17)**	
16C. What red flags or indicators of the TBML activity have you identified?	
No Report / Not Applicable etc: **(12)**	

	Yes	**No**
17C. Have investigations of Alternative Remitters identified instances of TBML?	**3**	**7**
Have investigations of Alternative Remitters identified instances of abuse of trade finance?	**2**	**7**
No Report / Not Applicable etc: (**10)**		

SECTION D. FIU

1D. Statistics on the number of TBML STRs in the past 5 years

Details	**2007**	**2008**	**2009**	**2010**	**2011**
Nos of TBML STRs received	15	49	186	690	1054
Nos of TBML STRs disseminated	7	28	130	474	699
Value of STRs received (USD)	$756	$15462	$164614	$486256	$7315
No Report / Not Applicable etc: (**15)**					

	Yes	**No**
2D. Is the FIU part of a joint financial investigation/ML task force that conducts	**3**	**15**

investigations into these offences?		
No Report / Not Applicable etc: **(2)**		
3D. Has the FIU received training on TBML?	**7**	**11**
Does it provide training to other agencies on TBML issues?	**7**	**11**
No Report / Not Applicable etc: **(2)**		
4D. Are there any impediments encountered when conducting intelligence gathering? For example, impediments regarding the release of FIU information, unable to receive law enforcement information, lack of access to databases etc.	**5**	**11**
No Report / Not Applicable etc: **(4)**		
5D. Can Customs agencies receive financial information from the FIU?	**18**	**-**
No Report / Not Applicable etc: **(2)**		
6D. Have requests been made for sharing financial intelligence (FIU to FIU, FIU to LEA etc)?	**14**	**4**
No Report / Not Applicable etc: **(2)**		

SECTION E. TAX AUTHORITIES

	Yes	**No**
1E. Do you have any estimates of the size of (detected and undetected) TBML and transfer pricing in your jurisdiction?	**2**	**9**
If yes, what is the size? USD 19 Million (1 Jurisdiction)		
No Report / Not Applicable etc: **(9)**		
2E. Does the Tax Authority conduct investigations/audits into TBML or Transfer Pricing?	**3**	**10**
No Report / Not Applicable etc: **(7)**		

3E. Statistics on the number of TBML/transfer pricing detections in the past 5 years

Details	**2007**	**2008**	**2009**	**2010**	**2011**
No of TBML/transfer pricing investigations initiated / identified		1	1	3	63
Amount involved in such offences (USD)		USD 234.6	USD 111.8	USD 49.3	USD 240.9
Result of investigations		*Not prosecuted*	Not prosecuted	Not prosecuted	Not prosecuted
Assets attached / frozen/confiscated					

Nil /No Report / Statistics not maintained for TBML cases /Not Applicable etc: (**18)**		
	Yes	**No**
4E. Is the Tax Authority part of a joint financial investigations/ML/Task Force that combats TBML?	**5**	**6**
If so, is there a lead agency?	**2**	**3**
No Report / Not Applicable etc: (**9)**		
5E. Has the Tax Authority received training on TBML?	**4**	**9**
Does it provide training to other agencies on TBML issues?	**1**	**10**
No Report / Not Applicable etc: (**6)**		
7E. Does the Tax Authority receive FIU data for the purpose of investigation of administrative issues?	**6**	**5**
No Report / Not Applicable etc: (**9)**		

SECTION F. AML REGULATOR

	Yes	**No**
1F. Has the regulator or supervisor provided guidance to reporting entities regarding TBML vulnerabilities and red flags?	**11**	**5**
No Report / Not Applicable etc: (**4)**		
2F. Does the regulator or supervisor provide training to reporting entities and their own staff on TBML?	**8**	**8**
Does the regulator have experts in the area of Trade Finance?	**5**	**7**
No Report / Not Applicable etc: (**4)**		
3F. Does AML supervision include trade finance aspects of compliance?	**10**	**6**
No Report / Not Applicable etc: (**4)**		
4F. Does your jurisdiction have foreign currency controls?	**11**	**4**
No Report / Not Applicable etc: (**5)**		
5F. Do foreign currency controls have a role in identifying abuse of trade finance or TBML?	**5**	**4**
No Report / Not Applicable etc: (**11)**		
6F. Have investigations of Alternative Remitters identified instances of TBML or abuse of trade finance?	**3**	**9**
No Report / Not Applicable etc: (**8)**		

PROJECT TEAM

CO-LEADERS

1. **BALESH KUMAR**
   Special Director, Enforcement Directorate, India;
   E-mail <**balesh.kumar@nic.in**>
2. **NICHOLAS MCTAGGART**
   Detective Superintendent
   Criminal Assets Confiscation Taskforce,
   Serious & Organised Crime , Australia;
   E-mail <**Nicholas.McTaggart@afp.gov.au**>

PROJECT TEAM

1. **RAJESH PANDEY**
   Joint Director, Enforcement Directorate, India;
   E-mail <**rajeshpandey@nic.in**>
2. **SUBHASH AGRAWAL**
   Joint Director, Enforcement Directorate, India;
   E-mail <**subhash.agrawal@nic.in**>
3. **RAY VILLANUEVA**
   Unit Chief, HSI TTU, USA;
   Email <**raymond.villanueva@dhs.gov**>
4. **MATTHEW YOUNGHO JOO**
   Investigator, Financial Investigation Division, Korea Customs Service, South Korea;
   E-mail <**matthew.youngho.joo@gmail.com**>
5. **MOHAMMAD ADBUR RAB**
   Deputy Director, Anti-Money Laundering Department, Bangladesh Bank, Bangladesh;
   E-mail <**abdur.rab@bb.org.bd**>
6. **HARI KUMAR NEPAL**
   Assistant Director, Nepal Rastra Bank,Central Office, Legal Division/FIU, Nepal,
   E-mail <**hariknepal@nrb.org.np**>

APG Secretariat

DAVID SHANNON
Principal Executive Officer
Asia/Pacific Group on Money Laundering
E-mail **mail@apgml.org**

SHAUN MARK
Principal Executive Officer (July - January 2011)
Asia/Pacific Group on Money Laundering**]**

Appendix AA:

FATF, *FATF Report: Virtual Currencies Key Definitions and Potential AML/CFT Risk* (Paris: FATF, 2014)

FATF

FATF REPORT

Virtual Currencies
Key Definitions and Potential AML/CFT Risks

June 2014

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

CONTENTS

ACRONYMS

AML/CFT	Anti-money laundering / countering the financing of terrorism
ECB	European Central Bank
FATF	Financial Action Task Force
NPPS Guidance	Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services

VIRTUAL CURRENCIES - KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS[1]

INTRODUCTION

As decentralised, math-based virtual currencies—particularly Bitcoin[2]—have garnered increasing attention, two popular narratives have emerged: (1) virtual currencies are the wave of the future for payment systems; and (2) virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.[3] Against this backdrop, this paper builds on the 2013 New Payment Products and Services (NPPS) Guidance (FATF, 2013) by suggesting a conceptual framework for understanding and addressing the anti-money laundering / countering the financing of terrorism (AML/CFT) risks associated with one kind of internet-based payment system: virtual currencies. Specifically, the paper proposes a common definitional vocabulary that clarifies what virtual currency is and classifies the various types of virtual currency, based on their different business models and methods of operation,[4] and identifies the participants in typical virtual currency systems. It also applies risk factors set forth in Section IV (A) of the 2013 NPPS Guidance to specific types of virtual currencies to identify potential risks; describes some recent investigations and enforcement efforts involving virtual currency; and presents a sample of jurisdictions' current regulatory approaches to virtual currency.

While the 2013 NPPS Guidance broadly addressed internet-based payment services, it did not define "digital currency," "virtual currency," or "electronic money." Nor did it focus on virtual currencies, as distinct from internet-based payment systems that facilitate transactions denominated in real money (fiat or national currency) (e.g., Pay-Pal, Alipay, or Google Checkout). It also did not address decentralised convertible virtual currencies, such as Bitcoin. The 2013 Guidance also notes that, "[g]iven the developing nature of alternate online currencies, the FATF may consider further work in this area in the future" (2013 NPPS Guidance, p. 11, para. 29). A short-term typologies project on this basis was initiated with the following objectives:

- develop a risk-matrix for virtual currencies (or perhaps, more broadly, for both virtual currencies and e-money);
- promote fuller understanding of the parties involved in convertible virtual currency systems and the way virtual currency can be used to operate payment systems; and
- stimulate a discussion on implementing risk-based AML/CFT regulations in this area.

This typologies project may lead to policy work by the FATF, e.g. the issuance of supplemental guidance for applying a risk-based approach to virtual currencies that would incorporate the proposed vocabulary and risk-matrix developed by the typologies project and explain how specific FATF Recommendations apply in the context of virtual currency.

KEY DEFINITIONS:

A common set of terms reflecting how virtual currencies operate is a crucial first step to enable government officials, law enforcement, and private sector entities to analyse the potential AML/CFT

risks of virtual currency as a new payment method. As regulators and law enforcement officials around the world begin to grapple with the challenges presented by virtual currencies, it has become apparent that we lack a common vocabulary that accurately reflects the different forms virtual currency may take. The following set of terms is intended to aid discussion between FATF members. It is important to note that this vocabulary may change as virtual currency evolves and as regulators and law enforcement/government officials continue to consider the challenges virtual currencies present. Nevertheless, the proposed vocabulary aims to provide a common language for developing conceptual tools to help us better understand how virtual currencies operate and the risks and potential benefits they offer.

VIRTUAL CURRENCY

Virtual currency is a digital representation[5] of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)[6] in any jurisdiction.[7] It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. **"real currency," "real money,"** or **"national currency"**), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e**-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency". In this paper to avoid confusion, only the terms "virtual currency" or "e-money" are used.

CONVERTIBLE VERSUS NON-CONVERTIBLE VIRTUAL CURRENCY

This paper proposes dividing virtual currency into two basic types: convertible and non-convertible virtual currency.[8] Although the paper uses "non-convertible" and "closed", and "convertible" and "open" as synonyms, it should be emphasised that the notion of "convertible currency" does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is "convertible" only as long as some private participants make offers and others accept them, since the "convertibility" is not guaranteed at all by law.

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.[9] Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.[10]

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include**:** Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

It should be noted that even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the "non-convertible" virtual currency for fiat currency or another virtual currency. Generally, the administrator will apply sanctions (including termination of membership and/or forfeiture of remaining virtual currency) to those seeking to create or use a secondary market, contrary to the rules of the currency.[11] Development of a robust secondary black market in a particular "non-convertible" virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency. A non-convertible characterisation is thus not necessarily static.

CENTRALISED VERSUS NON-CENTRALISED VIRTUAL CURRENCIES

All non-convertible virtual currencies are centralised: by definition, they are issued by a central authority that establishes rules making them non-convertible. In contrast, convertible virtual currencies may be either of two sub-types: centralised or decentralised.

Centralised Virtual Currencies have a single administrating authority (**administrator)**—i.e., a third party[12] that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may be either **floating**—i.e., determined by market supply and demand for the virtual currency--or **pegged**—i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney "WM units"; and World of Warcraft gold.

Decentralised Virtual Currencies (a.k.a. crypto-currencies) are distributed[13], open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; LiteCoin; and Ripple.[14]

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.

Bitcoin, launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters

that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual.. Therefore, Bitcoin is said to be "pseudo-anonymous". Bitcoin is capped at 21 million bitcoins (but each unit could be divided in smaller parts), projected to be reached by 2140.[15] As of April 2, 2014, there were over 12-and-a-half million bitcoins, with total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date.

Altcoin refers to math-based decentralised convertible virtual currency other than bitcoins, the original such currency. Current examples include Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin and dogecoin. One popular exchanger, Cryptsy, would reportedly exchange over 100 different virtual currencies (as of 2 April 2014). (Popper, N., 2013)

Anonymiser (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. (Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)).

Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.

Dark Wallet is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to Silk Road.

Cold Storage refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft.

Hot Storage refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage.

Local Exchange Trading System (LETS) is a locally organised economic organisation that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or bartered in exchange for goods or services. Theoretically, bitcoins could be adopted as the local currency used within a LETS. (Examples: Ithica Dollars; Mazacoin).

VIRTUAL CURRENCY SYSTEM PARTICIPANTS

An **exchanger (also sometimes called a virtual currency exchange)** is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

An **administrator** is a person or entity engaged as a business in **issuing** (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to **redeem** (withdraw from circulation) the virtual currency.

A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them (see definition of miner, below),and receive them as gifts, rewards, or as part of a free initial distribution.

A **miner** is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self-generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.

A wallet provider is an entity that provides a virtual currency wallet (i.e., a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet holds the user's private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. Wallets can be stored both online ("hot storage") or offline ("cold storage"). (Examples: Coinbase; Multibit; Bitcoin Wallet).

In addition, various **other entities** may participate in a virtual currency system and may be affiliated with or independent of exchangers and/or administrators. These include web **administration service providers (a.k.a. web administrators**); **third party payments senders** facilitating merchant acceptance; **software developers**; and **application providers** (some of the "other entities" listed in this paragraph may already fall into one of the categories above.). Applications and software development can be for legitimate purposes—e.g., to increase ease of merchant acceptance and customer payments or to respond to legitimate privacy concerns—or for illicit purposes—e.g., a mixer developer/operator can target illicit users with products designed to avoid regulatory and law enforcement scrutiny.

It must be emphasised that this list of participants is not exhaustive. Moreover, given the rapid development of virtual currency technologies and business models, additional participants could arise within virtual currency systems and pose potential AML/CFT risks.

Taxonomy of Virtual Currencies

	Centralised	**Decentralised**
Convertible	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin
Non-convertible	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

LEGITIMATE USES

Like other new payment methods, virtual currency has legitimate uses, with prominent venture capital firms investing in virtual currency start-ups. Virtual currency has the potential to improve

payment efficiency and reduce transaction costs for payments and fund transfers. For example, Bitcoin functions as a global currency that can avoid exchange fees, is currently processed with lower fees/charges than traditional credit and debit cards, and may potentially provide benefit to existing online payment systems, like Paypal.[16] Virtual currency may also facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the Internet, such as one-time game or music downloads. At present, as a practical matter, such items cannot be sold at an appropriately low per/unit cost because of the higher transaction costs associated with e.g., traditional credit and debit. Virtual currency may also facilitate international remittances and support financial inclusion in other ways, as new virtual currency-based products and services are developed that may potentially serve the under- and un-banked. Virtual currency - notably, Bitcoin- may also be held for investment. These potential benefits need to be carefully analysed, including whether claimed cost advantages will remain if virtual currency becomes subject to regulatory requirements similar to those that apply to other payments methods, and/or if exchange fees for cashing out into fiat currency are factored in, and whether volatility, consumer protection and other factors[17] limit their potential for financial inclusion.

POTENTIAL RISKS

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many of the reasons identified in the 2013 NPPS Guidance. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more

difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY

Law enforcement is already seeing cases that involve the abuse of virtual currency for money laundering purposes. Examples include:

LIBERTY RESERVE

In what is to date the largest online money-laundering case in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars).

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Russia Hackers," "Hacker Account," "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other

users, including front company "merchants" that accepted LR as payment. For an extra "privacy fee" (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.[18]

SILK ROAD

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600 000 bitcoins) in commissions for Silk Road. Hundreds of millions of dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of total sales price.

Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional "anonymisers," beyond the tumbler service built into Silk Road transactions (see discussion below).

Silk Road's payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user's Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user's bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user's / buyer's bitcoins from the escrow account to the vendor's Silk Road Bitcoin address. As a further step, Silk Road employed a "tumbler" for every purchase, which, as the site explained, "sen[t] all payments through a complex, semi-random series

of dummy transactions ... --making it nearly impossible to link your payment with any [bit]coins leaving the site."[19]

WESTERN EXPRESS INTERNATIONAL

An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyberfraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet "carding" web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.

The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the buyers. The money mover laundered the cybercrime group's illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds. One of the largest virtual currency exchangers in the United States, Western Express International exchanged a total of USD 15 million in WebMoney and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, plead guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more plead guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office.

NOTES

[1] The first draft of this paper was prepared jointly by Australia, Canada, Russia, the United Kingdom and the United States for the FATF meetings in February 2014. After that all delegations were invited to provide comments on the draft with a view to adopting a final paper at the next meeting. Comments were received from 10 delegations, and these have been taken into account in preparing this revision.

[2] "Bitcoin" (capitalised) refers to both the open source software used to create the virtual currency and the peer-to-peer (P2P) network formed as a result; "bitcoin" (lowercase) refers to the individual units of the virtual currency.

[3] It should also be noted that some observers, including former US Federal Reserve Chairman Alan Greenspan, Nout Wellink, a former President of the Dutch Central Bank, and Nobel Laureate economist Robert Shiller, maintain that virtual currency is a passing fad or bubble, akin to Tulipmania in 17th Century Netherlands.

[4] Virtual currency is a complex subject that implicates not only AML/CFT issues, but also other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards. The proposed vocabulary is thus relevant across a number of complementary regulatory jurisdictions. Adoption of consistent terms and a common conceptual understanding of virtual currency by all relevant government entities is important to avoid duplicating efforts and/or working at unintended cross purposes, and facilitates the capacity of governmental authorities to leverage their various perspectives and areas of expertise in order to most effectively identify and address relating to virtual currencies.

[5] **Digital representation** is a representation of something in the form of digital data—i.e., computerised data that is represented using discrete (discontinuous) values to embody information, as contrasted with continuous, or analog signals that behave in a continuous manner or represent information using a continuous function. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system,

[6] Legal tender status does not necessarily require an entity or individual to accept payment in a particular type of legal tender. For example, in many jurisdictions, a private business, person, or organisation is free to develop internal policies on whether or not to accept the jurisdiction's physical currency or coins (cash) as payment for goods and/or services.

[7] This definition differs from that offered in 2012 by the European Central Bank (ECB), which defined virtual currency "as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" ECB, *Virtual Currency Schemes* (October 2012), p. 6. The ECB recognised on p.13 of its report that its "definition may need to be adapted in future if fundamental characteristics change." Its definition now appears too limited, since math-based, decentralised virtual currencies like Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g., the United States, Sweden, and Thailand) now regulate virtual currencies.

[8] This categorisation differs from the ECB's three-part classification, which divides virtual currencies into three types: "Type 1 . . . refer[s] to closed virtual currency schemes . . . used in an online game. Type 2 . . . [refers to] schemes [that] have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can … be used to buy virtual goods and services . . . (and exceptionally also … real goods and services) . . . Type 3 [refers to] schemes . . .[with] bidirectional flows, i.e. the virtual currency . . . acts like any . . . convertible [real] currency, with . . . [buy and sell] exchange rates . . . [and] can . . . be used to buy [both] virtual . . . [and] real goods and services." ECB *Virtual Currency Schemes*, p. 6. This discussion paper adopts a simpler, bifurcated classification because at present, only (fully) convertible virtual currencies that can be used to move value into and out of the formal financial sector present significant AML/CFT risks. This is because money laundering requires: Conversion or transfer (of illicit funds); concealment or disguise of the source/origin (of illicit funds); or acquisition/possession/use (of illicit funds).

[9] Some convertible virtual currencies can be exchanged directly through the issuing administrator (directly exchanged); others must be exchanged through a virtual currency exchanger (third-party exchanged).

[10] For example, WebMoney is a virtual currency because "valuables" (assets) are transferred and stored in the form of a non-fiat currency, The units of measurement of the valuables' property rights stored by the guarantor are WebMoney Title Units (WM) of the corresponding type. http://wmtransfer.com/eng/about/

[11] For example, despite such deterrence measures, several exchanges allow blackmarket conversion of World of Warcraft Gold.

[12] A third-party is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction—i.e., a third party functions as a neutral entity between the principals (e.g., sender and receiver, buyer and seller) in a business or financial transaction. The third party's involvement varies with the type of business or financial transaction. For example, an online payment portal, such as PayPal, acts as a third party in a retail transaction. A seller offers a good or service; a buyer uses a credit or debit card entered through the PayPal payment service; and the trusted third party completes the financial transfer. Similarly, in a real estate transaction, a third-party escrow company acts as a neutral agent between the buyer and seller, collecting the documents from the seller and money from the buyer that the two principals need to exchange to complete the transaction.

[13] Distributed is a term of art that refers to an essential feature of decentralised math-based virtual currencies: transactions are validated by a *distributed* proof-of-work system. Each transaction is *distributed* among a network of participants who run the algorithm to validate the transaction.

[14] Apart from the initial creation and issuance of ripple coins (RXP), Ripple operates as a decentralised virtual currency. Ripple's founders created all 100 billion ripple coins and retained 20 billion of them, with the remainder to be distributed by a separate entity, Ripple Labs. However, all transactions are verified by a decentralised computer network, using Ripple's open source protocol, and recorded in a shared ledger that is a constantly updated database of Ripple accounts and transactions.

[15] In 2140, the block award will cease to be available and miners will be rewarded only by transaction fees.

[16] For example, PayPal is actively looking at accepting and clearing bitcoins on the PayPal platform, and JP Morgan Chase has filed a US patent application for an online electronic payments system using a math-based virtual currency protocol that would enable users to make anonymous payments without providing an account number or name, with the virtual currency to be stored on JPMC computers and verified through a shared log, much like the 'block chain' in the bitcoin system.

[17] For instance, it remains to be seen whether virtual currency systems can provide a pathway to other financial services, like credit and insurance.

[18] The Liberty Reserve investigation and takedown involved law enforcement action in 18 countries and jurisdictions, including Costa Rica; the Netherlands; Spain; Morocco; Sweden; Switzerland; Cyprus; Australia; China; Hong Kong, China; Norway; Latvia; Luxembourg; the United Kingdom; Russia; Canada; and the United States to restrain criminal proceeds, forfeit domain names, and seize servers.

[19] The Silk Road investigation involved multiple US law enforcement agencies, led the Federal Bureau of Investigation's (FBI')s New York Special Operations and Cyber Division, and the Drug Enforcement Administration's (DEA's) New York Organized Crime Drug Enforcement Strike Force (comprised of agents and officers of DEA, the Internal Revenue Service (IRS), the New York City Police Department, US Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the US Secret Service, the US Marshals Service, Office of Foreign Assets Control (OFAC), and NY Department of Taxation), with assistance and support of the ICE-HIS Chicago field office, the Department of Justice's Computer Crime and Intellectual Property and Asset Forfeiture and Money Laundering Sections, the United States Attorney's Office for the Southern District of New York, and foreign law enforcement partners, particularly the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

BIBLIOGRAPHY AND SOURCES

FATF (2013), FATF *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services,* FATF, Paris
www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

Popper, N. (2013), "In Bitcoin's Orbit: Rival Virtual Currencies vie for Acceptance", in *New York Times, Dealb%k,* (Nov. 24, 2013) http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0, accessed June 2014.

Appendix BB:

FATF, *FATF Report: The Role of Hawala and other Similar Service Providers in Money Laundering and Terrorist Financing* (Paris: FATF, 2013)

FATF

FATF REPORT

THE ROLE OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS IN MONEY LAUNDERING AND TERRORIST FINANCING

October 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

ACRONYMS

AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
CDD	Customer Due Diligence
CFT	Combatting the financing of terrorism
DNFBP	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HOSSP	Hawala and Other Similar Service Provider
MLA	Mutual Legal Assistance
MSB	Money Service Business
MSOs	Money Service Operators
MVTS	Money or Value Transfer Services
STR	Suspicious Transaction Report

EXECUTIVE SUMMARY

Twelve years after September 11th and the adoption of Special Recommendation VI on Alternative Remittance Systems, two often competing and conflicting views on *hawala* still stand. Many countries and communities, as well as the development community, view them as essential providers of financial services to the unbanked in countries with limited financial access. In significant numbers of jurisdictions and sometimes in the same jurisdiction, law enforcement views them as one of the leading channels for terrorist financing and money laundering.

Against this background, this typology seeks to demystify *hawala* and similar service providers. It seeks to provide a facts-based review of the extent of their vulnerability, as of today, to money laundering and terrorist financing. To this end, the typology project team sought input from members of the FATF and FATF-style regional bodies. The team received feed-back from 33 countries to a survey it had developed.

The term *hawala* is used in a number of jurisdictions and is associated with a money transfer mechanism that operated extensively in South Asia many centuries ago, and which still exists there, as well in the Middle East, and in Africa. In others countries, it has several different connotations in particular illegal money transmitter and in others, the term *hawala* is neither used nor understood, however, the service of remitting money may be covered by the country's legislative framework.

Hawala in fact is not a universal term. Still, there appears to be a universal recognition of the existence of *hawala* or *hawala*-like providers across jurisdictions, in so far as they present unique characteristics, focused on their settlement mechanisms. Recognizing this, this typology uses a broader term than *hawala* and instead focuses on "*hawala* and other similar service providers" or HOSSPs.

HOSSPs, for the purpose of the typology, are defined as money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. Some HOSSPs have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *underground banking*. While they often use banking channels to settle between receiving and pay-out agents, what makes them distinct from other money transmitters is their use of non-bank settlement methods, including settlement via trade and cash, as well as prolonged settlement time. There is also a general agreement as to what they are not: global money transfer networks (including agents) operated by large multinational money transmitters and money transfers carried out through new payment methods including mobile money remittance services. This description is based on *services* provided by them and *not their legal status*.

HOSSPs are used in some jurisdictions by legitimate customers for reasons of geography, culture, and lack of banking access. They are also used by individuals and entities seeking to evade currency controls, tax obligations, and sanctions. HOSSPs generally are cash-in and cash out businesses that primarily send personal remittances of low value. They generally operate in areas with a high percentage of expatriate workers and are visible to members of that community. They often run businesses other than money transfer, particularly currency exchange.

This typology reviews three major types of HOSSPs: pure traditional (legitimate) ones; hybrid traditional (often unwitting) ones; and criminal (complicit) ones. Distinct ML/FT risks apply to each. Pure traditional HOSSPs tend to be popular because of familial, regional or tribal affiliation and inadequate access to regulated financial services for senders/recipients in origin/receiver countries. Hybrid traditional HOSSPs also serve legitimate customers, but at the same time are used, wittingly or not, for illegitimate purposes to transfer funds cross-border. Criminal HOSSPs, on the other hand, are set up or expanded to service criminals.

Surveyed countries gave a number of reasons for the continued existence of HOSSPs, including their competitive pricing, faster money transmission, cultural preference, lack of banking access, low confidence in the banking system, as well as deliberate transfer or concealment of criminal proceeds and evasion of currency controls, sanctions, and taxes. At the same time, the typology highlights that many of the assumptions on HOSSPs are outdated. For instance, they, in some jurisdictions, offer services well beyond money transmission. More universally, they often have detailed records; are not necessarily based upon trust; often are highly visible to the community they serve; and are not always high risk. Further, they ultimately often settle through banks, meaning that banks that have been provided with high risk indicators by their authorities are positioned to identify suspicious activities and notify their authorities accordingly.

The typology explains the different settlement mechanisms used by HOSSPs, including simple reverse transactions, triangular settlement, settlement through value, and the use of cash couriers. It provides country-specific examples, as well outlines their communication techniques that in some cases permit the instant availability of funds. It finds that most countries cannot provide estimates on the scale of unregulated HOSSPs or their relative threat.

As always the case when criminals own or control financial intermediaries, criminal HOSSPs deserve particular attention. Although a limited number of case studies were provided to the project team, there are several reasons why HOSSPs continue to pose a money laundering and terrorist financing vulnerability. These include a lack of supervisory will or resources; settlement across multiple jurisdictions through value or cash outside of the banking system in some cases; the use of businesses that are not regulated financial institutions; the use of net settlement and the commingling of licit and illicit proceeds. While the settlement through value or trade that masks the individual fund transfers is a source of vulnerability, the most significant reason for concern is lack of supervisory resources and commitment to effective regulation.

Out of the cases gathered for this typology, a picture emerges of common elements used by *criminal* HOSSPs, including control by a professional third party money launderer called a controller or money broker, depending upon the jurisdiction. Based upon existing case studies, it appears that HOSSPs can also be abused or used for import and export fraud, to launder drug proceeds, and to evade sanctions.

Similarly, the typology's case studies provide examples of terrorists still using HOSSPs to move funds twelve years after 9/11. They are used for reasons of familiarity, culture, extensive international reach, speed of transfers, and often lax supervision or lack of political will. The latter factors make it more likely that these institutions may lack robust AML/CFT controls, making them attractive to criminals and terrorist financiers.

A slight majority of surveyed countries bar HOSSPs from operating legally. Those that allow them to operate legally, provided they license/register with the relevant authorities and comply with relevant AML/CFT and other laws, largely believe that legalization of HOSSPs helped expand remittances through legal channels. However, in most jurisdictions that allow HOSSPs to operate legally, relatively few HOSSPs have actually registered or become licensed, with a few notable exceptions.

Effective supervision of HOSSPs is one of the primary challenges facing regulators and their governments. Most countries do not appear to have separate examiner teams for HOSSPs. While most have criminal, civil, and, to a lesser extent, administrative sanctions available for violations of AML/CFT obligations, many countries do not appear to have used these sanctions. Few countries require that money transmitters, including legal HOSSPs, should only partner with money transmitters in pay-out countries that are legally licensed or registered. The absence of requirements on foreign counterparties may be a critical vulnerability posed by money transmitters, including HOSSPs and further consideration of the application of Recommendation 13 in the context of money transmitters offering cross-border may be beneficial. Similarly, the absence of more than a handful of case studies involving international cooperation suggests that further discussion is warranted on how law enforcement or other competent authorities can better obtain the tools and expertise needed to tackle HOSSPs involved in money laundering or terrorist financing.

In the first decade after 9/11, the globe has been largely ineffective in supervising HOSSPs. The international community can address the resulting vulnerability by bringing the HOSSPs under a risk-based AML/CFT regulatory and supervisory framework that is effectively implemented. FATF could take these findings into account when it considers the policy implications of this report.

Note: The findings highlighted in this report should also be useful to other streams of work at the FATF, within national governments and for other stakeholders, for example in relation to the implementation of the FATF Standards.

CHAPTER 1: SCOPE OF THE PROJECT

The scope of the project is a discussion of typology and role of *hawala* and other similar service providers (HOSSPs) in money laundering and terrorist financing. HOSSPs are a subset of money or value transfer services (MVTS).

MVTS are defined by Financial Action Task Force (FATF) as financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods.

One key lesson from the survey questionnaire prepared by the typology project team and distributed to members of FATF and FSRBs and discussed at the typology workshop held in Dakar, Senegal in 2012[1] is that there is no common definition to the term *hawala*, which is interpreted in varied ways, having different meanings across jurisdictions. Some HOSSPs have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *underground banking*.

The term *hawala* is traditionally associated with a money transfer mechanism that operated extensively in South Asia many centuries ago and had strong links along traditional trade routes in Middle East and parts of East Africa. It operated as a closed system within corridors linked by family, tribe or ethnicity. In recent times, the term *hawala* has often been used as a "proxy" to describe a wider range of financial service providers, beyond these traditional and geographically tied systems.

In other countries, the term *hawala* is actually not used at all. However, there is a general recognition of the existence of *hawala* or *hawala-like* providers in many jurisdictions and of the type of methods they use and services they provide. There is also a general agreement as to what they are not: global money transfer networks (including agents) operated by large multinational money transmitters and money transfers carried out through new payment methods including mobile money remittance services.

Based on experience across countries, HOSSPs provide both legitimate and illegitimate services. They are money transfer service providers that are legal in certain countries if registered or licensed and illegal in others. In other countries, HOSSPs are referred only within the context of underground or criminal money transfer services.

For the purpose of this typology, HOSSPs are defined as money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time.

[1] The 11-member project team prepared a 47 question questionnaire, which was circulated to the FATF membership and to the FSRBS in September 2012. The APG sent an abbreviated version of the questionnaire to its members. Received questionnaire results were discussed at a typology workshop in Dakar, Senegal in November 2012.

While HOSSPs often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other settlement methods, including trade, cash, and long-term net settlement. Against this background, it is important to highlight that the definition of "*hawala* and other similar service providers" is based on the services provided by them and is irrespective of their legal status.

As described below, why HOSSPs exist and their services are utilized reflects a rather diverse set of reasons, often linked to country-specific circumstances. These include reasons of history, geography, culture, lack of banking access, currency controls, tax evasion and sanctions circumvention which create a demand and a market, or lead to the emergence of the provision of services described in this report.

This Chapter will explain the attributes of *hawala* and other similar service providers, how HOSSPs operate, what services are provided by them, who uses their services and what technology is used to transmit customer and transaction related information. It includes a discussion on the different formats of *hawala* and other similar service providers operations and the scale and nature of the "*hawala* and other similar" markets around the world.

1.1 ATTRIBUTES OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

H*awala* and other similar service providers share many attributes with other money transmitters. Like many other money transmitters, HOSSPs generally:

a. Are cash-in and cash-out businesses that primarily send personal remittances of low value. This does not preclude them from sending high value business transfers.

b. Operate in areas with high percentages of expatriate workers (in particular in originating countries), often in competition with other money transmitters.

c. Offer legitimate financial services to migrants sending remittances; however, they can also be used (or abused) for illegitimate purposes to move illegal/illicit money across the borders.

d. Operate within a community, are visible and accessible to their customers, are able to know their customers and maintain accurate records sufficient to ensure they complete transactions whilst preserving their profit

e. Run other businesses in addition to money transfer.

f. Belong to networks of similar operators in other countries.

g. Communicate only limited information on the customer and beneficiary as far as individual transactions are concerned. This communication is limited to what is needed to complete the transaction. This information generally includes the beneficiary name, contact number and may also include a transaction reference number (code number/words to identify recipients), in order to ensure that the delivery is made to the right person in an efficient manner.

HOSSPs tend to use specific and distinct settlement tools: They settle through trade, cash courier or net settlement, often without any direct wire transfer between the originator and beneficiary.

However, they may also send wire transfers aggregating funds received through individual remitters through the international banking system. In addition, they sometimes reconcile/settle through third party payments, which may lead to long settlement durations.

1.2 TYPES OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS CATEGORIZED BY LEGITIMATE AND ILLICIT USE

For the purposes of this typology, there are three major types of *hawala* and other similar service providers that operate across the globe as categorized by legitimate and illicit use – to which distinct ML/FT risks apply:

- **Pure traditional** (legitimate) *hawala* and other similar service providers;
- **Hybrid traditional** (sometimes unwitting) *hawala* and other similar service providers and
- **Criminal** (complicit) *hawala* and other similar service providers

PURE TRADITIONAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

In South Asia and Middle East, the word *hawala* is commonly used to refer to "Pure Traditional *Hawala*", a centuries-old money transmission system which was often used for trade-finance. These systems have operated for centuries in an unregulated environment and are still present in some countries for trade-finance and personal remittances, sometimes under a regulatory umbrella, but more typically not. Pure Traditional *Hawala* and other similar service providers are also extensively used to send low-value remittances on behalf of individuals, for example, migrant workers – extending outside their historical geographical area as populations migrate and trade routes develop. For instance, *hawala* are a common provider for remittances to migrant workers in the United Arab Emirates, where a significant portion of the working class population is composed of expatriates. Pure Traditional *Hawala* and other similar service providers tend to be popular among migrants because of familial, regional or tribal affiliation and inadequate access to regulated financial services for senders/recipients in origin/ receiver countries. These service providers may primarily function to provide legitimate and efficient remittance/trade finance services to customers sending low value transactions. If sufficiently regulated and supervised, these providers, due to the low value of their average transactions, may present a low or lower money laundering and terrorist financing vulnerability. Minimal supervision in certain jurisdictions, however, may amplify the risk for misuse.

HYBRID TRADITIONAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Hybrid Traditional *Hawala* and other similar service providers or designated non-financial institutions or designated non-financial businesses and professions (DNFBPs) in the provision of legitimate services but at the same time they may also be used, wittingly or are also used, wittingly or not, for illegitimate purposes such as transmission of illicit money across the borders. These networks are not primarily set up to move illicit money but may be involved in illegal activities such as movement of money generated from tax evasion, to evade currency controls and to avoid sanctions, etc. These service providers utilize similar methods as traditional HOSSPs and are not a

part of a criminal network. They develop where there is an un-serviced demand for remittances; they may interact with other HOSSPs to complete transactions.

CRIMINAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

In some countries, there is concern that HOSSPs systems are increasingly being set up or expanded to service criminals. Providers who set up such systems are described in this report as "Criminal HOSSPs". Such systems are driven by illegitimate money flows and are often controlled by criminals or criminal groups. They therefore represent a high criminal money laundering and terrorist financing risk. A third party professional money launderer often runs the financial network. These criminal networks also enable other offences including tax fraud, currency offences and corruption. Criminal *Hawala* and other similar service providers are often a part of well-developed criminal networks that have been developed specifically to enable illegitimate activities. Initially these channels may be developed as networks to satisfy local/personal remittance needs by Traditional or Hybrid *Hawala* and other similar service providers. As the network grows into a strong transfer corridor, it becomes attractive to criminals and evolves into a criminal transfer corridor. These criminal networks are characterized by high value transactions between legal and natural persons that do not necessarily share the same cultural or geographic background. They are often used to send payments to countries with developed and regulated banking systems.

1.3 COMMON CHARACTERISTICS OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

This sub-section describes the common characteristics of "*Hawala* and Other Similar Service Providers" based on survey[2] results, previous FATF work on alternate remittance services, literature review and country presentations at *hawala* typology workshop. The descriptions are also influenced by the lack of a common definition or understanding of what HOSSPs are. All the characteristics may not always be present in all the countries of operations. In other words, only some of these characteristics may be present in some countries.

Generally *hawala* and other similar service providers include:

a. Illegal or unlicensed/unregistered money transmitters. More than half of the respondents confirmed that HOSSPs are generally either unregulated or illegal in their country. In most of the countries, *hawala* and other similar service providers have not traditionally been subject to any regulatory oversight. However, recent efforts have resulted in the shifting of *hawala* and other similar service providers into the regulated financial sector in several countries. In 50% of the countries that responded to the question, *hawala* and other similar service providers are now regulated. In some countries, the process of regulation is in its very early stage.

[2] Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, 22 countries provided an answer to this question and three countries could not because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

b. Alternative remittance providers that transfers funds outside of banks or other regulated financial institutions. All except one of the surveyed countries that responded to the question agreed to this, and this characteristic is the only one that is common in most of the surveyed countries.

c. Money transmitters that use net settlement with payout agents actually transferring no funds. In net settlement, there are no funds transferred for each and every transaction that takes place between *hawala* and other similar service providers. For these individual transactions, *hawaladar* (a money transmitter that provides *hawala* services) and similar service providers use their local cash pool to pay the beneficiary. After a set period of time (example after a month) only the net amount owed between the two *hawaladars* and other similar service providers is settled. About 80% of the surveyed countries concur that net settlement without transfer of funds is the most common settlement process used in their country by *hawala* and other similar service providers.

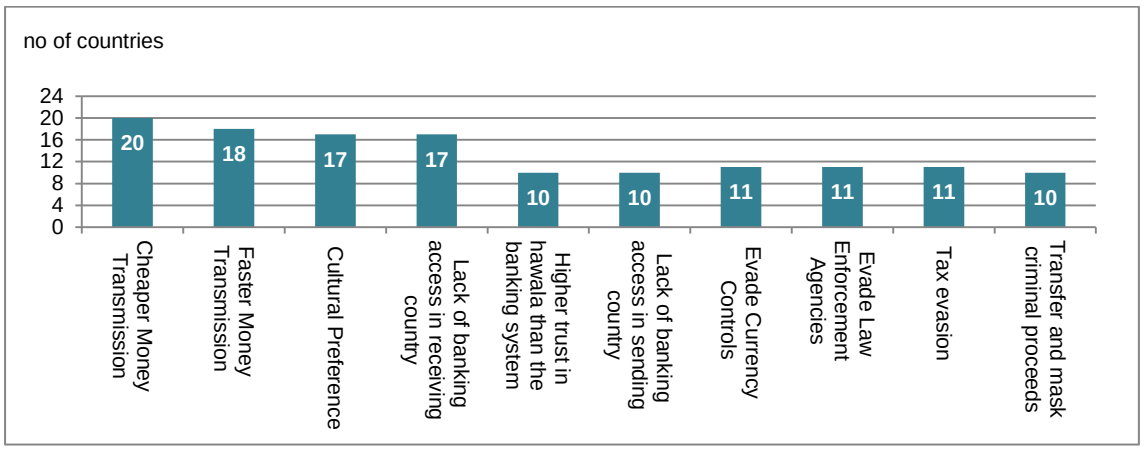
d. Money transmitters that settle through equivalent value instead of monetary instruments. Settlement through value may take place through trade transactions, such as merchandise or other commodities. At times, *hawaladar* and other similar service providers that owe debt to corresponding providers settle accounts by fulfilling commercial obligations of such corresponding providers such as paying a debt or invoice of same value that they owe. This approach is used in 68%of the countries that responded to the question.

e. Money transmitters that often only serve specific diaspora communities. About 32% of the countries believed that *hawala* and other similar systems serviced only specific communities. Traditionally, *hawala* and other similar channels were described as groups or networks that were based on familial, regional, or tribal affiliation. In recent times, *hawala* and other similar service providers have started servicing wider networks, but this is still an emerging trend.

1.4 REASONS *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS EXIST

This section highlights the main reasons for existence of *hawala* and other similar service providers in various countries. The survey sought information on what needs *hawala* and other similar service providers fulfil in the surveyed countries. Figure 1.1 below highlights the main reasons put forward and their frequency. As it can be observed, there are significant differences in the responses received, highlighting a noticeable disparity across countries, reflecting themselves the different characteristics of *hawala* and other similar service providers. Some characteristics are more prevalent in some countries than others. The responses indicated that some of the answers are not based on specific real-life examples, but more on perceptions of the roles and characteristics of HOSSPs.

Figure 1.1 **Reasons for Existence of *Hawala* and Other Similar Service Providers – Survey Result**



Source: F*ATF project questionnaire.*

Note: Only FATF member countries responded to this question. Out of 25 FATF member countries that responded 22 countries provided an answer to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

The most common reasons cited were:

a. **Cheaper Money Transmission:** *hawala* and other similar service providers usually charge 25-50% of the equivalent bank charge depending on destination of transfer, according to the responses of some countries. Depending upon the jurisdiction, customers generally obtain better exchange rates from HOSSPs than from the banks because they operate with very low overheads.

b. **Faster Money Transmission:** *hawala* and other similar service providers may have a vast network of counterparties located in specific countries. Money transmission can be completed in few hours or at the most in one or two days. In the same locations, banks can often take a few days or even longer in certain jurisdictions, to send an international wire transfer and money transmission networks may be unable or limited in their ability to compete. One of the reasons for quick transmission of funds under HOSSPs is that operators do not transfer cash for every client transaction, often resort to net settlement as do many other types of MVTS.

c. **Cultural Preference:** HOSSPs have existed for a long time in some areas of Central Asia, South Asia and Middle East, even long before the modern banking started operating. So it can be a cultural tradition for the people in these areas to transfer money through traditional *hawala* and other similar service providers. In many developed countries, such channels are primarily used by migrants because of ease of rapport building and access between *hawaladars* and other similar service providers and their customers, who share similar customs, lifestyle and language.

d. **Lack of Banking Access in Remittance Receiving and Sending Country:** Many remittance receiving countries have underdeveloped financial systems. In such

countries, *hawala* and other similar service providers have the ability to deliver money to distant locations where regulated channels do not exist. Countries like Nepal, Pakistan or some countries in North Africa and the Middle East are good examples of such situation. HOSSPs are also often the only channel through which funds can be transmitted in certain conflict regions like in parts of Somalia and parts of Afghanistan[3]. These remittance transfers are the safest, easiest and cheapest way to transfer funds in these countries.

In addition, on the remittance sending country side, where banking access is more developed, *hawala* and other similar service providers are often used by illegal foreign migrants residing in developed countries. Their illegal immigration status precludes these clients to access banks and other regulated financial services providers – leaving only limited cost-effective alternatives like unregulated service providers to send remittances to their families. It is worth emphasizing though that legal resident and migrants also extensively use these service providers for the other reasons stated in this section.

e. **Higher Confidence in *Hawala* and other similar service providers than in the banking system:** This is true in countries where there is a cultural lack of confidence towards banks – in particular in countries where customers have in the past lost their deposits when bank failures occurred. The limited understanding or familiarity with traditional financial services due to lack of financial literacy may be another reason explaining this lack of confidence towards regulated financial institutions. Finally, language barriers are likely to be a significant hurdle for immigrant populations.

f. **Evade Currency controls and international sanctions:** Responses to the survey highlight how, in some specific circumstances, *hawala* and other similar service providers seem to have been used to circumvent restrictions applying to international transactions – for instance exchange controls or international sanctions. These responses and examples show how *hawala* and other similar channels are used to bypass currency controls or international sanctions that increase money laundering and terrorist financing risks.

g. **Evade Taxes:** Responses note *hawala* and other similar service providers are used to evade taxes - as the tax authority have access to records kept in banks, but usually do not have the same tools for HOSSPs and other similar service providers – or do not even try to trace transactions in such circumstances. The use by commercial businesses of unregulated networks (instead of official financial service providers) may signal the underlying intention of concealing the funds being transferred for tax evasion purposes or to avoid sanctions.

h. **Transfer or Conceal Criminal Proceeds:** Responses note that criminals are perceived to prefer to use HOSSPs to transfer funds because commitment to CDD procedures performed by some *hawaladars* are not believed to be as rigorous and

[3] A 2005 World Bank study estimated that 80 to 90 per cent of Afghanistan's economic activity at that time was facilitated by *hawala*.

deep as those of banks and other regulated financial institutions, and are less likely to be accessible to the authorities. Therefore where holders of illicit funds have access to HOSSPs and the operators are willing to serve them, it is thought easier to transfer criminal money through these channels. In addition, tracing the money flow by the competent authorities may be made more challenging because, even when records are kept they can be falsified (ranging from counterfeit or hijacked customer identities to complete sets of entirely fictitious business records), making them, less easily followed by law enforcement.

This summary highlights that *hawala* and other similar service providers offer services for legitimate purposes, but can also be abused – or set up for criminal purposes. The level of regulation of HOSSPs at both ends of a remittance (and their actual implementation of AML/CFT requirements) has a link to their level of risk.

1.5 OUTDATED ASSUMPTIONS

Some surveyed countries also noted that some of widely repeated characteristics of pure traditional *hawala* do not necessarily match the reality in all the countries, particularly in Western Europe and North America. These were referred to as "***Hawala* Myths**".

a. **An ancient and static system:** Even pure traditional *hawala* is actually an ever evolving one. Country experiences suggest that entities within licit network adapt their structure and methods to ensure remittance corridors are serviced efficiently. Each end of a remittance reflects the rules, regulations and context that they operate in. In many countries, an operation described as *hawala* looks and acts the same as a MSB in another country.

b. **Remittance system only, it also offers other financial services:** In its heartland, "pure traditional *hawala*" are not pure remittance systems. Apart from sending remittances, they also usually offer other financial services such as currency exchange, and in some jurisdictions, short term lending, trade guarantees, and safe keeping of funds. In some countries, they may operate as pawn shops, travel agencies and mobile phone shops.

c. **Paperless system:** Many *hawala* investigations have revealed that *hawaladars* and similar service providers actually keep detailed records. They maintain manual accounts, ledgers, computerized records or a combination of these. The businesses of some *hawaladars* are based on small margins of profit, and recording and tracking deposits, payments and transfers is important to their good reputation and efficiency; alternatively HOSSPs that service the criminal market need to keep detailed records in order to keep track of transactions completed through complex settlement methods such as third party payments and trade transactions.

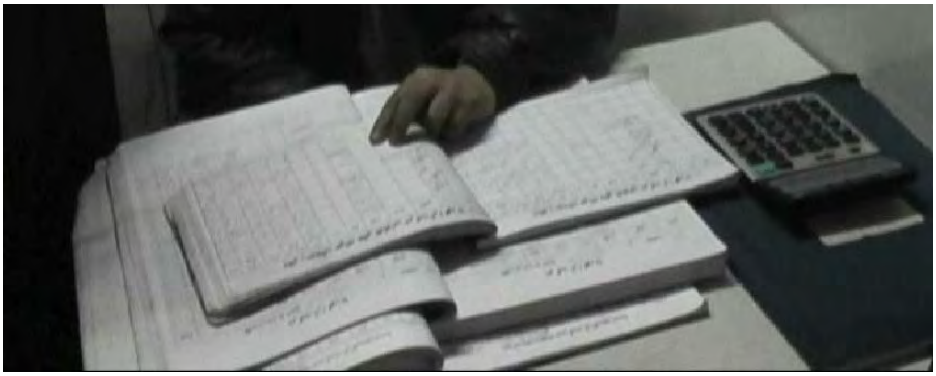


Image 1. **Hawala ledgers from Hawala Bazaar in Kabul, Afghanistan**

d. **Always Cheaper:** "*hawala* and other similar service providers'" transactions may be cheap but only within defined and specific corridors. Their competiveness is highest where customers need to send money to areas where traditional banking systems and large money transmitter's chains find it difficult, expensive or a high risk to operate. When such conditions are not met, the cost of sending funds through *hawala* and other similar service providers may actually not be that competitive.

e. **Trust based system of money transmission:** *hawala* are often defined as a trust-based system of money transmission. Rather than trust, *hawaladars* and other similar service providers actually rely on reputation for effective delivery. The customer chooses a *hawaladar* or other similar service provider because of their reputation for performance and this reputation is quickly lost when performance slips. *Hawaladar* and other similar service providers are also often relatively respected individuals within their community and success of their business is performance based.

f. **Underground:** In many countries, *hawaladars* and other similar service providers are actually highly visible within the community they serve and may even advertise their services openly (even when they are not a regulated or licensed or registered business).

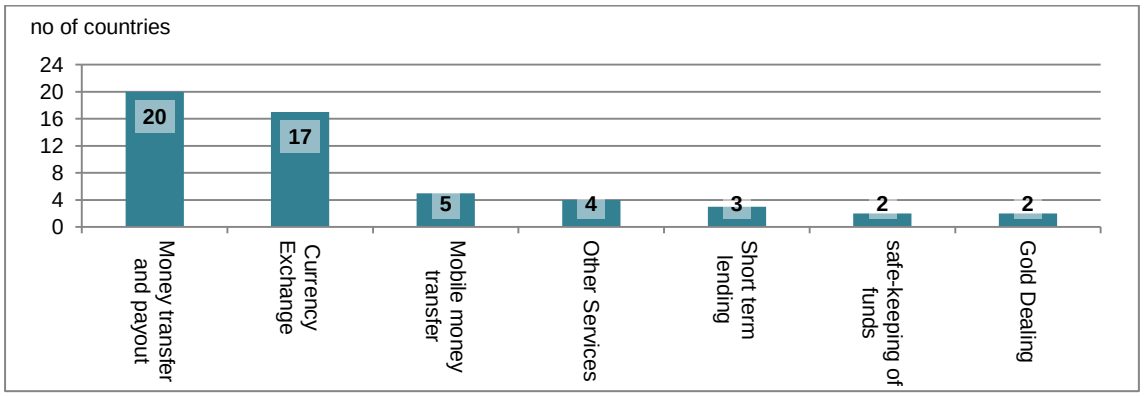
g. **High Risk always:** Depending on the type of *hawala* or other similar service provider and on the kind of services provided, the risk profile may actually differ significantly. The risk profile of the *hawala* and other similar services providers is dependent on its customer's risk profile, among others. *Hawala* transactions can be a lower risk if, for example, the service is provided by a regulated entity or entails low value transactions on behalf of low risk individuals.

1.6 SERVICES PROVIDED BY *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

The survey results as shown in Figure 1.2 summarize the feed-back on the types of services predominantly provided by *hawala* and other similar service providers. The two most common financial services provided are: 1) money transfer and pay-out and 2) currency exchange. Besides these services, *hawala* and other similar service providers may offer other services such as safe-

keeping of funds for the clients, short-term lending, mobile money transfers etc. although these are not as common.

Figure 1.2 **Financial Services provided by *Hawala* and Other Similar Service Providers**

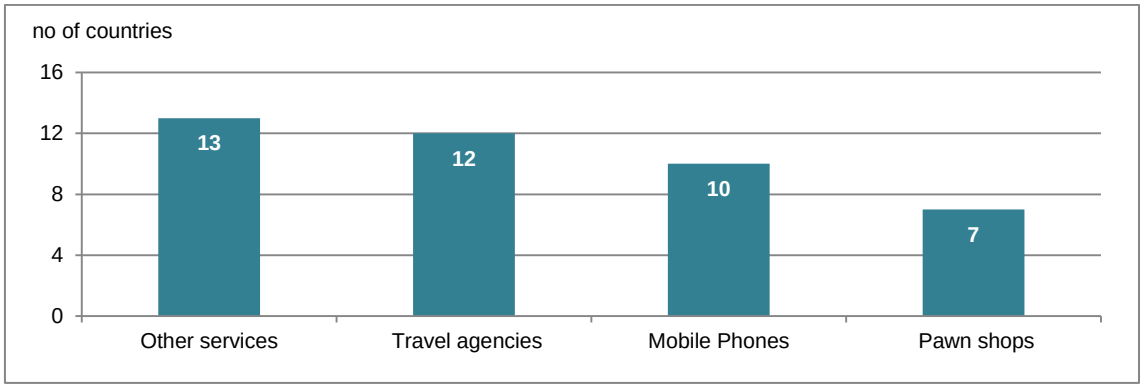


Source: FATF project questionnaire.

Note: Only FATF member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, 1 country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Apart from financial services, in many of the surveyed countries, *hawala* and other similar service providers also operate other business (see Figure 1.3). Typical side-line retail business includes travel agencies, pawn shops, selling mobile phones, SIM cards and mobile top-up cards. Many of them also operate as travel agents. In some cases they also operate as community specific grocers. Grocery stores are a typical venue for *hawaladars* and other similar services providers to conduct their remittance business. Many of them also provide import –export business – which creates an enabling environment for value settlement – in particular over-under invoicing when remitting funds to other geographic locations. Some *hawala* and other similar service providers also operate out of neighbourhood businesses, such as nail salons, beauty salons, flower shops etc. Such businesses not only generate more business for the service providers, but also provide a veil without being easily identified by regulators and law enforcement agencies. By running an additional business such as a travel or ticket agency or freight forwarding, criminal HOSSPs can derive an additional benefit that provides them with a ready supply of customer identity documents, which can be 'hijacked' and used to generate false customer records which are used to mask the receipt of criminally derived cash.

Figure 1.3 **Businesses Operated by *Hawala* and Other Similar Service Providers**



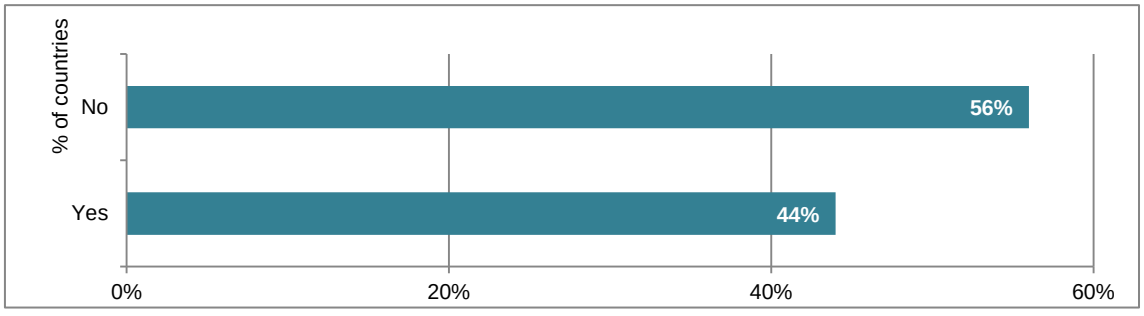
Source: FATF project questionnaire.

Note: Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, only 16 countries provided an answer to this question, 6 countries did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and Other Similar Service Providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

1.7 PROVIDING SERVICES TO UNBANKED

In a large minority of countries, HOSSPs are believed to provide services to the unbanked. Twenty five[4] surveyed countries answered the question whether HOSSPs provide legitimate financial service to the unbanked and under-banked in their country. Of those surveyed, 44% of the countries answered positively as shown in Figure 1.4. In the majority of the surveyed countries where HOSSPs are legal, they are considered to play an important role in providing financial services to the unbanked population, facilitate migrant remittances that support development, with the majority of the transactions being for overseas legitimate family support.

Figure 1.4 **Do HOSSPs Provide Legitimate Financial Service to the Unbanked?**



Source: FATF project questionnaire.

[4] Both FATF and APG member countries responded to this question. Out of 25 FATF member countries that responded 19 countries provided an answer to this question, 3 countries did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. Out of 8 APG member countries that responded 6 countries provided an answer to this question, 1 country did not respond to this question and 1 country could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country.

1.8 SETTLEMENT MECHANISMS USED BY *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

As noted above, settlement in the context of *hawala* and other similar service providers generally takes place through net settlement, with recourse to value settlement. The use of net settlement by HOSSPs is not unique, but a technique also often used by banks and other money transmitters. The use of value to settle is unique. Some however also use actual transfer of funds for the settlement purpose. Most of the regulated *hawala* and other similar service providers use regulated channels, such as the banking system, to settle if their respective ledger does not balance after certain time period.

In this context, the most frequent methods of settlement used by *hawala* and other similar service providers include:

a. Simple "reverse *hawala*": a remittance or payment going in the opposite direction. For example, an individual customer wants to send money from US to India. The service provider in the US will ask his counterpart in India to make a payment to the beneficiary in India. For this transaction, there is no transfer of funds between the two service providers, and the service provider in India will use his local cash pool to make the payments. To settle the accounts, sometime in the future the US service provider will make a payment to a beneficiary in US on behalf of a customer of the service provider in India. Over a period of time, the overall net amount of transactions may balance. When this does not occur, notably if the aggregate remittance flows are highly asymmetrical among countries, net settlement then takes place – often through wire transfers through the banking system.

b. "Triangular" settlement with networks of service providers. *Hawaladars* and other similar service providers may operate within a network that is spread across many jurisdictions. They use cross-provider balances on each other and correspondents to settle their respective accounts. In the above example, the service providers in the US and India both operate within the same broader network. After the initial transaction, the US service provider owes the Indian one. At the same time, the service provider in India has a customer who wants to send money to Somalia. If the service provider in India doesn't have any counterpart in Somalia, he would seek assistance from his counterpart in the US to identify a counterpart service provider in Somalia who owes debt to the US one. Once the Somalia service provider pays the beneficiary on behalf of the Indian one, all accounts are settled.

c. Value settlement through trade transactions, including through over or under invoicing. This type of arrangement is a common practice in Afghanistan, Iran, Pakistan and Somalia. In this case, operators use a surplus of cash or banked money to fund trade payments at the request of a business which in turn pays the individual recipients in the remittance destination region. International controllers or money brokers involved in criminal HOSSPs often settle by conducting completely separate trade transactions with criminally derived cash in their control.

d. Settlement through cash transport – notably cash couriers, including cross border.

Box 1.1 **Country Examples of Settlement procedures given by survey respondents**

Belgium: In some cases money remitters (HOSSPs) used the banking system to transfer bulk funds received from different clients to the bank account of hawaladars in Dubai. From there on, the money is send to the beneficiaries' in East-African countries using settlement through value or mobile payment systems. In other cases, money was directly transferred from Belgium to Pakistan using settlement through value, licensed money remitters and the regular banking system.

Sweden: Money is generally not moved physically or electronically at the time of the individual (usually rather small) payment order. Each month or at agreed point in time there is a settlement or clearance of transactions between the Swedish agent and the foreign agent. The difference is sent from the Swedish agent to the foreign (local) agent in one big lump sum through a Swedish bank to the bank account of the agent overseas. Settlement may also take place with merchandise or other commodities. In recent years it has also become more frequent that individuals (with or without their own business) make their own bank accounts available to international payment transfers.

Chinese Taipei: "Underground Money shops" (the Chinese term for HOSSPs) settle transactions either by direct remittances, cross-border transportation of precious metals, cash or mingling remittance transfer with trade accounts. In some recent cases, settlements were done through Western Union Remittance System and China Union Pay Cards as well.

Italy: Evidence from STRs in Italy suggest that HOSSPs may collect remittances from their customers (usually belonging to their own diaspora communities) and perform bulk transfers to the country of origin by making use of official channels, either by depositing the funds on his/her own bank account and making a wire transfer to his/her correspondent in the beneficiary country or by placing an order at a licensed money remittance transmitter. The use of prepaid cards in the remittance collection phase is also being observed.

Germany: Illegal HOSSPs often use relatives in foreign countries for the pay-out. Sometimes they travel to the foreign country themselves regularly to pay out the money. Another way is they use registered service providers, but act in their own name instead of the name of the customer. In some rare cases, authorized agents conduct money remittance business on their own behalf in an illegal way by using the software given by the principal remittance service provider.

Source: Country investigations, FATF project questionnaire.

1.9 TECHNOLOGIES AND COMMUNICATION TOOLS USED BY *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

The techniques and tools used by *hawaladars* and other similar service providers require effective communication mechanisms, as they cannot rely on the IT communication services of international funds transfers' providers.

Effective communication is also one key competitive advantage of these services providers, as clients value the immediate availability of funds. Telephone, fax and e-mails to communicate transmission messages to other services providers across the borders are therefore essential. Recently, authorities have been observing the use of advanced internet technologies by *hawala* and

other similar agents and suspect they are exclusively using protected online services to conduct their activities and maintain their accounts, leaving no manual accounts. Some of these authorities suspect that these services and websites are being hosted from servers located in Dubai[5]. The same authorities also consider that such agents also operate through banks located in Dubai for net settlement of their transactions, leaving no trail after being processed through these banks.[6]

1.10 SCALE OF UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

The scale of unregulated *hawalas* is unknown and is impossible to generalize. Most countries have difficulties reaching credible estimates of the size of unregulated *hawala* and other similar service providers. Variations are understood to be significant from one country to the other, as are the structure of the *hawala* and other similar services markets. In some countries, traditional *hawala* and other similar services providers are believed to be more prominent while in others, illegal/criminal operators reportedly represent the highest market share. The situation is further complicated as in many countries regulated money transfer agents are reportedly used to conduct illegal *hawala* and other similar services transactions separately and covertly in addition to their regulated activities. Such market structures make it even more difficult to estimate the amount of illegal HOSSPs in a country.

Out of the 21[7] countries that responded to the question on the size of illegal *hawala* and other similar service providers in their jurisdiction, only 8 countries attempted to provide some information on the scale of unregulated *hawala* and other similar services operations in their country. The remaining 13 countries acknowledged the existence of unregulated *hawala* and other similar service providers but could not provide any estimate. The estimated number of unregulated *hawala* and other similar services provided by countries ranged from 25 to several hundred. Countries pointed out that these estimates most likely underestimate the real number of unregulated operators. Some countries provided a rough estimate of the market share of unregulated *hawala* and other similar service providers in total remittance market, ranging from 10% to 50%. These estimates are largely based on investigations, are anecdotal, and may not be representative.

Against such difficulties to reach even reasonable estimates, regulating, supervising and monitoring unregulated *hawala* and other similar service providers proves very challenging.

Several reasons can be identified to explain the challenge in providing reasonable estimates, including: (1) Very small number of ML/TF investigations involving *hawala* and other similar service providers; (2) Very limited number of operations by public authorities to detect unregulated *hawala* and other similar service providers; (3) Strong variations and diversity in the structure of

5 Netherlands Authorities.

6 *Ibid.*

7 Only FATF member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, one country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

the *hawala* and other similar service providers markets; and (4) The absence in most countries of coordinated policy and operational coordination to identify unregulated *hawala* and other similar service providers.

1.11 LACK OF SUPERVISION EXACERBATES MONEY LAUNDERING AND TERRORIST FINANCING VULNERABILITY

One of the key findings of this survey is that how best to regulate and supervise *hawala* and other similar service providers remains one of the key challenges authorities face in many countries today and that a lack of supervisory resources for MVTS is a global problem. As with other sectors, the less regulated and supervised the *hawala* and other similar service providers market is, the greater the money laundering and terrorist financing vulnerability. Completely unregulated operators are particularly vulnerable to Money Laundering/Terrorist Financing risks because they permit funds to be sent with little or no CDD requirements, allowing a money launderer or terrorist financier to freely send funds with limited risk of being identified. The information collected from the questionnaire shows that with no requirement to comply with core AML/CFT obligations, most of the unregulated *hawala* and other similar service providers maintain records in a format that are not easily accessible to law enforcement authorities. Similarly, the findings highlight how limited supervisory capacity for the MVTS sector in most countries only exacerbates this problem. FATF could take these findings into account when it considers the policy implications of this report.

On the other hand, unregulated *hawala* and similar services provide legitimate and efficient remittance services to lower risk customers who pose lower ML/TF risk. Their services are particularly relevant where access to the regulated financial sector is difficult or prohibitively expensive.

The multi-dimensional nature of unregulated *hawala* and other similar service providers makes regulating the sector a complex issue, all the more so given the significant resources constraints facing supervisors of the MVTS sector. Understanding the dynamics of unregulated *hawala* and other similar service providers in the framework of broader financial system is important before designing a monitoring/regulatory/supervisory regime for the sector. One of the concerns expressed by the development community is whether over-regulating *hawala* and other similar service providers could result in such providers becoming completely underground and as a result, more vulnerable to ML/TF risks. Hard evidence, however, is difficult to come by to document this concern. As countries are imposing stricter AML obligations such as CDD in the regulated financial sector - including remittance and money transfer businesses, it is possible that unregulated sector might become more attractive for money laundering activities. Therefore it becomes of paramount importance for countries to balance these two facets of the sector in order to most effectively mitigate ML/TF risks.

While much attention has been paid to *hawala* and other similar service providers over the last ten years, the complexity, diversity, varying drivers and variety of the *hawala* and other similar service providers, particularly in countries where the regulated financial sector is far from having reached maturity, continues to make the set up and enforcement of effective regulatory and supervisory frameworks a challenge in many countries.

CHAPTER 2: MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH HAWALA AND OTHER SIMILAR SERVICE PROVIDERS

2.1 VULNERABILITY TO MONEY LAUNDERING AND TERRORIST FINANCING

As is always the case when criminals own or control financial intermediaries, criminal HOSSPs deserve particular attention. Although a limited number of case studies were provided to the project team, there are several reasons why HOSSPs continue to pose a money laundering and terrorist financing vulnerability. These include a lack of supervisory will or resources; settlement across multiple jurisdictions through value or cash outside of the banking system in some instances; the use of businesses whose primary focus may not be regulated as financial institutions; the use of net settlement or cover payments, not serial payments, to settle through the banking system that makes it difficult to track individual transfers; the commingling of criminal and illicit proceeds; and the masking of illicit proceed transfer that appears to be trade. None of these factors are unique to HOSSPs. The most significant reasons for concern are two-fold and jurisdiction-specific: lack of supervisory resources and settlement through value or cash that makes HOSSPs transactions particularly difficult for law enforcement to follow the money.

High threat HOSSPs networks often rely on the fact that the full size of the network is not visible in any individual country and that national registers of registered or licensed money transmitters are either not accessible or are difficult to find.

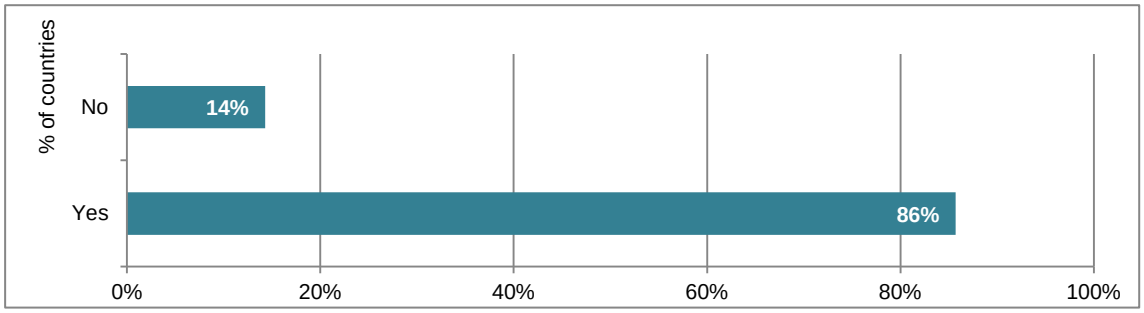
Most countries view HOSSPs as highly vulnerable to money laundering. Despite a limited number of cases provided to the project team, twenty eight[8] surveyed countries answered the question whether HOSSPs are regarded as high risk for criminal money laundering in their country. Of those, 86% of the surveyed countries stated that HOSSPs are vulnerable to ML risks as shown in Figure 2.1. All 4 countries that said no to the question clearly stated that HOSSPs are not commonly used in their countries because of the existence of highly efficient and convenient banking and remittance services.

Among the countries that answered positively to the question, very few responding countries clearly mentioned that there have been convictions of illegal HOSSPs for money laundering crimes. Some countries explicitly stated that they do not have the data to support the contention that HOSSPs are highly vulnerable, but base this conclusion on financial intelligence investigations/reports. A few countries raised concerns that increased customer due diligence and compliance processes in place at other types of financial institutions may make unregulated HOSSPs more attractive for money laundering. For these countries, HOSSPs are seen as vulnerable because they avoid attention from authorities including law enforcement authorities,

8 Both FATF and APG member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, 1 country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. Out of 8 APG member countries that responded 7 countries provided an answer to this question and 1 country could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country.

evade restrictions on foreign exchange controls and leave a minimal paper trail for law enforcement agencies to follow in comparison to banks or other money transmitters.

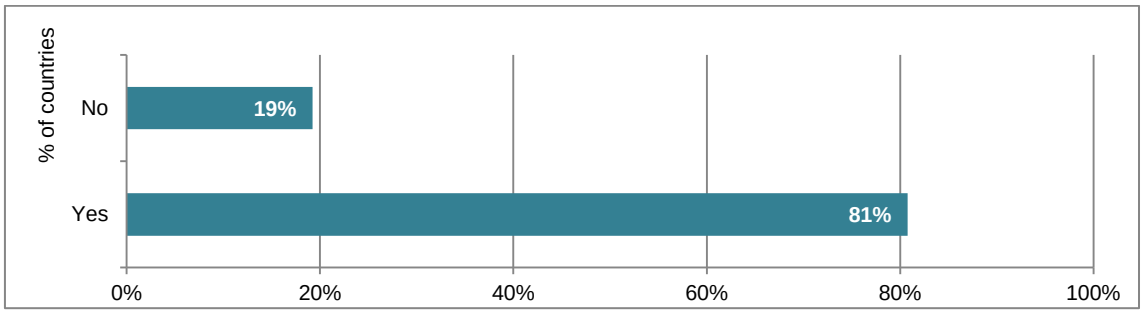
Figure 2.1 **Are HOSSPs vulnerable to money laundering risk?**



Source: FATF project questionnaire.

Most countries also view HOSSPs as highly vulnerable to terrorist financing. Twenty six[9] surveyed countries answered the question whether HOSSPs are regarded as high risk for terrorist financing (TF) in their country. 81% of the surveyed countries agreed that HOSSPs are vulnerable to TF risks as shown in Figure 2.2. All 5 countries that said no to the question clearly stated that HOSSPs are not commonly used in their countries because of the existence of highly efficient and convenient banking and remittance services.

Figure 2.2 **Are HOSSPs vulnerable to terrorist financing risk?**



Source: FATF project questionnaire.

Among the countries that answered positively to the question, only a few countries like India mentioned that there have been quite a few cases where the funds from abroad by the terrorist organizations were received in the country through HOSSPs. Many countries consider HOSSPs as high vulnerability for TF but have very few domestic cases to support the statement.

9 Both FATF and APG member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, 1 country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. Out of 8 APG member countries that responded 5 countries provided an answer to this question, 2 countries did not respond to this question and 1 country could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country.

2.2 CRIMINAL HOSSPS

A distinct form of criminal remittance network has been reported as operating internationally and servicing the needs of criminal organizations. These criminal HOSSPs appear to exist predominately to serve the criminal needs. In Europe and Australia, they are focussed on the collection of cash and transfer of value across borders, whilst in India or Pakistan they may be focussed on capital flight, exchange control violations or tax fraud.

2.3 WHAT MAKES CRIMINAL HOSSPS DISTINCT

Criminal HOSSPs primarily exist to facilitate the movement and/or laundering of criminal proceeds generated by drug trafficking, smuggling and fraud. Their existence is primarily driven by the demand from criminal customers to dispose of cash on their behalf and pay the equivalent value to the criminal group on demand elsewhere in the world. To achieve this criminal HOSSP networks use cash pools and reciprocal settlements by servicing remittances for other HOSSP groups. Individual criminal HOSSPs groups co-operate to form unregulated networks with surplus cash or individual electronic remittances are shared to complete the remittances demanded by different markets.

2.4 CRIMINAL HOSSPS METHODOLOGY FOR CRIMINAL PROCEEDS TRANSFERS

Law enforcement case studies indicate that criminal HOSSPs generally involve at least four individuals for the placement stage of criminal proceeds. These are:

- **Controller or Money Broker** – a trusted individual normally who arranges for the collection of street money (e.g., drug proceeds) and arranges for the delivery of an equivalent value to its ultimate destination (e.g., to businesses controlled by a drug cartel).
- **Collector** – instructed by the Controller to collect money from criminals and dispose it upon the controller's instructions.
- **Co-ordinator** – an intermediary who manages parts of the money laundering process for one or more Controller.
- **Transmitter** – receives and dispatches the money to the control of the Controller.

Role of the Controller: The Controller (also called a money broker in some jurisdictions) is the key to success of the system. The criminal customer tells the controller who will hand over the money and where the value is to be paid. Acting as a third party money launderer, the Controller serves multiple criminal organizations in multiple countries. The Controllers back office needs to keep records of the money he collects, controls and disburses. The Controller will normally be responsible for the money from the time it is collected until the value is successfully delivered as instructed. He may bear the cost of funds that are lost or are not effectively transferred.

Role of the Collector: The Collector is the Controller's trusted representative operating on instructions sent to him by the Controller, or his back office, by text message, email, and

Blackberry messenger or by other means. He faces the highest risk of arrest, because he has to meet the criminals to collect the cash. The Collector contacts the criminals and arranges to collect the cash at a discrete place or in circumstances where such activity, even if overt, does not attract attention. Over time the criminal and Collector may contact each other directly to arrange the pick-ups, but the collector will be told how much money he is responsible for and will dispose it on the instructions of the controller. The Controller will receive instructions from the criminal group directly or by such means which ensures the information is accurately received and understood.

2.5. COMPLETING THE CRIMINAL PROCEEDS TRANSFERS

Once the cash is counted, and any shortages accounted for, the Controller completes the criminal transaction by arranging for the equivalent value to be made available to the criminal group in the chosen destination, either by an electronic payment from a business controlled by an associate or through another handover of cash. Where the transaction is completed with a cash handover, the Controller arranges for this to be done by a Collector working for him or through another controller who co-operates with him. A token may also be used for this handover from a Collector to a criminal customer, but the process will start with a Collector nominating a bank note to be used, and conclude with the bank note being passed to the Collector.

2.5.1 AUTHENTICATING THE HANDOVER – USE OF A TOKEN

A regular feature of criminal cash handovers is the use of the unique serial number on a banknote to act as a means of identification and a rudimentary receipt for the handover. A Collector starts the process by identifying banknotes in his possession to be used as "tokens" in future transactions. He gives his Controller the serial number, and the controller then passes this on to the criminal customers holding the cash to be laundered. The criminal group ensures that the courier delivering the cash to the meeting knows what banknote will be presented to him. The collector shows the banknote and usually passes it over when he has received the cash. The criminal cash courier then takes the token away with him to show his bosses he has passed the money to the right person.

Box 2.1 **Use of Tokens in UK**

Communication between Controller & Collector to arrange Token number

		Send me any token no ugnt	06/01/2012 12:16:01 UTC (Device)	06/01/2012 12:15:57 (Network)	06/01/2012 12:15:57 (Network) 06/01/2012 12:16:01 UTC (Device)	Read	Inbox	
		LC26126666	06/01/2012 12:17:11 UTC (Device)		06/01/2012 12:17:11 UTC (Device)	Sent	Sentbox	

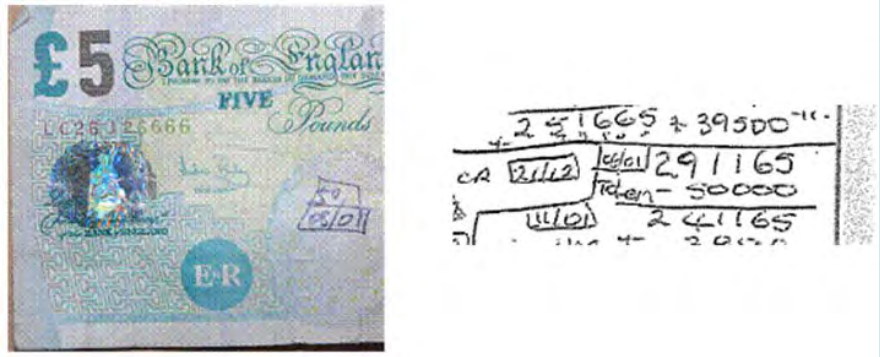
continued on following page

continued from previous page

Collector arranging handover with criminal customer and reporting to Controller

Simone west hounslow		Tw5 0Lf new HESTON road 122	08/01/2012 14:56:36 UTC (Device)	08/01/2012 14:56:34 (Network)	08/01/2012 14:56:34 (Network) 08/01/2012 14:56:36 UTC (Device)	Read	Inbox
		Have u recieved 50pin	08/01/2012 15:14:28 UTC (Device)	08/01/2012 15:14:26 (Network)	08/01/2012 15:14:26 (Network) 08/01/2012 15:14:28 UTC (Device)	Read	Inbox
		Nope gonna go pick up dis evening from same person in west london like last time	08/01/2012 15:17:11 UTC (Device)		08/01/2012 15:17:11 UTC (Device)	Sent	Sentbox
		Ok once u get plz let me know guys waiting for ks this side	08/01/2012 15:18:58 UTC (Device)	08/01/2012 15:18:53 (Network)	08/01/2012 15:18:53 (Network) 08/01/2012 15:18:58 UTC (Device)	Read	Inbox

Token seized from criminal courier marked with the amount collected and recorded in her drugs ledger



Step by step explanation – Use of tokens by criminal HOSSPs in UK

1. The first text message above is from a Controller to a Collector requesting the Collector sends a token number for use in a handover of criminal cash.
2. In the second text, the Collector sends the serial number of a Bank of England GBP 5 note to the Controller for use as a token; the Controller would then forward this token number, with the Collector's mobile telephone number, to the criminal customer.
3. In the third text, the Collector sends the criminal customer's courier the details of where to meet to conduct the handover – a UK postcode and address (probably for entering into a satellite navigation device).
4. In the fourth text, the Controller asks the Collector if the handover has taken place – the words '50pin' refer to the collection of GBP 50 000.
5. In the fifth text, the Collector confirms that the handover will take place later that evening from a criminal courier she has met before.
6. In the sixth text, the Controller asks for confirmation when the handover has taken place as his customers need the money elsewhere and he needs to make the equivalent value available to them as soon as possible.
7. The banknote shown has the same serial number as the token number in the second text and is annotated with the amount collected and the date (50 08/01 – note dates on text messages). In this case the Collector has retained the token, possibly because the criminal courier and collector already knew each other (see above).The extract from the ledger (completed by the collector) shows the Collector's record of the transaction.

Source: United Kingdom.

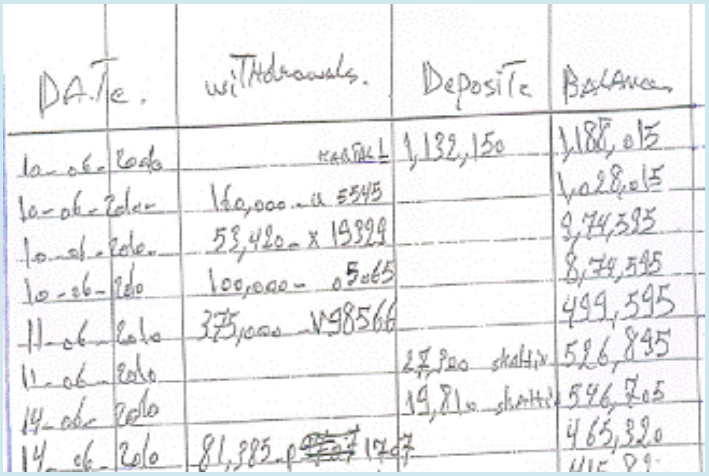
Box 2.2 **Use of Tokens in the Netherlands**

Another example of use of tokens can be seen in the following extract from a Dutch investigation. While the case example below is a real one, note the mobile phone numbers are fictitious. The real numbers have been replaced with randomly generated phone numbers.

Information that is sent through payment chain for conducting illegal transfer

- HOSSPs broker sends a SMS-message:
- 236430126 (mobile phone number)
- 163665 (amount to be transferred USD 163 665)
- X4569 (Token, identification number)
- The HOSSPs broker calls the mobile phone and delivers the money.

Example of a token. Part of a banknote is used as identification for a transfer.



DATE.	WITHDRAWALS.	DEPOSITE	BALANCE
10-06-2010		1,132,150	1,188,015
10-06-2010	160,000.- a 5545		1,028,015
10-06-2010	53,420.- x 19999		974,595
10-06-2010	100,000.- 05665		874,595
11-06-2010	375,000.- V98566		499,595
11-06-2010		27,300 shuttle	526,895
14-06-2010		19,810 shuttle	546,705
14-06-2010	81,385.-		465,320

Record from a Dutch Collector showing a Token number (*e.g.,* V98566) being used for each "withdrawal" or handover.

Source: Netherlands.

2.5.2 CRIMINAL HOSSPS CONTROLLER TRANSFER METHODS

The Controller takes responsibility for the cash once the Collector has made the handover. The Controller may charge a fee based on the percentage of the money and/or manipulate the exchange rate used to make a profit. The cash value becomes his as he uses value held in separate cash pools to complete the criminal transaction. Controllers have used the following identified methods to dispose of the cash:

a. Using local complicit money service businesses to bank and transmit the money to third parties or into accounts run by the Controller;

b. Passing the cash to other "customers" of the Controller to complete separate inward remittances which can be legitimate but are most profitable when they complete a different criminal transfer;

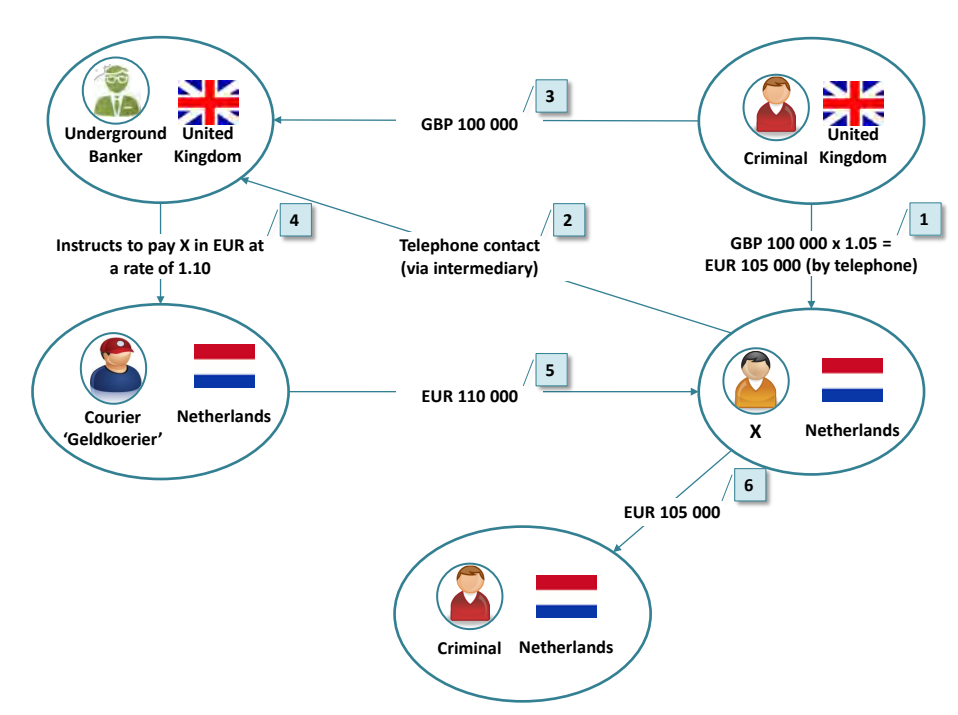
c. Paying the cash into bank accounts on behalf of the Controller to complete separate inward remittances (cuckoo smurfing); and

d. The physical movement of the cash (cash smuggling) by courier or in freight for sale or disposal at a safer location.

None of these techniques are necessarily unique to Criminal HOSSPs.

Box 2.3 **Illegal Currency Trade**

The following example from the Netherlands shows how the Criminal HOSSPs network profit from criminal proceeds transfer.



The picture above shows the working of the underground banking currency traders. The procedure of illegal currency trade is as follows (boxed numbers in above figure correspond to

transaction).

1. Underground broker/criminal HOSSPs broker X resides in the Netherlands and makes a phone call to a criminal or an intermediary in UK who has GBP 100 000 and wants to pay Euros to a criminal contact in the Netherlands. X buys the GBP 100 000 and offers an exchange rate of 1.05. This rate is lower than the official exchange rate. Either the criminal accepts or negotiates the rate with the underground broker.
2. X makes a phone call to a criminal HOSSPs broker in UK. In this phone call X offers GBP 100 000 at an exchange rate of 1.1 to EUR. This rate is higher than the official exchange rate. The broker in UK agrees to pay higher exchange rate probably because he can probably sell pounds later for better exchange rate.
3. The GBP 100 000 is physically transferred in UK from the criminal in UK to the underground broker in UK.
4. The underground broker in UK calls a contact in Netherlands (in picture 'Geldkoerier Nederland') and directs him to pay EUR 110 000 (GBP 100 000 x 1.1) to X.
5. The contact *Geldkoerier Nederland* in Netherlands brings EUR 110 000 physically to X.
6. X pays EUR 105 000 to a criminal in Netherlands. X makes a profit of EUR 5 000 on this specific criminal currency trade and there is no physical money transfer across the border. Such transactions can be easily undertaken without paper trail.

Source: Netherlands.

2.6 MONEY LAUNDERING VULNERABILITY OF HOSSPS

2.6.1 USE OF THIRD PARTY PAYMENTS TO TRANSFER CRIMINAL PROCEEDS

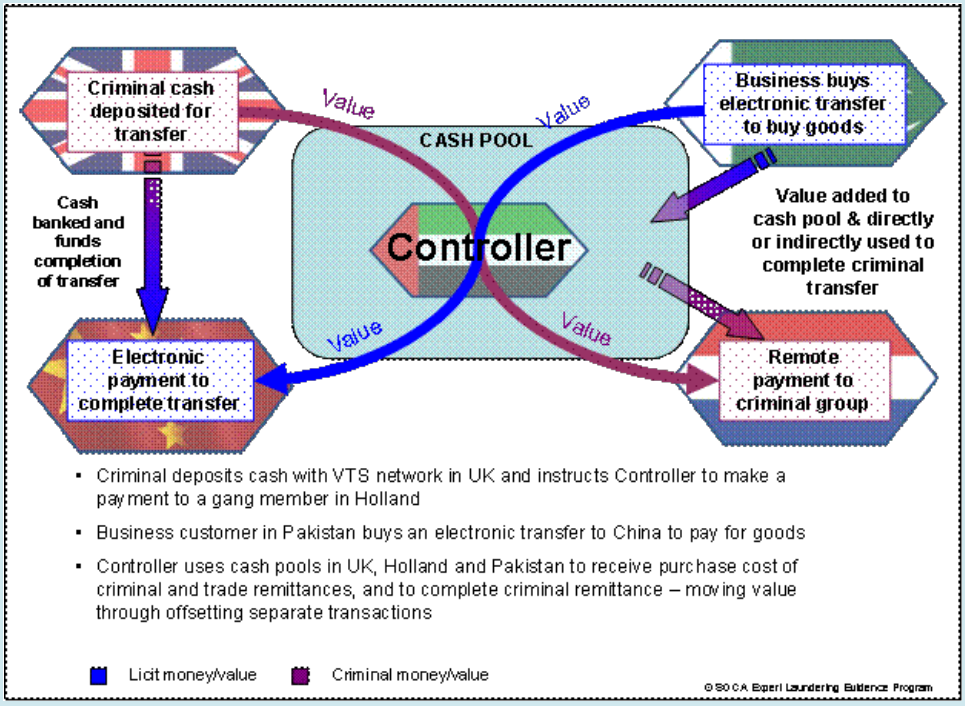
A common technique used by criminal HOSSPs is to use third party payments to transmit funds as well as to commit export and import fraud. Controllers build up large cash pools in countries where they service drug traffickers and other cash based criminals. To move the value of this cash, they directly or indirectly offer remittance services to other markets which have a demand for electronic remittances. They can do this by undercutting bank costs and exchange rates and use their cash pool to complete licit remittances, but they are also uniquely placed to service other criminal remittance corridors serving customers undertaking tax fraud, import fraud, export fraud or breaching exchange controls.

The Controller sends limited information to their transmitter, just enough information to complete a bank electronic transfer request. This will typically comprises of the beneficiary account Name, account number, SWIFT code and amount. In a country where the banks or regulators are vigilant the transmitter has often been observed creating false invoices to provide a false provenance for the transfer made.

This process is known as third party payment or invoice settlement, and has commonly been used by criminal HOSSPs, because it is an efficient way of moving excess values from a cash pool and HOSSPs get paid to do so.

Box 2.4 **The Use of Trade to Transfer Criminal Proceeds**

The example below is a typical third party payment settlement.



Controllers have a lucrative second market in servicing businesses and individuals who want to move value to breach local rules or to facilitate fraud. This may occur in countries where the amount of outward remittances in foreign currency is restricted or where exchange control or restricted access to foreign currency creates delay or high exchange costs. However access to a Controllers cash pools can also facilitate fraud.

Source: United Kingdom.

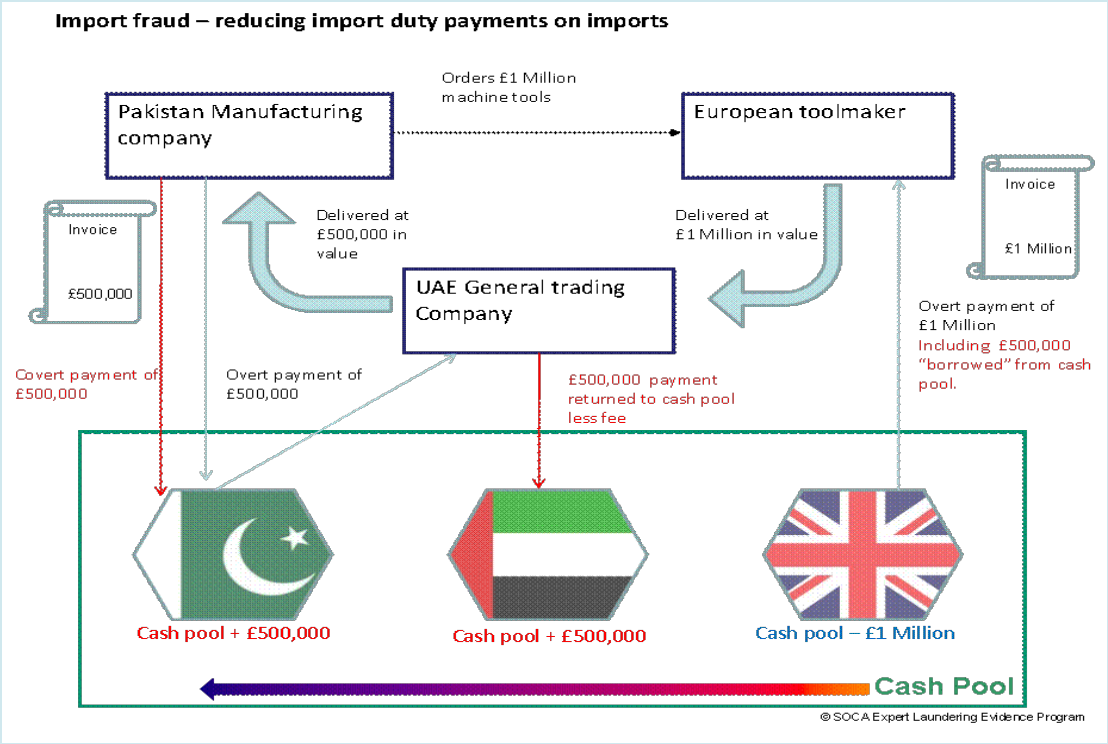
Box 2.5 **Import Fraud through third party payment**

In this example a Controller makes a third party payment to facilitate an import fraud. The example provided involves the United Arab Emirates and Pakistan:

- A Pakistan manufacturing company seeks to buy a new machine costing GBP 1 000 000.
- It identifies a European supplier and places a provisional order.
- To avoid import tax it uses a UAE general trading company as an intermediary. The UAE Company invoices them for the same equipment at GBP 500 000 in value, and an overt payment is made through an MSB associated to the cash pool. This provides all the documents required to validate the import of the machinery at a reduced value.
- At the same time the Pakistani manufacturer arranges for the full GBP 1 000 000 payment to be made through the cash pool in the UK. The goods are delivered to the UAE intermediary for onwards shipment to China.
- The UAE Company has a surplus of GBP 500 000 which it returns to or leaves in the cash pool

in UAE. The Pakistani manufacturing company also has a debt to the cash pool of GBP 500 000 (the balance of the true value of the imported goods) which it settles with a covert payment to the cash pool.

- The net result is that the UK cash pool is reduced by GBP 1 000 000 whilst the Pakistan & UAE cash pool increase by GBP 500 000 each.



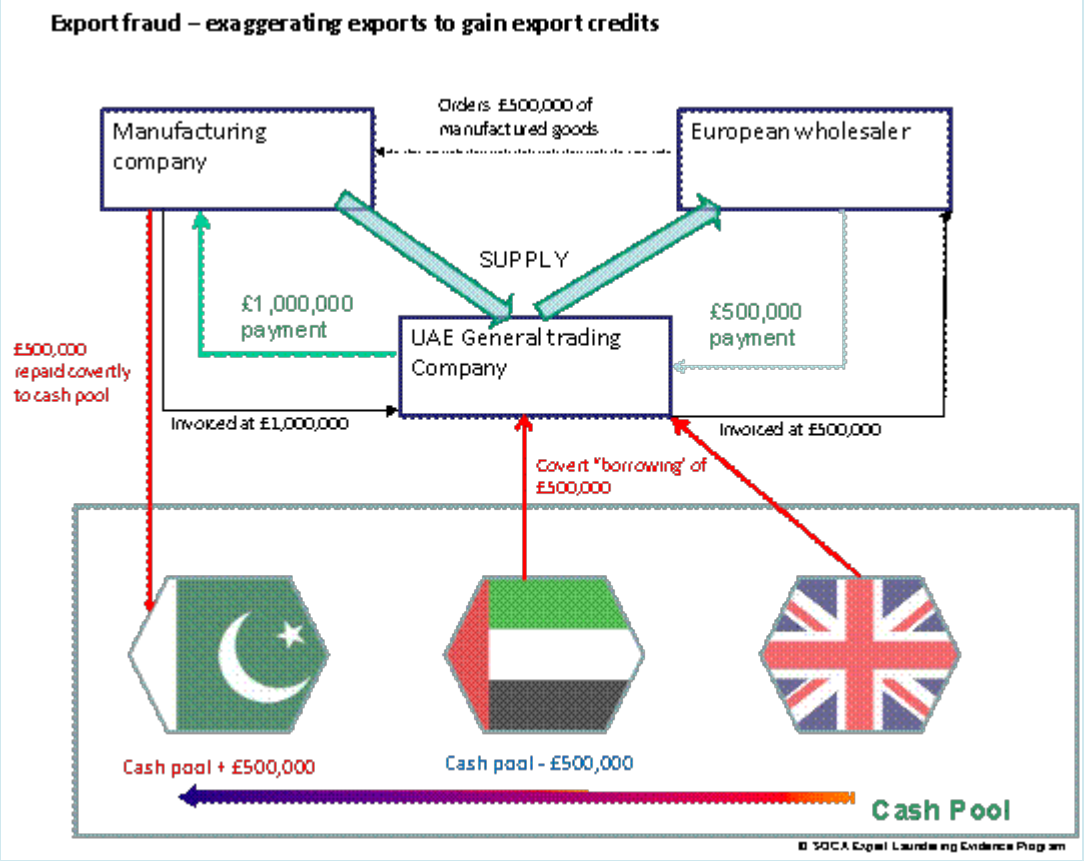
Source: United Kingdom.

Box 2.6 **Export fraud through third party payment**

- Case studies indicate that HOSSPs are used to facilitate export fraud. Export fraud can work in many ways, but the principal is the same – to overvalue export goods to benefit from export credits or tax rebates. This example uses Pakistan, where exporters can benefit from export rebates, GST rebates (equivalent of UK VAT), as well as beneficial access to credit.
- A European wholesaler orders GBP 500 000 of manufactured goods from a Pakistani manufacturing company.
- The Pakistani company arranges to supply the goods through a UAE company. This company invoices the buyer at a true value of GBP 500 000, receives payment and supplies the goods.
- At the same the Pakistani manufacturer raises an invoice for the same goods to the UAE Company but for a false value of GBP 1 000 000. The UAE Company "borrows" GBP 500 000 from the cash pool, combines this with the licit payment from the buyer and pays the full value of the false GBP 1 000 000 invoice.
- The Pakistani company returns GBP 500 000 to the cash pool in Pakistan to settle the amount borrowed in UAE plus any fees. The Pakistani company benefits from increased tax

rebates and access to credit.

- The net effect of the fraud is to move GBP 500 000 in value from the UAE to Pakistani cash pool.



Source: United Kingdom.

2.6.2 USE OF TRADE BY CRIMINAL HOSSPS TO LAUNDER DRUG PROCEEDS

Ample evidence underscores the use of criminal HOSSPs to launder drug proceeds. The use of trade by criminal money brokers has been identified by law enforcement as a common technique to facilitate the movement of drug proceeds generated in one jurisdiction to drug cartels outside of the jurisdiction. The net settlement technique called the "black market peso exchange" system is a common criminal HOSSPs method used in the United States and elsewhere by drug cartels.

Developed in the 1990s, Colombian and Mexican drug cartels export drugs to the United States, where they are sold for US dollars. The drug cartel enters into a contract with a peso broker (the controller), who uses a US-based agent to buy the US dollars from the drug sales. Once the US dollars are received, the peso broker deposits the equivalent in pesos into the drug cartels' account in Colombia or Mexico. To obtain the pesos, the peso broker buys the pesos from Colombian or Mexican-based exporters, who need to purchase goods in dollars in the United States or abroad. The broker then arranges for the importers to obtain the dollars in the United States to purchase goods for export to the importers' home country.

Box 2.7 **Criminal HOSSPs Use of Trade to Launder Drug Proceeds**

Case 1: Toy Company Used to Launder Proceeds

A Los Angeles-based toy company named Angel Toy Company manufactured plush toys like teddy bears. In March 2011, all three defendants pleaded guilty to conspiracy to structure currency transactions. In court documents, all three defendants admitted that, from 2000 through July 2010, there was an agreement that cash deposits into ATC's bank accounts had to be under USD 10 000 in order to avoid financial reporting requirements, specifically the filing of a Currency Transaction Report. The owners of Angel Toys received cash deposits, which were drug proceeds, into their banks accounts. The money was returned to drug traffickers when actual goods – in the case of the company, stuffed animals such as Teddy bears – are exported to the foreign countries and sold to generate local "clean" money.

The investigation revealed two primary ways in which ATC received and structured cash: in some cases, people affiliated with drug traffickers simply dropped cash at ATC's offices in downtown Los Angeles; the second method involved cash deposits made directly into an ATC bank account, sometimes by individuals located as far away as New York. During one four-year period, the investigation tracked more than USD 8 million in cash deposit into ATC accounts, and not a single transaction was for more than USD 10 000, according to court documents. The owners of Angel Toys were sentenced to more than three years in prison.

Source: United States.

Case 2: Use of Underground Money Shops and Local Banks to Launder Drug Proceeds

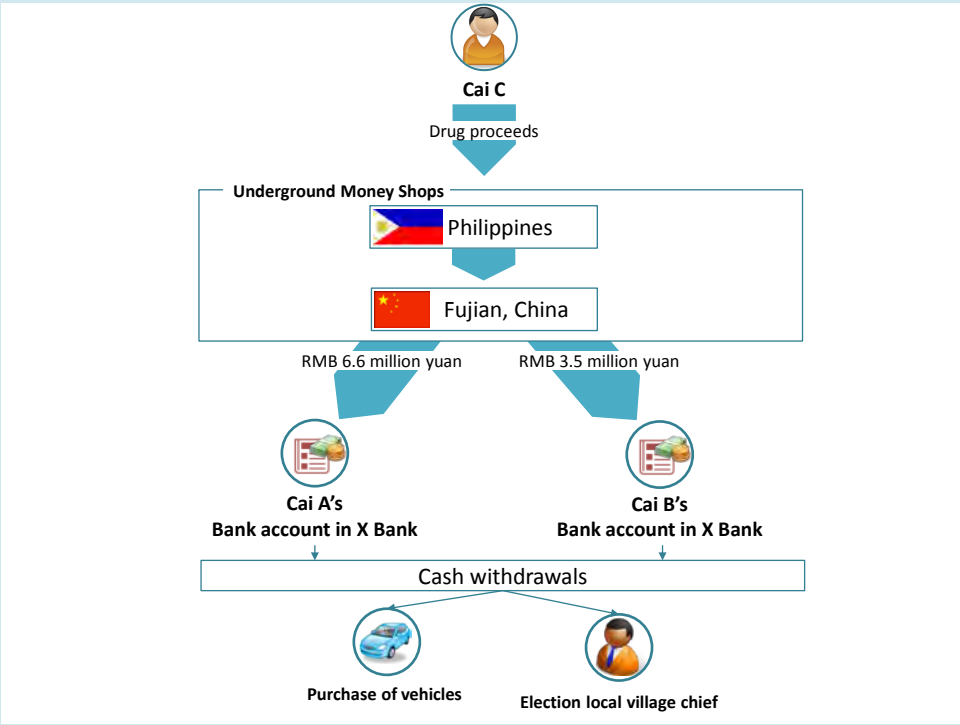
On May 9, 2005, fifteen defendants involved in '5.12' transnational drug trafficking case, which was jointly investigated by the Chinese and Malaysian police, were convicted of drug manufacturing and trafficking and money laundering by the Intermediate People's Court of Quanzhou, Fujian. Found guilty of money laundering, Cai A was sentenced to three years' imprisonment and a fine of RMB 330 000 yuan, and Cai B was sentenced to two and a half years' imprisonment and a fine of RMB 175 000 yuan.

From August 2002 to April 2004, the drug dealer Cai C had transferred the drug proceeds from underground money shops in Philippines to their counterparts in China. Abetted by Cai C, his relatives Cai A and Cai B respectively opened accounts with their own names in the local banks and deposited the illicit money in these accounts. The total amount of illicit money deposited in Cai B's accounts was about RMB 3.5 million yuan while that deposited in Cai A's account was about RMB 6.6 million yuan. Afterwards, most of the illicit money had been used for the purchase of vehicles and the election of local village chief.

The main process of money laundering activities in this case can be divided into the following steps:

1. Cai Ci transferred drug proceeds from underground money shops in Philippines to their counterparts in Quanzhou, Jinjiang and Shishi in China;
2. Underground money shops in Quanzhou, Jinjiang and Shishi deposited these funds in Cai A and Cai B's bank accounts;
3. Cai A and Cai B withdrew cash to purchase vehicles and so forth ordered by Cai Ci.

The flow of funds is depicted as follows:



Source: China.

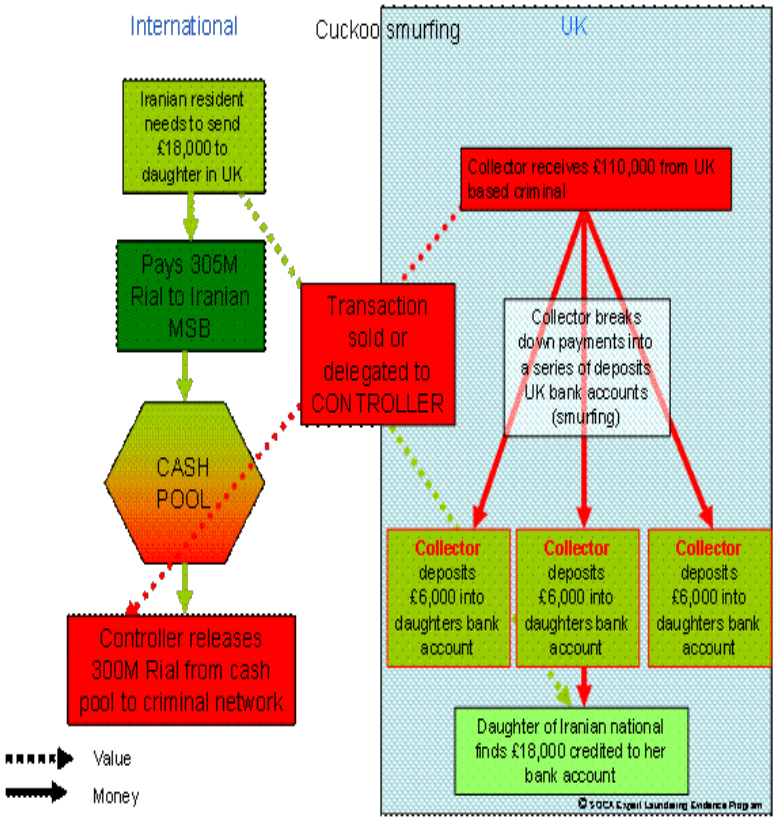
2.6.3 USE OF CRIMINAL HOSSPS TO EVADE SANCTIONS

Criminal HOSSPs are used to evade sanctions and to allow the transfer of funds into and out of sanctioned jurisdictions because these entities offer an alternative to banks and other regulated financial institutions that will no longer process transactions on behalf of sanctioned entities. Criminal HOSSPs are used instead because they can mask the identity of the ultimate originator from the banks or money transmitters that wire the funds on behalf of the HOSSPs. As illustrated below, one common technique is cuckoo smurfing. It occurs where the destination account is in the same country as surplus of criminal cash.

In the example in Figure 2.3, the Controller has a relationship with a *saraf* or money exchanger in Iran. A customer approaches the *saraf* to make a transfer of GBP 18 000 to the bank account of their daughter in UK. The Controller has a surplus of cash from a collection made from a Criminal group in UK and instructs their Collector to use part of this cash to make a series of small deposits into account number given by the family in Iran. The Iranian sender and recipient have no control over how the remittance is completed. The Collector chooses to "smurf" or structure the deposits to limit the likelihood of his role be identified by the receiving bank.

For the Controller this technique has the advantage of avoiding the costs and risk of running any overt business and also the bank charges are met by the person receiving the inward remittances. This technique has been the subject of large scale prosecutions in UK and Australia, with individual groups of Collectors responsible for cuckoo smurfing deposits into business and personal bank accounts in excess of GBP 100 million.

Figure 2.3 **Cuckoo Smurfing by Criminal HOSSPs**



Source: United Kingdom.

Box 2.8 **Sanctions Evasion by Criminal HOSSPs**

Iran Sanctions Evasion by Criminal HOSSPs: Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) agents arrest Manhattan management consultant on charges of criminally violating the Iran Trade Embargo. ICE agents, acting as part of a New York-based Task Force, arrested Mahmoud Reza Banki on January 7, 2009. The investigation was conducted jointly by ICE and the U.S. Treasury's Office of Foreign Assets Control. According to the indictment, BANKI provided money transmitting services to residents of Iran by operating a *hawala* in which BANKI received wire transfers in a personal bank account he maintained at Bank of America in Manhattan totalling about USD 4.7 million from companies and individuals located in the following countries: Saudi Arabia, Kuwait, Latvia, Slovenia, Russia, Sweden, the Philippines, the United States, and other countries.

Generally, BANKI did not know the wire originators personally. He received the funds with the understanding that an equivalent amount of Iranian currency would, in turn, be disbursed to intended recipients residing in Iran. Banki informed an Iran-based co-conspirator, when funds had been received and the co-conspirator then disbursed the funds in Iran, less any fees. Banki, according to the indictment, used specific funds transferred into his Bank of America account to make joint investments in the United States with the Iran-based co-conspirator. Among other things, Banki used the funds to purchase a USD 2.4 million Manhattan condominium; to invest in securities for his own benefit and that of the co-conspirator; and to make payments on his credit card accounts, including about USD 55 000 in one month alone in the summer of 2007.

Banki was charged with violating the International Emergency Economic Powers Act (IEEPA), together with Executive Orders and U.S. Department of Treasury regulations; conducting an unlicensed money transmitting business; and conspiracy to commit those crimes. Banki was found guilty on June 4, 2010, of one count of conspiracy to violate IEEPA and to operate unlicensed money transmitting business; one substantive count of violating IEEPA; one substantive count of operating an unlicensed money transmitting business; and two counts of making false statements to a Federal agency. In response to a special verdict form, the jury found that BANKI was an aider and abettor with respect to the substantive IEEPA and unlicensed money transmitting counts. BANKI was also ordered to forfeit USD 3 314 047, which represents the sum of money involved in the offenses and the proceeds derived there from. In October 2011, the United States Court of Appeals reversed the lower court's decision that al-Banki had acted as unregistered money transmitter on technical grounds, but did not challenge the facts of the case.

Source: United States.

2.7 TERRORIST FINANCING AND HOSSPS

More than a decade after the promulgation of Special Recommendation VI, terrorists continue to use HOSSPs to transmit funds. Terrorist exploitation of money transmitters is a function of geography, culture and financial access. In many countries of greatest concern, HOSSPs traditionally were a legitimate and accepted type of remitters and the primary vehicle for fund transfers, both legitimate and illicit. Limited banking access and high degrees of corruption and tax evasion in some of these jurisdictions continues to lead legitimate customers and criminals alike to use networks of unregistered HOSSPs.

There are several reasons why HOSSPs continue to pose a terrorist financing vulnerability, including: a lack of supervisory will or resources; settlement across multiple jurisdictions through value or cash outside of the banking system in some cases; the use of businesses that are not regulated financial institutions; the use of net settlement and the commingling of licit and illicit proceeds. While the settlement through value or trade that masks the individual fund transfers is a source of vulnerability, the most significant reason for concern is lack of supervisory resources and commitment to effective regulation. Inadequate efforts of outreach to the unregulated sector to pull them into the regulated sphere in some countries plus limited or no enforcement actions against unregistered entities also minimizes the incentives for unregulated entities to subject themselves to regulation and supervision, making them more vulnerable to terrorist abuse.

Box 2.9 **Terrorist Abuse of HOSSPs – United States Cases**

Case Example 1: Terrorist Abuse of HOSSPs - Hamza Case

In April 2008, Money remitter sentenced to over 9 years for money laundering conspiracy and concealing terrorist financing Saifullah Anjum Ranjha, a Pakistani national residing in Washington, D.C. and Maryland, was sentenced to 110 months in prison for conspiring to launder money and for concealing terrorist financing in addition to being ordered to forfeit USD 2 208 000 worth of assets. This was an Immigration and Customs Enforcement (ICE)-led

investigation. According to his guilty plea, Ranjha operated a money remitter business in the District of Columbia known as Hamza, Inc. A cooperating witness, acting at the direction of law enforcement, held himself out to Ranjha and his associates to be involved in large scale international drug trafficking, international smuggling of counterfeit cigarettes and weapons. He also represented that he was providing assistance and financing to members of al Qaeda and its affiliated organizations and their operatives. From October 2003 to September 19, 2007, the cooperating witness gave Ranjha and his associates a total of USD 2 208 000 in government funds in order to transfer the monies abroad through a hawala. The cooperating witness represented that the monies were the proceeds of, and related to, his purported illegal activities and Ranjha laundered these funds believing they were to be used to support those activities. Ranjha was the primary point of contact for the cooperating witness and received the bulk of the monies from the cooperating witness, for a total of 21 hawala transactions in amounts ranging from USD 13 000 to USD 300 000. Most of the monies were turned over to Ranjha in locations in Maryland. On a few occasions the cooperating witness met Ranjha and other co-conspirators at Hamza, Inc. to provide monies for a particular hawala transfers. Ranjha arranged with his associates for the equivalent amount of monies, minus commissions, to be delivered to the cooperating witness, his third party designee, or a designated bank account in Canada, England, Spain, Pakistan, Japan and Australia. Ranjha kept a commission of approximately five per cent of the amount of currency sought to be transferred on each occasion. Other conspirators involved in a particular transaction retained an additional commission of between three to five per cent of the transaction amount. All the funds transferred abroad were picked up by cooperating individuals and returned to the Government.

Case Example 2: Terrorist Abuse of HOSSPs - Times Square Bomber case

On August 18, 2011, Mohammad Younis pled guilty in Manhattan federal court to operating an unlicensed money transfer business between the United States and Pakistan. One of the money transfers was used to fund the May 1, 2010, attempted car bombing in New York City's Times Square by Faisal Shahzad who is serving a life sentence in federal prison.

From January to May 2010, Younis provided money transmitting services to individuals in the New York City area by assisting in the operation of a hawala. On April 10, 2010, Younis engaged in two separate hawala transactions with customers who travelled from Connecticut and New Jersey to meet with him in Long Island. In each of the transactions, Younis provided thousands of dollars in cash to the individuals at the direction of a co-conspirator in Pakistan, but without knowledge of how the customers were planning to use the funds. At no time did Younis have the license to operate a money transmitting business from either state or federal authorities.

One of the individuals to whom Younis provided money was Shahzad, who, on June 21, 2010, pled guilty to a ten-count indictment charging him with crimes relating to his attempt to detonate a car bomb in Times Square on May 1, 2010. During the course of his plea allocution, Shahzad acknowledged receiving a cash payment in April 2010 in the United States to fund his preparations for the May 1, 2010, attempted bombing. According to Shahzad, the April cash payment was arranged in Pakistan by associates of the Tehrik-e-Taliban, the militant extremist group based in Pakistan that trained him to make and use explosive devices.

On September 15, 2010, Younis was arrested by the FBI and other agents of the New York Joint Terrorism Task Force.

Younis 45, of Long Island, New York, pled guilty to one count of conducting an unlicensed

money transmitting business.

Case Example 3: Terrorist Abuse of HOSSPs - Carnival Ice Cream Case

Abad and his nephew Aref Elfgeeh ran a money-transfer operation at Abad's Carnival French Ice Cream (or "Carnival") shop in Brooklyn, New York. Abad was arrested in January 2003; an arrest warrant was issued for Aref, who was arrested in December of that year. Carnival French Ice Cream maintained an account at J.P. Morgan Chase Bank ("Chase"), as well as account statements from 12 "feeder" accounts at Chase and other banks. Bank statements showed large totals of money deposited into the Carnival account in small amounts as transfers from 12 feeder accounts, and large sums of money wired out of the Carnival account to accounts in 25 other countries, including Yemen where one of the recipients was a known member of Al Qaeda that used the Abads business to transmit funds to him. In a one-month period during the fall of 2000, more than USD 245 000 was deposited into the Carnival account and more than USD 268 000 was wired out. Between 1996 and 2003, the total amount deposited into the Carnival account was USD 22 190 642.21, and the total amount withdrawn was USD 21 995 556.54. Abad was charged with operating an unlicensed money transmission business.

The money arrived in the feeder accounts by various means, including check deposits, cash deposits, and wire transfers. Then, money went from the feeder accounts to the Carnival account in generally one of two ways. Most often there were checks written from one of the 12 feeder accounts, payable to the order of Carnival French Ice Cream account and then it was deposited into the Carnival French Ice Cream account. On some occasions the feeder accounts would wire money over to the Carnival French Ice Cream account. There were hundreds of checks from the feeder accounts made out to the Carnival account. One of the feeder accounts was a Chase bank account opened in the name of Prospect Deli that was opened by Aref and listed the home address and telephone number of Abad. The Prospect Deli was a business a few blocks away from the Carnival French Ice Cream shop; the Prospect Deli was in operation only from 1996 to 1998, but activity in the Prospect Deli bank account continued until 2002. For example, bank records showed that in 2001 approximately $850,000 was deposited into the Prospect Deli account and about USD 823 000 was transferred out to the Carnival account. Aref was sentenced principally to 51 months' imprisonment, followed by a three-year term of supervised release, and was ordered to pay a USD 500 000 fine and to forfeit USD 22 435 467. Abad was sentence principally to 188 months' imprisonment to be followed by a three-year term of supervised release, and was ordered to pay a USD 1 250 000 fine and to forfeit USD 22 435 467.

Source: United States.

Box 2.10 **Terrorist Abuse of HOSSPs – Indian Cases**

Case Example 1: Terrorist Abuse of HOSSPs

In a case of hawala money transfer to terrorists of the proscribed terrorist organization "X" in India, two hawala operators along with two receivers of hawala money for the terrorists were apprehended in the year 2011 and an amount of approximately INR 2 000 000 (USD 32 000) was recovered from them. They revealed that the hawala money was provided by the organization leaders based in country "Y" and routed through another country "Z" where another over ground worker of the terrorist organization is based. The modus operandi is that the terrorist leader in country "Y" collects terror funds in that country and sends it to another terrorist agent in country "Z" who contacts hawala operators who operate freely in that country. Apparently hawala is not illegal in country "Z". The hawala operator in country "Z" then gives a number on a currency note to the agent along with the telephone number of the person who would deliver the money in India. The agent then informs the same to the terrorist leader at "Y". The terrorist leader at "Y" then contacts the over-ground worker of the proscribed terrorist organisation at Delhi and gives the telephone number of the hawala agent and the number of the currency note. This over-ground worker then contacts the hawala operator at the given number and then collects the money at the decided location after giving the number of the currency note. The over-ground worker does not get to know the identity of the hawala operator as he delivers the money wearing a scooter helmet.

Note: The terrorist agent does not have to pay any commission at the receiving end.

Case Example 2: Terrorist Abuse of HOSSPs

In another case of Terrorist financing, a sum of INR 10 000 000 (USD 160 000) was intercepted in a State A in India which was meant to be delivered to a terrorist gang X. Investigation revealed that a number of earlier consignments had earlier been delivered to the terrorist gang earlier. It was revealed that development funds of a particular area in that State was defalcated and then sent to location P in that State. From location P, it was sent to location Q in another State B with the help of hundi operators operating between State A and State B. The hundi operators are told that the money belongs to a very influential person at state A. The hundi operators do not object conducting the transaction hearing the name of this influential person and deliver the money at state B to the person authorized by the agent of the terrorist gang. The money is delivered after deducting a commission of 1 per cent from the total money which is transferred. At State B, the hawala money is then changed from INR to Dollars in an unregulated exchange market and then transferred to another country E where arms and ammunition are purchased by the terrorist gang leaders based there. These arms and ammunition are then transferred across the borders and then delivered to the terrorist gang operating in State A for carrying our terrorist activities. In this case a total of 15 accused were arrested and charge sheeted and the trial is being held. The arrested members include terrorists, contractors, agents and government servants.

Source: India.

CHAPTER 3: REGULATORY AND SUPERVISORY RESPONSES TO MITIGATE ML/TF RISKS

The findings highlighted in this chapter should also be useful to other streams of work at the FATF, within national governments and for other stakeholders, for example in relation to the implementation of the FATF Standards.

3.1 A REGULATORY/SUPERVISORY RESPONSE INFLUENCED BY THE LEGAL STATUS OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS (HOSSPS)

This section focuses on the legal status of HOSSPs in the surveyed countries. The findings of the survey confirm that countries have taken different approaches to the regulation of *hawala* and other similar service providers, with a slight majority of countries treating *hawalas* and other similar service providers as illegal.

Among the 33[10] surveyed countries, 18 countries treat *hawala* and other similar service providers as illegal while 15 countries consider them legal if registered or licensed. Interestingly, most developed countries allow licensing or registration of HOSSPs, while developing countries do not. Within the developed countries respondents, only six out of 17 countries define *hawala* and other similar service providers as "illegal" and the remaining eleven have legalised *hawala* and other similar activity if service providers are either registered or licensed. On the other hand, 12 out of 16 developing countries respondents define *hawala* and other similar activity as "illegal" and only 4 countries allow them to operate legally if licensed or registered (See Table 3.1.). One of the reasons put forward by developing countries to consider *hawala* and other similar service providers as "illegal" is their capacity constraints.

Table 3.1 **Legal Status of *Hawala* and Other Similar Service Providers**

	Status of *hawala* and other similar service providers		
	Illegal	**Legal**	**Total**
Number of Countries	**18**	**15**	**33**
of which Developed Country	6	11	17
of which Developing Country	12	4	16

Source: FATF project questionnaire.

At the same time, caution needs to be exercised when analysing the survey results. As explained in Chapter 1, countries have varying definitions of what *hawala* means. In the 18 countries where

10 25 FATF and eight APG member countries provided answer to the question on legal status of *hawala* and other similar service providers in their country. Please note that three FATF member countries responded to this question where *hawala* and other similar service providers do not exist as a money transmission channel but *hawala* and other similar service providers is either legal or illegal under an existing law.

hawala and other similar service providers are illegal, two rather different approaches can be identified:

- Countries that do not allow *hawala* or other similar service providers to operate because *hawala* in these countries is synonymous to "illegal" operations. However, providers of the same kind of services can legally operate if licensed or registered but under a different name such as money service providers, or payment institution, or money remitters and therefore not included in the definition used in this report
- Countries where only traditional financial institutions – such as banks -are allowed to provide money remittance services. In such countries, *hawala* and other similar service providers are simply supposed to be non-existent.

3.2 IMPACT OF THE LEGALISATION OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS ON THE FORMALISATION OF THE REMITTANCE MARKET?

To gauge the impact of the legalisation of *hawala* and other similar service providers, the surveyed countries were asked whether legalizing *hawala* and other similar service providers has helped in formalizing the remittance market successfully in their country. 80%[11] of the surveyed countries where *hawala* and other similar service providers are legal answered positively to this question, confirming that licensing or registration requirements have led to an expansion of the regulated remittance market (Figure 3.1). However, this seems contradicted by the numbers of registered/licensed *hawala* and other similar service providers provided in the questionnaire responses by the countries where *hawala* is legalised. The number of domestic principal licensed/registered *hawala* and other similar service providers in seven[12] countries reporting numbers ranged from four to 26. In one country, the number of businesses registering as unregulated value transfer services (informal value transfer services or IVTS), a broader category than HOSSPs, was over 1 000. This country uses the term IVTS to refer to any system, mechanism, or network of people that receives money for the purposes of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form.

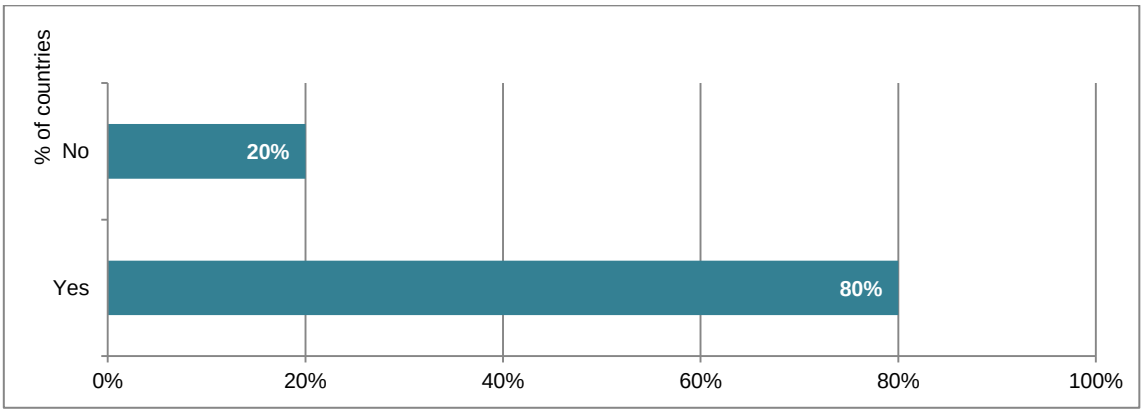
In general, the numbers of regulated HOSSPs are still very few—making it very likely that unregulated *hawala* and other similar service providers are in effect continuing their business in these countries. In most of the countries where *hawala* and other similar service providers have been legalised, they operate as licensed Money Service Operators (MSOs) and are required to

11 15 surveyed countries have legalised *hawala* and other similar service providers. Out of 15, 10 countries responded to the question. 4 countries where HOSSPs are legal did not respond to the question and one country could not respond because *hawala* does not exist as a money transmission channel in that country though *hawala* and other similar service providers is legal under an existing law.

12 Out of the 15 surveyed countries that legalised *hawala* and other similar service providers, eleven countries have provided information about licensed or registered domestic *hawala* and other similar service providers. But only seven countries could provide exact number of licensed/registered *hawala* and other similar service providers operating in their country.

conduct customer due diligence (CDD), keep records and implement other AML/CFT obligations set out in law - which contributes to mitigating ML/TF risks.

Figure 3.1 **Did Legalisation of Hawala and Other Similar Service Providers Help Formalise the Remittance Market?**



Source: FATF project questionnaire.

3.3 LESSONS LEARNED REGARDING THE LICENSING /REGISTRATION REQUIREMENTS FOR REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Building on the survey results, this section presents the licensing/registration requirements for regulated *hawala* and other similar service providers and their agents/branches.

3.3.1 SURVEY RESULTS: LICENSING/REGISTRATION REQUIREMENTS FOR REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Under a registration regime, the service provider has to identify its business to the authorities and provide certain information (as may be requested by the authorities). Authorities usually attach few or no conditions to the ability of the service provider to provide its services under the registration regime, making the market entry easier. Although there are varying practices of registration requirements, registration regime tend not to require AML/CFT compliance systems prior to registration unlike licensing system, and the initial application fee for registration is also lower than that for obtaining a license. A licensing regime provides more front-end screening by authorities and requirements to meet certain criteria. Regulatory authority grants the licensee the permission to engage in certain activities subject to specified terms and conditions. Such terms and conditions may define purpose, time-period, territory, compliance requirements, and operational instructions among others.

The survey results as shown in Table 3.2 illustrate that registration and licensing regimes are almost equally used in countries where *hawala* and other similar service providers have been legalised. The licensing approach is slightly more common with a total of seven countries adopting it compared to five countries which adopted a registration regime. Two countries— Republic of Guinea, and Sweden—have dual system depending on the size and type of service providers. For example in Sweden, a legal or natural person who is involved in commercial money remittance is

obliged to be either licensed (as a payment institution) or registered (as a registered payment service provider). The turnover of business is one among other factors that determines whether registration is sufficient or not. Similarly in the UK, a dual system is in place by which the service provider needs to obtain a license from the Financial Conduct Authority as an authorized payment institution or a payment service provider, but at the same time, also needs to register with the Customs and Tax authority for AML/CFT purpose.

Table 3.2 **Licensing/Registration Requirement for *Hawala* and Other Similar Service providers**

	Licensing	Registration	Dual
Developed Country	6	3	2
Developing Country	1	2	1
Total	7	5	3

Source: FATF project questionnaire.

3.3.2 SURVEY RESULTS: LICENSING/REGISTRATION REQUIREMENTS FOR AGENTS OR BRANCHES OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

In the majority of the countries where *hawala* and other similar service providers are legal, they usually can operate through branches or agents, which allow them to reach out to remote areas and expand their business. Survey results illustrate that in the case of agents, registration is by far the preferred approach, while in the case of branches, registration, licensing, as well as dual systems are used.

In the case of branches, one of the reasons why licensing or dual systems are used more often than in case of agents is that these are service providers which usually deliver only financial services (Table 3.3). By contrast, agents tend to provide remittance or other financial services as ancillary services to other businesses, such as operating supermarket, gas station, grocery stores, etc.

Table 2.3 **Licensing/Registration Requirements for Agents/Branches of Hawala and Other Similar Service Providers**

	Branches	Agents
Only Licensing	2	1
Only Registration	5	7
Dual System	1	0

Source: FATF project questionnaire.

3.3.3 REGULATING MARKET ENTRY FOR *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS: LICENSE OR REGISTRATION REQUIREMENT? [13]

Several factors determine the choice between a licensing regime and a registration regime—which in themselves have different impact on the ease/control of market access and the resources required for regulatory/supervisory oversight. This choice is also likely to have a bearing on the incentives for businesses between staying informal or entering the regulated economy.

Registration regimes require fewer conditions to be fulfilled at the time of entry thus making it easier to enter the market. Licensing regimes are most often more involved processes with more demanding conditions. They also usually require front-end screening of the applicants by the authorities. As a result, registration processes are expected to be faster and less resource consuming, while more supervisory capacities are expected to be necessary for licensing regimes. All things being equal, the less stringent up-stream conditions under registration regimes are expected to call for more on-going supervision and surveillance—particularly if the market is composed of a large number of smaller players.

Another important factor is how the registration/licensing regimes comparatively affect the incentives for expanding remittances through regulated channels. Survey results do not point to any clear cut benefit from one system compared to the other. It is however expected that the lower the barriers at entry and application fees, the easier it would be for market participants (notably the smaller ones) to enter the regulated market.

Both registration and licensing regimes create a framework for supervisors to exercise control over who can act as a principal service provider or an agent and to ensure compliance with AML/CFT obligations. Licensing requirements are expected to be more comprehensive and rigorous; they are also more expensive, which increases compliance costs for both the authorities and the service providers – irrespective of ML/TF risks.

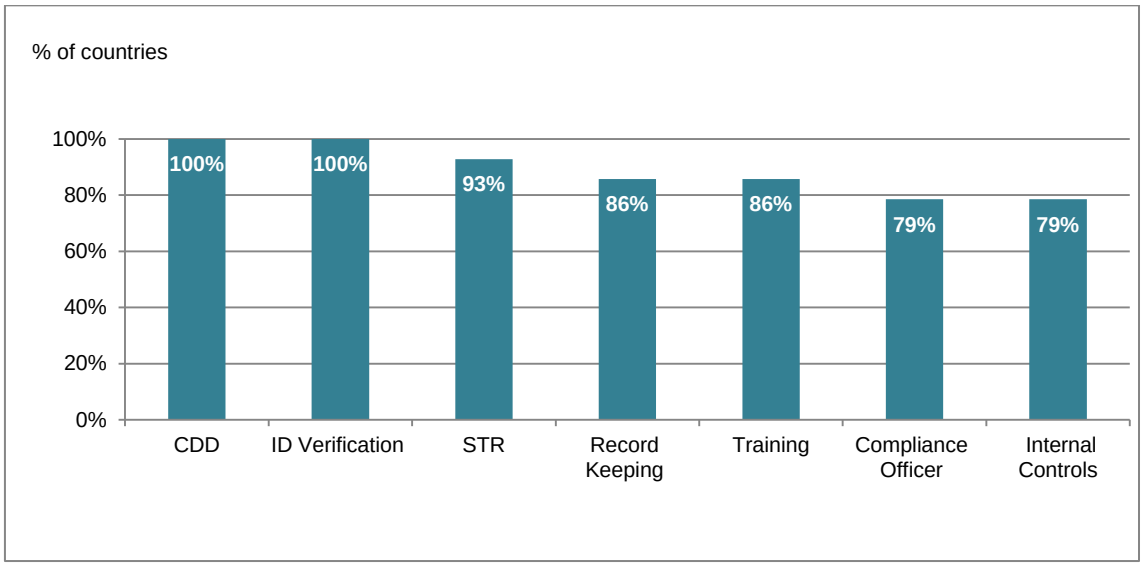
3.4 AML/CFT OBLIGATIONS OF REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Where legal, money service businesses and *hawala* and other similar service providers are usually treated the same way and subject to the same regulations as far as AML/CFT obligations are concerned. Out of 15 countries where *hawala* and other similar service providers are legal, 14 countries provided data on AML/CFT obligations of regulated *hawala* and other similar service providers in their countries. Survey results as shown in Figure 3.2 indicates that 75-100% of these countries impose Customer Due Diligence (CDD), Identify (ID) verification, Suspicious Transaction Reporting (STR), Recordkeeping, Training, Compliance Officers, and Internal Controls Requirements. In particular, all these countries require compliance with CDD requirements. All except one country require STR reporting. All except two countries require training of staff on AML/CFT regulations and record keeping for a minimum of five years. Only three of these countries

[13] Discussion in this sub-section relies on information provided in the World Bank report "Making Remittances Work: Balancing Financial Integrity and Inclusion" (soon to be published). Authors: E. Todoroki, W.Noor, K.Celik and A. Kulathunga.

do not require the appointment of a compliance officer and development and implementation of an internal control program.

Figure 3.2 **AML/CFT Obligations of *Hawala* and Other Similar Service Providers (percentage of countries)**



Source: FATF project questionnaire.

3.5 SUPERVISION AND ENFORCEMENT RELATED TO *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Effective supervision of HOSSPs is one of the primary challenges facing regulators. This section discusses the survey results on the supervision of *hawala* and other similar service providers, sanctions applicable to regulated *hawala* and other similar service providers for failure to implement AML/CFT obligations and requirement on foreign counterparties with respect to money transfers.

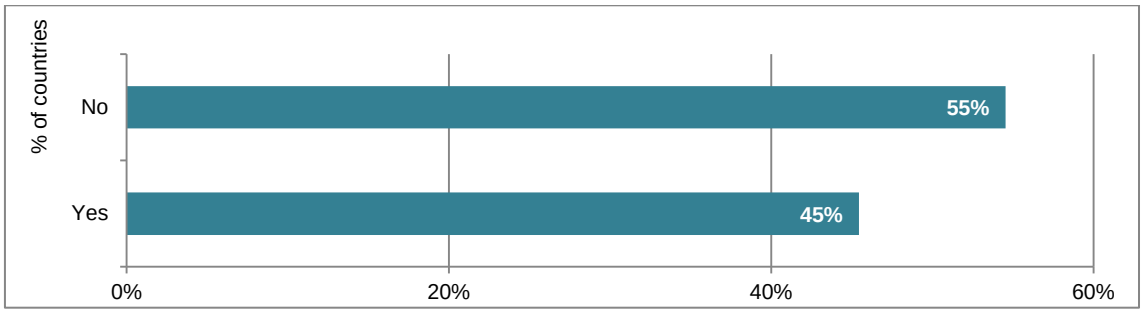
3.5.1 SUPERVISION OF REGULATED HAWALA AND OTHER SIMILAR SERVICE PROVIDERS

Five countries responded that they have a separate examination approach and teams for regulated *hawala* and other similar service providers while six[14] countries did not have such a separate approach, as shown in Figure 3.3. It is not clear whether the separate examination team is only for *hawala* and other similar service providers or it is for general remittance companies, money service providers, or payment institutions, among others.

In the case of Australia, within the FIU, there is a centralised team that focuses on remittance service providers.

[14] Only 11 out of 15 surveyed countries where *hawala* and other similar service providers are legal provided the information.

Figure 3.3 **Separate Team to Examine Regulated *Hawala* and Other Similar Service Providers (percentage of countries)**



Source: FATF project questionnaire.

3.5.2 SURVEY RESULTS: REGULATORY AND SUPERVISORY AUTHORITIES

In developing countries, the Central Bank is most of the time the supervisory authority for HOSSPs, while there is more diversity in the case of developed countries. Except for one country, the same agency is responsible both for regulation and supervision of the legal *hawala* and other similar service providers. Though the sample size is small, there are essentially four different institutional arrangements for the regulation and supervision of legal HOSSPs:

1. Central Bank
2. Financial Supervisory Authority (FSA)
3. Financial Intelligence Unit (FIU)
4. Others like Excise and Customs department, Department of Internal Affairs

Having the central Bank as the regulator and supervisor is the most common model in developing countries, as the Central Bank is the default supervisor for the whole financial market in addition to being one of the most established state agencies in these countries.[15]

The most common regulator and supervisor in developed countries is the Financial Supervisory Authority. In the case of Germany, Norway and Sweden, this authority is the sole regulator and supervisor for the legal HOSSPs. In the UK, the FCA (Financial Conduct Authority) regulates and supervises in cooperation with another authority, "H M Revenue and Customs".

In several countries, the FIU has been designated as the AML/CFT regulator and supervisor of legal *hawala* and other similar service providers – for instance Canada and United States. In the U.S., the FIU has delegated examination of HOSSPs to their tax authority. In Australia, all the AML/CFT supervision including those of *hawala* and other similar service providers is undertaken by the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian FIU.

All these various arrangements are outlined in Table 3.4.

15 See Todoroki, Noor, Celik, Kulathunga (2013).

Table 3.4 **AML/CFT Regulatory and Supervisory Authorities in Surveyed Countries**

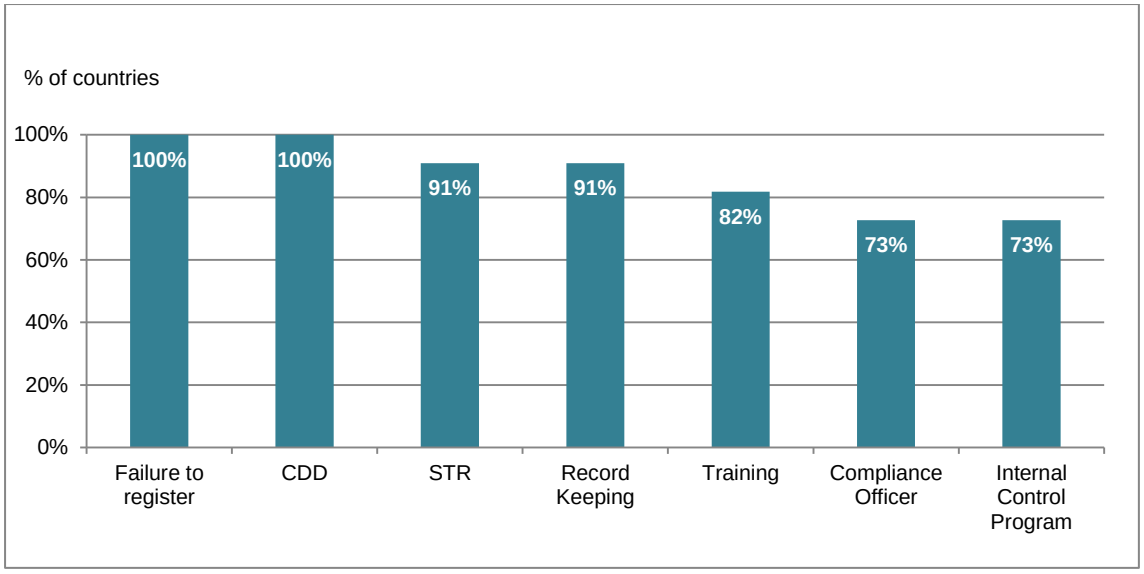
Countries	Regulatory Authority	Supervisory Authority
Australia	AUSTRAC (Australia's AML/CTF regulator and FIU)	AUSTRAC (Australia's AML/CTF regulator and FIU)
Germany	BaFin (Financial Services Authority)	BaFin (Financial Services Authority)
Republic of Guinea	Central Bank	Central Bank
Norway	Finanstilsynet (The Financial Supervisory Authority of Norway, FSA)	Finanstilsynet (The Financial Supervisory Authority of Norway, FSA)
Lebanon	Central Bank	Central Bank
Hong Kong	Customs and Excise Department	Customs and Excise Department
Slovenia	Central Bank	Central Bank, Office for money laundering Prevention
Netherlands	Central Bank	Central Bank
Sweden	Finansinspektionen (The Swedish Financial Supervisory Authority)	Finansinspektionen (The Swedish Financial Supervisory Authority)
New Zealand	Department of Internal Affairs	Central Bank
Indonesia	Central Bank	Central Bank
UK	HM Revenue and Customs, Financial Services Authority	HM Revenue and Customs, Financial Conduct Authority
US	FIU	FIU (HOSSPs examinations delegated to tax authority)
Canada	FIU	FIU

Source: FATF project questionnaire.

3.5.3 SANCTIONS APPLICABLE TO REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS FOR FAILURE TO IMPLEMENT AML/CFT REQUIREMENTS

Survey results (Figure 3.4) highlight the range of compliance issues that can lead to sanctions applied to regulated *hawala* and other similar service providers (failure to register/become licensed; failure to comply with AML/CFT obligations such as CDD, STR, record keeping, training, compliance officer and internal control program) and the percentage of surveyed countries having such sanctions available.

Figure 3.4 **Sanctions for Failure to Implement AML/CFT Obligations (percentage of countries)**



Source: FATF project questionnaire.

Note: *Hawala* and other similar service providers are legal in 15 countries. Out of 12 FATF member countries where Hawala and other similar service providers are legal, 11 countries provided the data. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

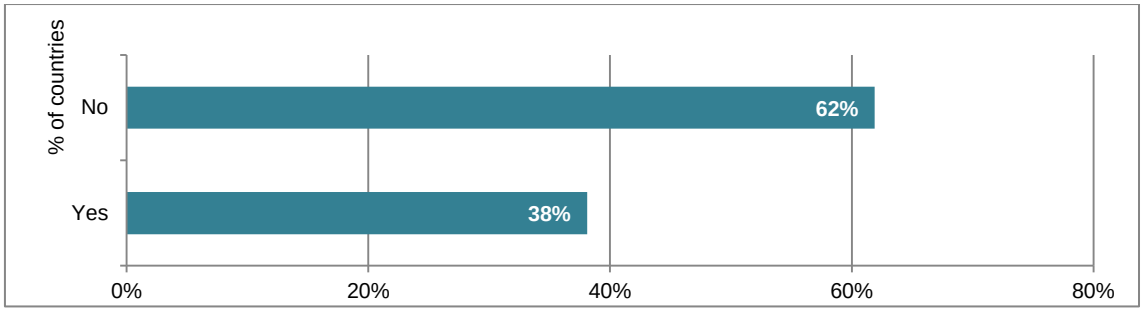
As *hawala* and other similar service providers are treated the same as any other remittance companies for the purpose of AML/CFT obligations, sanctions applicable to *hawala* and other similar service providers for failure to implement AML/CFT requirements are general provisions that apply to all MVTS whether they are called remittance companies, money service providers, or payment institutions. The questionnaire did not specifically ask whether sanctions are the same for all the financial institutions including MVTS or not, but some countries impose the same range and scale of sanctions for all the financial institutions while others have different scale and range of sanctions depending on types of financial institutions (for example, there are differences between banks and MVTS).

Though sanctions are applicable for failure to implement AML/CFT requirements in most of the countries, survey data pointed out that actual enforcement cases where sanctions were imposed against *hawala* and other similar service providers have been very few in most of the countries in the last five years.

3.5.4 REQUIREMENTS ON FOREIGN COUNTERPARTIES

Twenty one surveyed countries answered the question whether money transmitters in their countries can only deal with registered/licensed money transmitters in the ultimate recipient country and only eight out of these twenty one impose such a requirement (Figure 3.5).

Figure 3.5 **Requirement to Deal only with Regulated Money Transmitter in Ultimate Recipient Country (percentage of countries)**

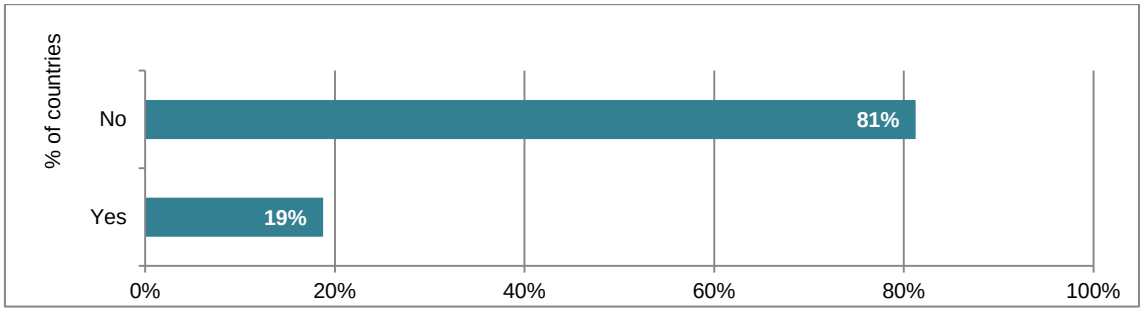


Source: FATF project questionnaire.

Note: Out of 25 FATF member countries, 21 responded to this question. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Only three out of the 16[16] countries that responded to the question whether "it is a requirement in their country that funds should be sent directly to the pay-out countries by the originating money transmitter." answered positively (Figure 3.6).

Figure 3.6 **Requirement to Send Funds Directly to Pay-Out Country by Originating Money Transmitter (percentage of countries)**



Source: FATF project questionnaire.

This would suggest that further discussion of Recommendation 13 in the context of money transmitters would be useful, in particular whether countries should interpret R13 to require that money transmitters, including *hawala* and other similar service providers, should only deal with licensed or registered foreign counterparties.

3.6 SUPERVISION AND ENFORCEMENT RELATED TO UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

This section discusses the survey results of the oversight of and enforcement against unregulated *hawala* and other similar service providers, sanctions against unauthorized money transmitters, as

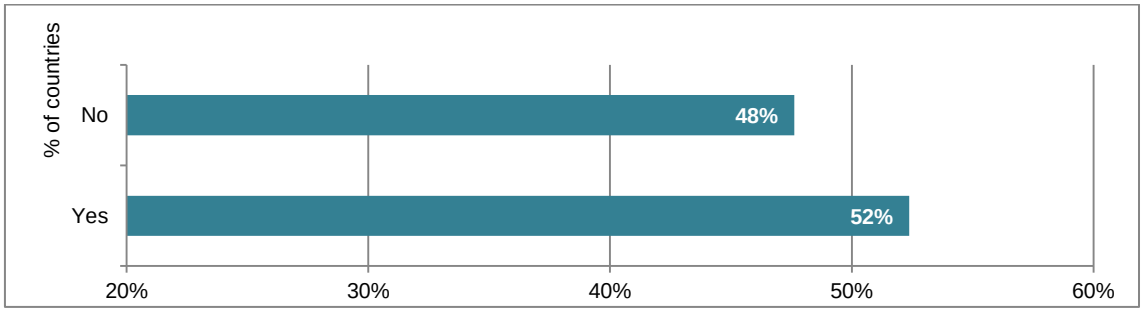
16 Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, 16 countries provided an answer to this question. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

well as various strategies used by countries to identify unregulated *hawala* and other similar service providers and steps taken to shift unregulated players to regulated channels.

3.6.1 IDENTIFICATION OF UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

A majority of surveyed countries have set up specific mechanisms to identify HOSSPs. Out of the 21[17] countries that provided answers to whether they have set up any mechanism to identify illegal *hawala* and other similar service providers in their country, a small majority provided a positive answer (eleven out of 21), see Figure 3.7. Many countries have not yet devised effective mechanisms to identify, monitor and take action as needed against illegal *hawala* and other similar service providers – either in terms of promoting their integration in the AML/CFT regime or cracking down on illegal operations. Given the vulnerabilities of unsupervised financial services providers, this lack of identification and lack of enforcement actions means that HOSSPs may remain a significant vulnerability.

Figure 3.7 **Taskforce to Identify Illegal Hawala and Other Similar Service Providers (percentage of countries)**



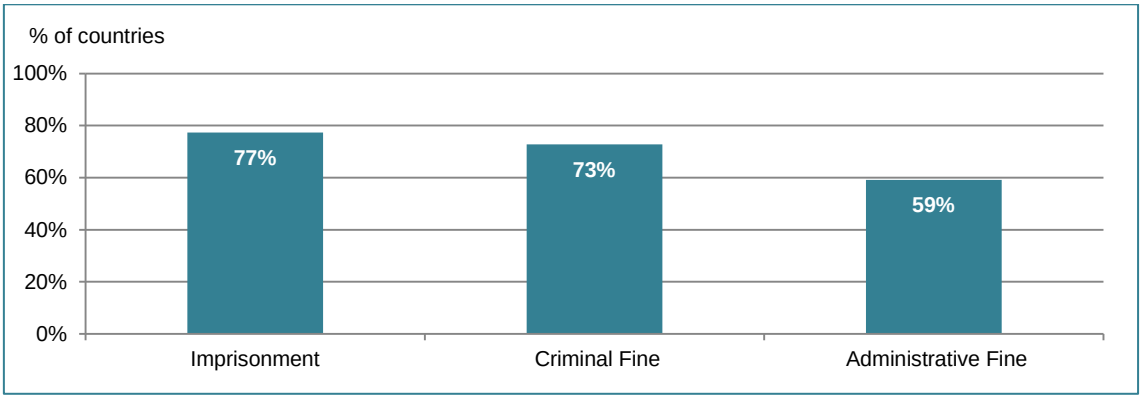
Source: FATF project questionnaire.

3.6.2 SANCTIONS AGAINST UNAUTHORISED MONEY TRANSMISSION OPERATIONS

Most countries have some form of sanctions available for unlicensed/unregistered money transmitters, but few surveyed countries appear to have used them. Surveyed countries indicate having both criminal and administrative sanctions available if HOSSPs keep operating as money transmitters without a license or registration after initial warnings. Most of the surveyed countries consider unauthorized operations as a criminal violation and apply sanctions such as imprisonment and criminal fines. As shown in Figure 3.8, in respectively 77% and 73% of the 22 countries that provided data, imprisonment and criminal fine can be imposed for unauthorized money transmission operations. In only 59% of the countries administrative sanctions are available.

17 Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, 21 countries provided an answer to this question. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Figure 3.8 **Sanctions against Unauthorized Operations (percentage of countries)**



Source: FATF project questionnaire.

Note: Out of 25, 22 FATF member countries provided the data on sanctions. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Though sanctions are available, the survey shows that countries have not used them effectively against unauthorized operations in the last five years.

3.6.3 IMPORTANCE OF SUSPICIOUS TRANSACTIONS REPORTING OBLIGATIONS IN IDENTIFYING ILLEGAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Suspicious Transaction Reporting (STRs) can be a very effective tool in identifying illegal *hawala* and other similar service providers. The survey sought information on suspicious transaction reports (STRs) submitted by regulated *hawala* and other similar service providers or by banks on unregulated *hawala* and other similar service providers for the last three years. The majority of the surveyed countries were unable to provide the data, with only seven countries providing such statistics. For these countries, STRs filed by both regulated *hawala* and other similar service providers and banks on unregulated *hawala* and other similar service providers ranged from about eight reports per year to about 220 reports per year.

It is important that all types of money service businesses including regulated *hawala* and other similar service providers report promptly to the financial intelligence unit (FIU) or any relevant authority if they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing or related to unlicensed money remittance business. The information collected by FIU through STRs can be used by law enforcement agencies (or by supervisors) to conduct further investigations which can help identify illegal *hawala* and other similar service providers. STRs can be very useful technique to track down flow of money especially when banks and other financial institutions are used as a medium of settlement.

To improve STR reporting by regulated *hawala* and other similar service providers as well as by banks and other financial institutions on illegal *hawala* and other similar service providers, the regulatory authorities, in collaboration with the FIU, may issue specific guidelines. Such red flag indicators can be developed also in collaboration with MVTS players which can help detect suspicious transactions.

Box 3.1 **Guidance to Financial Institutions on Red Flag Indicators and Case Studies Leads to Increased STR Filings**

In September 2010, the United States Financial Intelligence Unit FinCEN published an advisory on informal value transfer systems (IVTS) to U.S. financial institutions, including recent case typologies. The advisory asked filers to include the term "IVTS" in SAR narratives to report IVTS related activity. Following publication of the Advisory, STR filings referencing IVTS increased over 500%. In October 2011, FinCEN published an analysis of STRs referencing IVTS. How many of the STR filings involved actual hawala and other similar service providers have not been determined. The findings were as follows:

a. Currency exchange and unregistered money transmissions dominate STR filings: 57% of filings referenced suspicious currency exchange, while 30% referenced unregistered Money service businesses (MSB) activity (with unregistered currency exchange being the leading cause). 48% of the suspicious currency exchange activity referenced Venezuela, Argentina, Brazil, and Mexico. While 89% of STRs before the advisory referenced Latin America, only 41% of post-Advisory STRs did. Post-advisory transactions involving exchange houses in the UAE, Jordan, and Kuwait, Yemen, and Iran were common.

b. For the subject location, over 49% (1 019 subjects) were associated with foreign addresses, almost 40% of them in Venezuela. Over 90% of New York filings reporting possible unregistered money services business activity involved convenience/grocery stores and the Middle East.

Source: United States.

3.6.4 INDICATORS TO DETECT SUSPICIOUS HAWALA AND OTHER SIMILAR SERVICE PROVIDERS

This sub-section provides guidance on transactions patterns that are often associated with illegal/unregulated money transfer providers, including *hawala* and other similar service providers. These transaction patterns can be identified through effective monitoring and CDD mechanisms and should often raise suspicions by the financial or reporting institutions. Such suspicious transaction patterns include:

1. Extensive use of collective accounts. These can be identified by the reporting institutions if lots of small sums are deposited into the bank account of individuals (often stating their name in the reference line), or if large cash sums are deposited at regular intervals before transfers aggregating all of the smaller amounts from the account are made to foreign accounts. Indicators of such collective accounts can be individuals possibly organized under the aegis of a cultural association collecting money through banking system, or one or more individuals making an aggregated transfer of a large sum of money to a bank or money remitter abroad.
2. Money being transferred at regular intervals to international locations such as Dubai. Dubai is a major international clearing house for remittances and other value transfers. Many trading companies/criminal groups route their money through Dubai to other destinations through *hawala* channel. Most of the hybrid *hawala* transactions are routed through some major international destination such as Dubai.

3. An account been used as a temporary repository and the funds are transferred in and out of the account immediately.
4. Usage of third party accounts to disguise and to avoid detection by authorities. Often such third party accounts have no business connection to the *hawaladar* or sender.
5. Frequent wire transfer activity from an account in sending country to international bank account.
6. Wire transfers frequently sent by traders to foreign countries, which do not seem to have any business connection to the destination countries.
7. Money remitter or trader conducting transactions such that they fall beneath the identification, STR or CTR reporting threshold.
8. Business accounts used to receive or disburse large sums of money but show virtually no normal business related activities such as payment of payrolls, invoices etc.
9. Frequent deposits of third party checks and money orders into business or personal accounts.
10. Frequent international wire transfers from bank accounts which appear inconsistent with stated business activities.
11. Frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
12. Sudden change in pattern of financial transactions from low value international fund transfers to large value transfers by a money remitter.

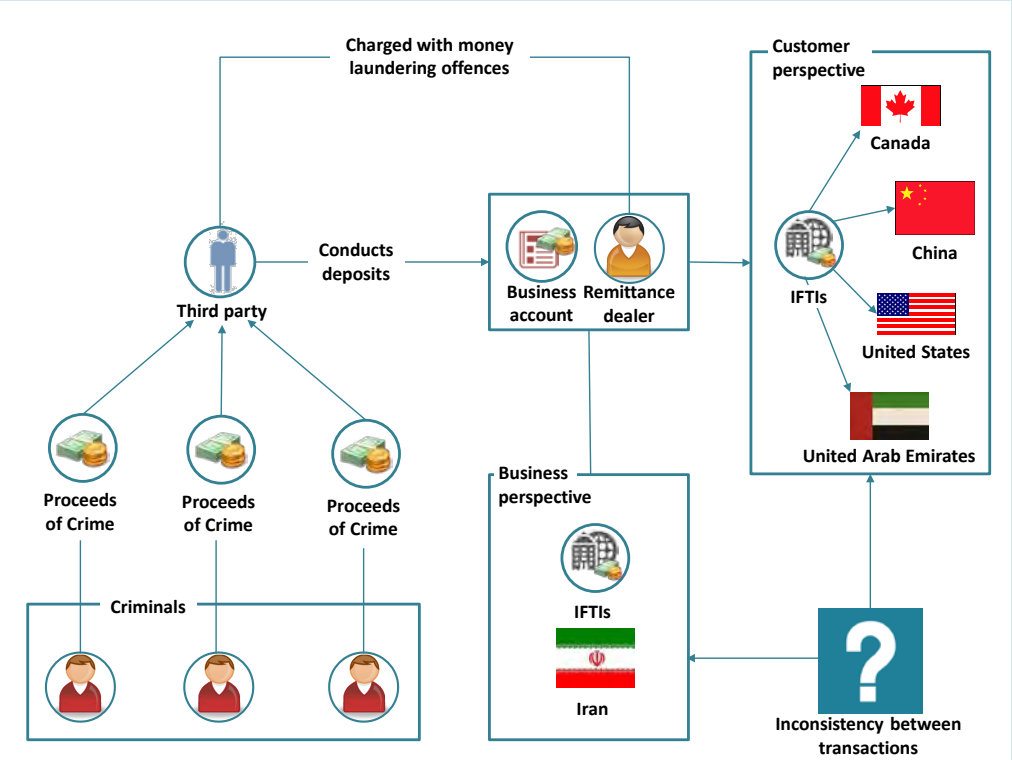
Box 3.2 **Case Study: Money laundering revealed through transaction patterns of the remittance dealer – "Suspicious Transactions"**

AUSTRAC's (Australian Transaction Reports and Analysis Centre) monitoring systems identified a substantial increase in cash activity undertaken by a remittance dealer. Further analysis identified significant inconsistencies between the information the remitter had reported to AUSTRAC, and the information reported by the financial institutions where the remitter was a customer.

This information was referred to the Australian Crime Commission's (ACC) Financial Intelligence Assessment Team (FIAT). After the AUSTRAC referral, the FIAT undertook further investigations and disseminated the intelligence to the Australian Federal Police (AFP), who conducted the investigation. As a result of the investigation two suspects were charged with money laundering offences under the Criminal Code Act 1995. One of the suspects was the remittance dealer, while the second suspect, an associate of the first suspect, allegedly acted on behalf of third parties to deposit large amounts of cash into accounts owned by the remittance dealer.

This investigation was triggered by recognized money laundering indicators. AUSTRAC data revealed significant discrepancies between the transactions reported by the remittance dealer from its own 'business' perspective, and the transactions reported to AUSTRAC by the financial institutions which dealt with the suspect remittance dealer as a customer (that is, transactions

reported from a 'customer' perspective).



Transaction reporting information received by AUSTRAC revealed a number of significant and suspicious changes in the financial transaction patterns of the remittance dealer involved:

- The remittance dealer's activities changed from facilitating small outgoing international funds transfer instructions (IFTIs), to accepting large cash deposits and facilitating large IFTIs. This spike in financial transaction activity was clearly inconsistent with the remitter's previous profile and history.
- Shortly after this increase in the size of IFTIs, business bank accounts held by the remittance business stopped receiving deposits. However, AUSTRAC analysts identified additional accounts operated by the remittance business, which had been opened under a new company name. Under this new company name, the remitter's business practices appeared to change. While the remitter continued to report to AUSTRAC that the majority of its remittances were being sent to Iran, information received from institutions dealing with the remitter as a customer reported that a significant proportion of the business's outgoing IFTIs were now being sent to the United Arab Emirates (UAE).
- The remitter's transaction activity continued to escalate while operating under the new company name. Over a three-month period the remitter recorded cash deposits of AUD34 million and outgoing IFTIs of AUD33 million. At the peak of activity, the remitter was receiving cash deposits into its bank account of AUD1 million each day, and on one occasion received almost AUD4 million in two days. The third party making these large cash deposits made no attempt to conceal them, and they were conducted at the same bank branch.
- Information provided by reporting entities was also invaluable in highlighting discrepancies in

the remitter's activities. The value of the remittance dealer's business activity as reported to AUSTRAC was significantly less than that reported by the financial institutions that dealt with the remitter as a customer. This discrepancy in reporting strongly suggested to authorities that the remittance dealer was dealing with proceeds of crime, rather than funds generated by legitimate business activities.

The following table highlights the discrepancies in the remitter's transaction activities as reported from customer and business perspectives, over a 10-month period:

Transaction Types	Value as reported by the remittance business (*i.e.*, from the "business perspective")	Value as reported by reporting entities dealing with the remittance business (*i.e.*, from the "customer perspective")	Difference
Cash deposits recorded in TTRs	AUD 48 million	AUD 92 million	AUD 44 million
Outgoing IFTIs	AUD 55 million	AUD 95 million	AUD 40 million

As the remitter's cash activity escalated, law enforcement agencies executed warrants against the syndicate and stopped its operations. The AFP arrested two individuals, and restrained AUD1.2 million. While the original source of the funds could not be established, the large amount of cash involved led authorities to suspect that the funds were the proceeds of crime.

Source: Australia.

3.6.5 STRATEGIES TO IDENTIFY UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS AND POSSIBLE AVENUES TO CREATE INCENTIVES TO FORMALISE THEIR BUSINESS

There are many different strategies and techniques used by countries to identify illegal *hawala* and other similar service providers [18]. Many of those are used in combination.

Some of the most common methods used to detect such operations are:

1. identifying advertisements placed by such businesses in community newspapers,
2. conducting internet search,
3. searching through social media,
4. following up on leads from general public or service providers,
5. use of AML monitoring systems especially leveraging on useful indications originating from STRs filled by financial institutions,
6. working in partnership with other agencies and gathering information from law enforcement and AML regulatory authority's investigations and inspections and
7. specific targeted investigations and physical surveillance of suspicious entities.

[18] See also FATF (2003).

It is important for countries to foster close co-ordination within the relevant authorities for the purpose of developing inter-agency strategies and efficiently utilizing the available resources to identify illegal operators.

Box 3.3 **Specific strategies used by some surveyed countries to identify illegal hawala and other similar service providers**

Australia: AUSTRAC (Australia's FIU and AML/CTF regulator) along with relevant law enforcement and intelligence agencies identify illegal hawala and other similar service providers. AUSTRAC has an extensive transaction reporting regime entailing threshold transactions reports (TTRs), International Funds Transfer Instructions (IFTIs) and Suspicious Matter Reports (SMRs). The use of transactions reports is one of the mechanisms that are used to highlight potential illegal remittance service providers; particularly those using the banking systems to bulk settle transactions. In addition, AUSTRAC's supervision teams engage with various ethnic communities who may provide useful intelligence about the illegal operators. There have been instances where regulated remittance businesses have provided information in relation to the operation of unregulated remittance businesses.

Malaysia: A surveillance team has been formed within the Central Bank to identify unlicensed money services business (MSB) operators, generally based on public tip off and information from the licensed MSB operators. The surveillance team is also increasingly moving towards gathering its own intelligence to detect illegal hawala and other similar service providers through collaboration with the Financial Intelligence and Enforcement Department and MSB supervision team, as well as information from the internet and public database (such as company registry etc.).

Austria: Awareness training programs for the financial sector, the non-financial sector, law enforcement and supervisory authorities are organized in order to raise awareness as regards the way hawala and similar unregulated value transfer systems work to facilitate the process of cracking down illegal money transfer businesses including hawala and other similar service providers.

United States: The Department of Homeland Security's Homeland Security Investigations (HSI) runs the Cornerstone Initiative to identify illegal operators including HOSSPs. The Cornerstone Outreach Initiative seeks to: 1) Identify the means and methods used by criminals to exploit financial systems in order to transfer, launder and otherwise mask the true source of criminal proceeds, 2) Works with specific private sector industries to gather new information and reduce vulnerabilities found within existing financial systems and 3) Investigate and prosecute criminal organizations exploiting traditional and non-traditional financial systems.

In 2010, HSI published a Cornerstone report dedicated to HOSSPs. The Cornerstone Report is a public facing document and is a mechanism by which private partner sectors are informed about risks of dealing with various players in the market; the sharing of information allows the financial, trade, and retail communities to take precautions in order to protect themselves from exploitation.

The FBI makes extensive use of the over 1 million STRs filed each year in the US to identify HOSSPs. HOSSPs are also identified through linkages with FBI cases and leads from the Joint Terrorism Task Force.

Source: Country Authorities, FATF project questionnaire.

Box 3.4 **FinCEN's Unregistered Money Service Business Outreach Initiative**

FinCEN, the U.S. FIU, has adopted a strategy to identify unregistered money services businesses (MSBs) and coordinate appropriate regulatory actions. FinCEN aims to reduce the number of unregistered MSBs that should be registered by using information from Suspicious Transaction Reports (STRs) and other FinCEN data to assist in identifying these businesses. Once identified through analysis of STRs and other data, institutional outreach is conducted to raise awareness of BSA requirements for MSBs, including registration.

FinCEN data is regularly searched using special search terms (e.g., "unlicensed," "unregistered," "illegal") to identify potential unregistered MSBs named as subjects in STR filings. The FinCEN database is further queried to determine whether any additional FinCEN data exists on the subject(s), and FinCEN's MSB Registrant Search web site is also queried to determine whether they are currently registered. All subjects are also reviewed prior to outreach to identify recent or on-going investigations for determination of whether or not they should be contacted. As a result of FinCEN's July 2011 re-definition of MSBs that included foreign-located entities, foreign-located entities that may be required to register with FinCEN will now be identified for purposes of outreach as well.

An entity identified for outreach is contacted to learn more about the types of activities the entity conducts that may make it an MSB, in order to determine whether the entity must register and to assist it in the registration process. Depending on the outreach results, cases may be referred for possible BSA examination or for possible enforcement actions.

Source: United States.

Box 3.5 **Dutch Migrant Study on Payment Channels**

One potential method to better understand which payment methods remitters prefer and why is through a survey. For instance, The Netherlands Central Bank in April 2013 published a paper investigating the determinants in migrants' choice of payment channels when transferring money to relatives abroad. The paper's authors surveyed 1,680 migrants in the Netherlands and identified five remittance channels: bank services, money transfer operator services, in-cash transfers via unregulated intermediaries, ATM cash withdrawals abroad and carrying cash when travelling home. The survey identified that migrants who regularly used internet banking for other purposes were more likely to use bank services for remittances as well. The paper also found that other drivers exist in determining the choice of payment channels used, such as personal characteristics and country-specific factors, costs (real and perceived), ease of use and availability of remittance transfer options. The paper concluded that financial education, cost reduction, and mobile remittance solutions could expand use of regulated channels.

Source: Kosse, Ameka and Vermeulen, Robert (2013).

Box 3.6 **UK Project QUAVER**

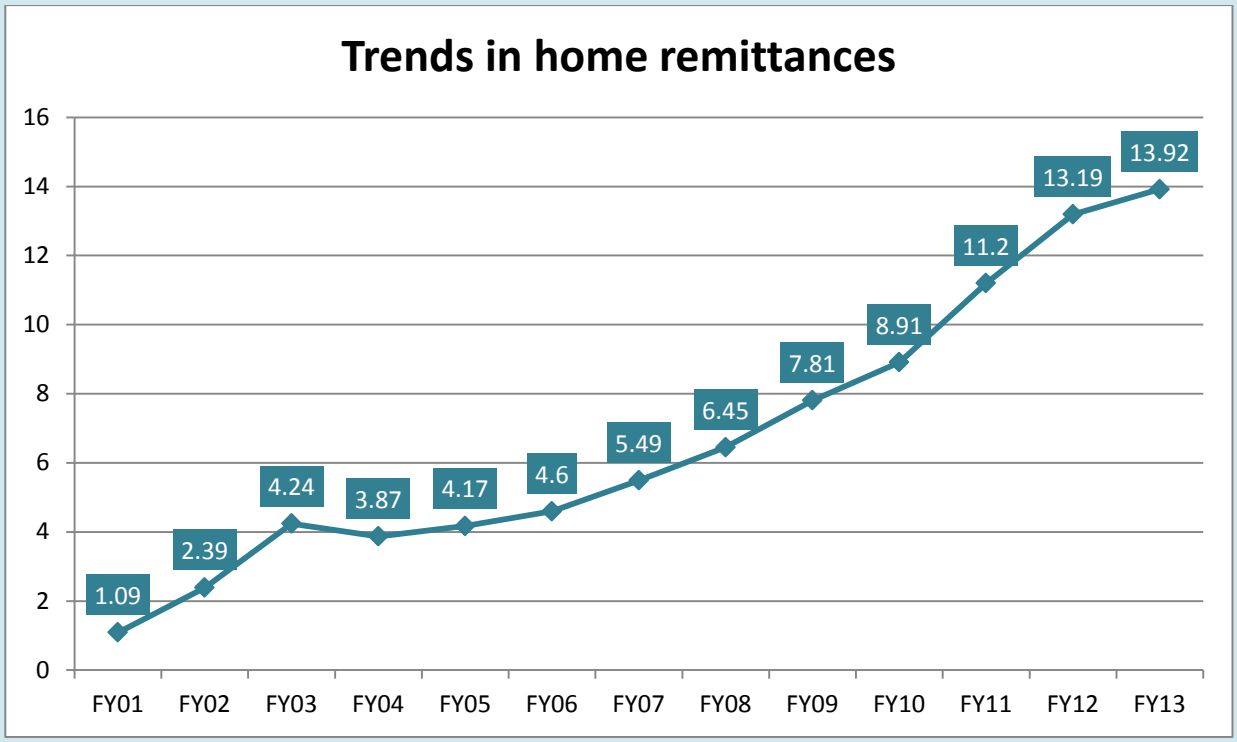
In the UK, all HOSSPs are defined by law as money service businesses (MSB) and are regulated and supervised as such, but are still subject to widespread exploitation by criminal groups. Law enforcement and regulatory bodies have for the last two years been co-operating closely on Project QUAVER, an initiative designed to minimize this criminal exploitation. The project focuses on the communication of commonly seen criminal techniques to the MSB sector, Banks and other financial institutions, designed to improve understanding and facilitate a better appreciation and management of risk in the regulated sector and, accordingly, enhanced compliance with AML/CTF requirements. In addition Serious Organized Crime Agency (SOCA) has been educating regulators and law enforcement colleagues and advising them on how to best approach criminal prosecutions of complicit HOSSPs; the UK has a number of trained Expert Witnesses in money laundering and has delivered similar expert evidence training to colleagues from the USA, Australia and the Netherlands.

The reaction to the project has been positive, with a number of banks and other financial institutions (including large scale MSBs providing payment services for other MSBs) displaying an improved attitude to risk, for example, by closing high risk bank accounts, refusing to carry out third party payments, and by insisting on independent audits of the processes of MSB customers; in addition, a number of MSBs have changed their business practices and are now unwilling to carry out the type of transactions favoured by criminal HOSSPs. The quality and number of Suspicious Activity Reports submitted by businesses in the regulated sector has also increased significantly.

Source: United Kingdom.

Box 3.7 **Pakistan Remittance Initiative (PRI)**

One possible model for moving remittances into regulated channels is the Pakistan Remittance Initiative. A sharp jump had been witnessed in inbound remittances to Pakistan after Financial Year (FY July- June) 2001 as home remittances rose from USD 2.3 billion in FY01 to USD 4.2 billion by FY03 (Figure 1). However, these inflows moderated in subsequent years and reached USD 13.92 billion by FY13. There was increasing realization that a substantial part of these inflows are routed through unregulated channels. Initially, State Bank of Pakistan made policy interventions in the FX market to discourage hawala/hundi system in the country. These efforts helped resume an uptrend in home remittances. Accordingly, in order to provide an ownership structure in Pakistan for remittance facilitation, State Bank of Pakistan, Ministry of Finance and Ministry of Overseas Pakistanis launched a joint initiative called Pakistan Remittance Initiative (PRI) in April, 2009. This initiative has been taken to achieve the objectives of (a) facilitating and supporting efficient flow of remittances and (b) leading to provide investment opportunities in Pakistan for overseas Pakistanis.



At the outset of the drive, a comprehensive objective analysis of the Home Remittance System was carried out with a view to; collect and analyse remittance related data, identify the bottlenecks and weak links in the system, review the recent international efforts on remittances specially in the global and regional perspective, evaluate schemes implemented earlier to enhance remittance flows to Pakistan, and compile practices followed by various jurisdictions to boost remittances. The subject analysis led PRI to formulate a comprehensive strategy aimed at greater commitment of financial sector towards remittance services and resultant inculcation of remittance culture, transparency of remittance market with adequate consumer protection, efficiency of payment system infrastructure, and incentives for the remitters, beneficiaries and overseas entities. These were the basic ingredients to compete with the unregulated channels and provide quality, fast, efficient, cheap and safer services to remitters and beneficiaries through regulated channels.

Through a consultative process, the number of financial institutions involved in remittance services has increased significantly. The realization of business cases in remittances by additional financial institutions has not only facilitated the larger strata of remittance beneficiaries but also resulted in creating a more competitive environment.

PRI is encouraging financial institutions in Pakistan to enhance their outreach worldwide through new remittance- specific related arrangements. Around 400 new arrangements have been finalized by banks in Pakistan with their overseas correspondents since the inception of PRI.

Reliable and efficient payment systems are vital to facilitate delivery of home remittances securely and efficiently and State Bank of Pakistan has already taken number of steps to develop related Payment Systems Architecture of the country.

- Utilization of PRISM (RTGS) to transfer and settle inter-bank Home Remittance transactions. This has enabled banks to transfer inter-bank transactions into beneficiaries' accounts on the same day.

- Apart from RTGS, through ATM Switch, instant A/C credit facility is also available for beneficiaries through IBFT Inter Bank Fund Transfer. This has reduced turnaround time considerably.

Keeping in view of the rising trend in the Home Remittances and importance of the same for the economy, SBP has allowed banks to open dedicated Home Remittance payment centres. Payments can be made to beneficiaries via cash, demand drafts and pay orders. In addition, such Home Remittance Payment Centres would also be allowed to perform the functions of Sales & Service Centres.

In order to provide a reliable and immediate contact point, 24 hours, 7 days a week; a call centre has been established by PRI. All overseas Pakistanis and their families back home can inquire about the remittance services of banks and lodge their complaints with the call centre (0092-21-111-222-774). There are toll free numbers for overseas Pakistanis residing in 12 countries/ regions of the world. Further PRI has its own website http://www.pri.gov.pk for related purposes.

With a view to encourage and to protect the remitters / beneficiaries from any losses that they may incur due to unwarranted delays in receipts of funds in the beneficiaries' accounts, the beneficiary shall be entitled to a return of sixty five (65) paisa per thousand rupees per day from the concerned bank for the number of days credit/payment on account of remittance was delayed.

PRI have organized various training programs related to various facets of remittances services ranging from strategic framework for remittance services to policy level initiatives. PRI also awarded appreciation certificates to top performer branch managers of banks in recognition of their services for the national cause.

International Association of Money Transfer Networks (IAMTN) has awarded Pakistan Remittance Initiative (PRI) with Money Transfer Award 2011 for the category of 'Asia Pacific Including South Asia' and the same has been presented during the ceremony held on November 15, 2011 in London. This award was conferred in recognition to the efforts being made by the PRI to facilitate the flow of remittances through regulated channels to Pakistan.

At the moment, all PRI efforts are aimed at bringing structural changes in the Remittance System of the country with a long-term vision about these recurring flows. It is a daunting task to introduce changes in the decades old systems and procedures with a strongly embedded particular mind-set of the stakeholders involved. The task becomes more difficult in wake lack of financial literacy, perceptual barriers and volatility of exchange rates. Notwithstanding to the impediments, PRI is geared up to achieve its objective of maximizing the flow of remittances through regulated channels in the country.

Source: Pakistan.

3.7 INTERNATIONAL COOPERATION RELATING TO HOSSPS

International cooperation is an important key component to ensure effective oversight of HOSSPs necessary to mitigate the risk of HOSSPs being exploited for money laundering and/or terrorist financing. HOSSPs often transfer funds or their equivalent in value across borders and an evidential or intelligence picture cannot be obtained by one country's authorities without the open exchange of information between all the other countries in which the HOSSPs has a presence. Unfortunately,

few examples of international cooperation were provided in the responses to the survey, likely due to lack of training and expertise of law enforcement or other competent authorities related to HOSSPs.

Box 3.8 **International Controller Investigation**

In 2006, as a result of international co-operation with the Spanish authorities in respect of a UK citizen resident in Spain who was believed to be involved in drug trafficking and money laundering, the UK authorities identified a prolific International Controller operating from Dubai. In the course of UK Operation OVERGO, Dubai Police Operation CANCER and Italian Guardia de Finanza Operation KHYBER PASS it was identified that this person was using a number of Dubai registered trading companies to launder money on behalf of criminal networks in numerous jurisdictions including the UK, the USA, Italy, Albania, India and Colombia.

After a lengthy investigation involving extensive mutual co-operation and evidence gathering between the authorities in Dubai, the UK, the USA and Italy, the Dubai Police arrested the Controller in early 2007, but released him from custody a short while later. On the same day, the Italian authorities arrested further members of the Controller's network, and subsequently issued a European Arrest Warrant for the Controller himself.

The Controller subsequently left Dubai and moved his activities to India, however following further international co-operation between the authorities in the USA and India, including the freezing of several million dollars in bank accounts linked to the Controller, the Indian Enforcement Directorate commenced an investigation and subsequently instituted proceedings for Foreign Exchange and money laundering offences against the Controller; these proceedings are on-going.

Source: UK Authorities.

Box 3.9 **Unlicensed Money Transmitter Investigations**

Case 1.

In August 2010, HSI San Francisco began investigating a U.S. based trading company (TC) suspected of operating as an unlicensed money transmitting business sending funds to Iran. Bank Secrecy Act (BSA) information disclosed wire transfers from high risk countries, as well as businesses previously identified as possibly transmitting funds to Iran in violation of OFAC sanctions. A review of bank accounts disclosed transactional activity consistent with the operation of a Money Service Business (MSB). This activity showed incoming wire transfers from suspect "Trading Companies" followed by pay-outs to individuals with no apparent logical business connection. Further investigation revealed that none of the business or individuals involved in these transactions had a license from the Financial Crimes Enforcement Network (FinCEN) or Office of Foreign Assets Control (OFAC) to transmit money and funds were being sent to/from Iran. It was discovered that the group utilized international wire transfers through a variety of overseas businesses located in the UAE, China, Sweden, and Korea to circumvent existing OFAC regulations. Once these funds were deposited into U.S. bank accounts, the funds would be paid out to other Iranians living in the U.S., or a CPA would "layer" the funds through other US bank accounts owned or controlled by the organization all in an effort to hide it from the Internal Revenue Service. In May 2012, a plea

agreement was reached for one count of Title 18 USC § 1960 and one count of 50 USC §1702 (IEEPA). The business owner later agreed to cooperate with the government admitting that he had worked with family members in Iran as well as an Iranian HOSSP to supply money transmitting services. As part of the plea agreement, it was disclosed how front companies worldwide and HOSSPs were used in conjunction with trade to circumvent OFAC sanctions.

Highlights of International Cooperation: Through numerous HSI Attaché Offices, investigative leads were coordinated with law officials from Afghanistan, the UAE and additional partner countries.

Source: United Kingdom.

Case 2

ZSQ Exchange was a HOSSP operating out of Fremont, California which had transmitted millions of dollars all over the world through a complex system of wire transfers, emails, faxes, commodity exchange and traditional hawala services. Bank Secrecy Act (BSA) documents associated with ZSQ Exchange and the owner, Qader QUDUS, indicated that over a one year period, more than USD 1.2 million dollars was deposited into Qudus' bank accounts. These deposits were followed by wire transfers to various individuals in the Middle East, Pakistan, China, Europe and Japan. A joint HSI, FBI and DEA investigation was conducted with a Confidential Informant (CI) infiltrating a Pakistani-based heroin trafficking organization operating in Maryland. The CI purchased two kilograms of heroin and was instructed to send payments through five separate bank accounts located in New York, San Francisco and Pakistan. The heroin proceeds eventually ended up in the hands of a Pakistani heroin trafficker identified as Momin KHAN-AFRIDI of Peshawar, Pakistan. KHAN-AFRIDI was known by the DEA to be a large-scale heroin and multi-ton hashish trafficker. KHAN-AFRIDI is responsible for heroin distribution throughout the United States, United Kingdom, Thailand, and Canada. The U.S. Treasury Department, Office of Foreign Assets Control (OFAC) designated Khan-Afridi as an international narcotics trafficker. (It was alleged that proceeds from the sale of heroin in the U.S. was commingled with refugee relief money and intelligence sources indicated that some of this narcotics money was being used to finance Al-Qaeda.) Qader QUDUS pled guilty to operating an unlicensed money transmitting business in violation of Title 18 USC § 1960, in the United States District Court, Northern District of California. QUDUS was sentenced to 27 months in prison and ordered to forfeit USD 406 640 to the U.S. Government.

Highlights of International Cooperation - An Internet web site for ZSQ Exchange was discovered identifying ZSQ as a HOSSP. The web site explained how money was to be deposited and identified the bank used and provided the names and address of ZSQ's overseas offices in Kabul, Peshawar, Islamabad, Quetta, Lahore, and Karachi. Bank records revealed numerous wire transfers from ZSQ Exchange to businesses and individuals in thirteen different countries, the majority of which were sent to Japan, China, and Hong Kong. Collateral leads were sent to our HSI attachés in London, Paris, Hong Kong, China, Netherlands, Germany, and Russia.

The UK Metropolitan Police began an investigation to assist HSI London. Japanese police interviewed an individual who received a large number of wires transfers from ZSQ. The individual, a former Mujahedeen General, stated that ZSQ is used to settle large financial transactions between terrorist organizations.

Source: United States.

3.7.1 REGULATOR TO REGULATOR COOPERATION

In order to understand fully the regulatory position of HOSSPs, it is important that the regulators in individual countries are able to share information about the regulatory status of companies that they supervise, and the legal framework under which they are obliged to operate. In order to facilitate this and to allow banks to determine whether HOSSPs are legally licensed or registered before providing banking services, a number of countries make these details available on line. This is the case in Pakistan, United Kingdom, United States, and others. This can be helpful when considering if an unregulated HOSSP has been used for part of the transaction. A transaction may be commenced in accordance with the regulations in the host state, but it may be settled using an operator that is illegal in the destination state. In such cases, there is a greater possibility that the unregulated HOSSP could divert the funds at a later stage and use them for other purposes, such as the payment of an unrelated business transaction between two third parties, as they pass through another jurisdiction, and not be caught.

Alternatively a transaction may be commenced by regulated entities, such as through the banking system at the 'first mile,' but may be paid out by unregulated entities. This is typically seen with remittances from European countries and the United States to Somalia, which are generally initiated with a licensed or registered money transmitter receiving customer funds and remitting them via the banking system to associated companies in the UAE, after which point the UAE companies connected to the international clearinghouse operations of the money transmitters use the funds to purchase goods for export into Somalia, with the ultimate settlement of the transaction being made from the proceeds of the sale of the goods there.

Box 3.10 **EU Passporting System**

In the EU, businesses conducting remittance activity are required to comply with the terms of the EU Payment Services Directive (full title Directive 2007/64/EC on payment services in the internal market). This directive is enacted into law in the domestic legislation of each of the EU member states. The main purpose of the directive is prudential, *i.e.,* to ensure that anyone using payment services in the EU has their money protected by a single legal framework.

Amongst the provisions of the directive is one which allows a business that is regulated in one member state to carry out payment services in another without the need to be supervised by the regulator in that state. This is known as 'passporting'. In such circumstances it is essential that, in order to adequately fulfil their regulatory responsibilities, the regulatory bodies in each country into which the business passports enter into an open information sharing agreement with the authorities in the host country.

Source: European Commission (2007).

3.7.2 EGMONT REQUESTS

The Egmont Group of Financial Intelligence Units was formed in 1995 with the aim of providing a forum for financial intelligence units around the globe to improve international co-operation in combating money laundering and terrorist financing. The group currently has 139 members. Amongst other things, the group facilitates the exchange, on an intelligence only basis, of

information and intelligence relating to suspected offences impacting the group member states. This information exchange takes place between the FIUs in the relevant jurisdictions. It also publishes information relating to typologies and indicators of criminal activity, including fraud, money laundering and terrorist financing identified in the course of its co-ordination activities.

Sharing information in this manner has led to numerous examples of persons being convicted of offences in their country of residence where information received from an overseas FIU generated a new and significant line of enquiry.

Box 3.11 **Egmont information sharing**

An African national residing in a European country (Country Z) declared that he performed hawala banking activities. His account was exclusively credited by cash deposits and numerous transfers for small amounts.

Over the course of several months the funds were transferred to company A in Africa. Shortly thereafter the funds were transferred to company B in Country Z. Companies A and B performed international money remittance services. According to the subject, he performed hawala activities for fellow countrymen wishing to send money to Africa. However, he did not hold any position within companies in country Z where he executed the transactions and he was not registered as a representative of an authorized exchange office.

Police enquiries revealed that he was known to be a member of a terrorist organisation and it is thought that this alternative remittance system may have been used for terrorism financing.

Source: Egmont group website – www.egmontgroup.org/library/cases.

3.7.3 JOINT INVESTIGATION TEAMS (JITS)

A Joint Investigation Team is an investigation team set up for a fixed period, based on an agreement between two or more European Union member states and/or competent legal authorities for a specific purpose. Non EU member states can also participate in a JIT with the agreement of all other parties. The concept of JITs is set out in Article 13 of the 2000 EU Convention on Mutual Legal Assistance.

JITs are specifically geared towards assisting EU member state law enforcement and judicial authorities tasked with instigating complex investigations into organized crime groups, by virtue of which cross jurisdictional serious criminality can be tackled by different Law Enforcement agencies and Prosecutors working in single teams. The JIT is usually set up in the member state in which the investigation begins.

Europol, the European Law Enforcement Agency, and Eurojust, the European Union's judicial co-operation unit, assist in the setting up, implementation and conduct of JITs. In addition, Eurojust, can provide legal advice to member states engaging in JITs.

The key advantages of a JIT are:

- No requirement for international mutual legal assistance requests
- Intelligence and evidence sharing between JIT members. Such evidence can be used in court

- Members of the JIT can be present at house searches, interviews of suspects and other associated areas of operational activity in all jurisdictions covered.

Funding for the establishment of JITs is available from Eurojust. This funding is available for reimbursing travel costs, accommodation, translation and interpretation; in addition, Eurojust can fund/host operational meetings.

3.7.4 MUTUAL LEGAL ASSISTANCE (MLA)

In contrast to Egmont requests, which allow for the sharing of information for intelligence purposes only, MLA requests are required (although not in all circumstances) when the authorities in one country wish to gather, or have gathered, material in another country which will be required to be used as evidence in criminal or other proceedings.

MLA requests are generally required when a request for evidence to be gathered in another jurisdiction requires some form of judicial oversight, a degree of coercion or the invasion of privacy; for example when a request is made for the obtaining of evidence by questioning of a suspect after arrest, the search of a premises under warrant, or a judicial order for the production of information, such as banking or other information held under the presumption of confidentiality.

MLA requests can result in certain types of evidence being obtained and used in one country that would not be permissible under that country's domestic legislation; for example, transcripts of telephone intercepts conducted outside the UK are in certain circumstances admissible as evidence in UK courts, even though the law in the UK explicitly excludes the use of such material gathered in the UK as evidence.

MLA requests are issued by the competent legal authority in one jurisdiction on the application of either a prosecuting authority or, where proceedings have been instituted, on behalf of the person charged. The judicial authority can only issue an MLA requests if it appears to them that an offence has been committed, or if there are reasonable grounds for suspecting that an offence has been committed, and that proceedings in respect of the offence have been instituted, or the offence is being investigated. The nature of the assistance sought must be specified in the request, as must the use to which the resulting information is to be put.

Whilst MLA requests have a vitally important role in supporting prosecutions of HOSSPs, it is frequently the case that, for various reasons, such as for example a simple lack of resources, or because the requesting country does not fully understand the legal requirements of the receiving country for dealing with such requests, that the servicing of the request by the receiving country is delayed (on occasions the results can be received after the conclusion of proceedings). This can have significant implications for the prosecution in the country issuing the MLA requests, ranging from the proceedings being delayed, to vital evidence being unavailable during court proceedings. Regular and on-going communication between the authorities in the issuing and receiving countries is therefore vital during the MLA requests process.

Ironically delays in the MLA requests process can work to a defendant's advantage as there are numerous cases whereby a defendant's legal team has been able to adduce evidence gathered in an

overseas jurisdiction, due to them not having to follow the MLA requests procedure, when an MLA requests in respect of similar prosecution evidence has been held up by judicial procedures.

BIBLIOGRAPHY

European Commission (2007), *Directive 2007/64/EC on payment services in the internal market*, EU Payment Services Directive.

FATF (2003), *Combating the Abuse of Alternative Remittance Systems: International Best Practices, June 2003,* OECD, Paris.

Kosse, Ameka and Vermeulen, Robert (2013), *Migrants' Choice of Remittance Channel: Do General Payment Habits Play a Role,* DNB Working Paper, No. 375, April 2013.

Appendix CC:

FATF, *Report on New Payment Methods* (Paris: FATF, 2005)

Financial Action Task Force

Groupe d'action financière

REPORT ON NEW PAYMENT METHODS

13 OCTOBER 2006

Executive Summary

New and innovative methods for electronic cross-border funds transfer are emerging globally. These new payment tools include extensions of established payment systems as well as new payment methods that are substantially different from traditional transactions. New payment methods raise concerns about money laundering and terrorist financing because criminals can adjust quickly to exploit new opportunities.

The present study analyzes prepaid cards; Internet payment systems; mobile payments; and digital precious metals in order to: (1) Identify trends in the adoption of new payment technologies; (2) Assess money laundering (ML) and terrorist financing (TF) vulnerabilities; and (3) Determine whether the Financial Action Task Force (FATF) Forty Recommendations and Nine Special Recommendations (40 + 9) adequately address any potential vulnerabilities.

The study found there is a legitimate market demand served by each of the payment methods analysed, yet potential money laundering and terrorist financing vulnerabilities do exist. Specifically, offshore providers of new payment methods may pose additional money laundering and terrorist financing risks compared with service providers operating within a jurisdiction.

While it is believed that the FATF 40 + 9 provide the appropriate guidance to address the vulnerabilities associated with these new methods of payment, the study does suggest further examination of the effect these evolving technologies may have on cross-border and domestic regulatory frameworks in order to ensure their compatibility with the FATF 40 + 9.

Table of Contents

1. Introduction

Payment innovations that use the Internet, wireless devices, and even well-established payment networks are appearing globally. Both domestic and offshore service providers may offer these new payment methods (NPMs). While a few NPMs operate or are used in multiple countries or even globally, most are limited in their operational reach or use to specific geographic markets or for specific types of transactions involving the purchase of goods and services. Some NPMs also support domestic, and in some instances, cross-border fund transfers between individuals.

The present study analyzes prepaid, cards; Internet payment systems; mobile payments; and digital precious metals to: (1) Identify trends in the adoption of new technologies; (2) Assess actual money laundering (ML) and terrorist financing (TF) vulnerabilities; and (3) Determine whether the Financial Action Task Force (FATF) Forty Recommendations and Nine Special Recommendations (40 + 9) address any vulnerabilities identified.

This report updates a review of NPMs that FATF members conducted in 1996-1997.[1] Most of the specific payment tools described in this report were not yet in use when the previous FATF study was conducted, which was at the dawning of the Internet era. Accordingly, the previous FATF study of new payment methods concluded: "It is premature to consider prescriptive solutions to theoretical problems."[2] Many of the concerns of ten years ago, however, no longer appear to be theoretical.

More recently, in the FATF 2004-2005 Typologies Exercise, participants re-examined new payment methods as part of the Alternative Remittance Systems (ARS) typologies project.[3] The ARS report stated: "[T]his study very briefly touches on the issue of new payment methods including e-money. Although many of these systems might also be included in the term *alternative remittance systems*, their characteristics are so atypical that they would almost deserve a separate study." Some of the tools and techniques identified in that report are considered in more depth in this study.

The research underlying this report began with a questionnaire that attempted to identify the new payment methods appearing around the world and to estimate market size; how or if those payment tools were subject to regulation, supervision, or licensing; whether there was evidence of ML or TF activity associated with those new payment methods; and whether there were relevant law enforcement cases. Thirty-eight jurisdictions responded to the questionnaire.

The results of the questionnaire show in general that it is not always easy to identify new payment methods (NPM). As a consequence, these results may not mirror the real supply of NPM around the world, but only the perceived supply in the jurisdictions which have provided responses to the questionnaire. The periodic surveys of NPMs conducted by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements (BIS)[4] are a useful complement to this report. However, these surveys on developments in

---

[1] The first formal FATF study of the emerging payment methods discussed in this report is found in the 1996-1997 Report on Money Laundering Typologies, February 1997, Section V and Annex 1. See http://www.fatf-gafi.org/findDocument/0,2350,en_32250379_32237235_1_32247552_1_1_1,00.html.

[2] February 1997 Typologies Report, p. 14. These conclusions were subsequently updated and generally re-endorsed in two later annual FATF typologies reports of 10 February 1999 and 1 February 2001.

[3] 10 June 2005, section I, see http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf

[4] The CPSS, under the auspices of the BIS, regularly publishes reports analyzing developments in domestic and cross-border payment, clearing, and settlement systems. See "Survey of developments in electronic money and internet and mobile payments," CPSS publications no. 62, March 2004, at http: www.bis.org/publ/cpss62.htm. For the most recent statistical information on payments and settlement systems (including certain NPMs), see CPSS, "Statistics on payment and settlement systems in selected countries—Figures for 2004," BIS, CPSS #74, March 2006, at http://www.bis.org/publ/cpss74.htm.

payments market do not focus on anti-money laundering (AML) or countering the financing of terrorism (CFT) as they apply to NPMs, which is the purpose of this study.[5]

The project team, which included representatives from Asia, the European Union member countries, and the United States, conducted additional primary research by consulting public and private sector experts. At the 2005-2006 Typologies Experts Meeting on ML and TF in Rio de Janeiro, the project team heard Mr. Joshua Peirez of MasterCard and Mr. Allen Love of PayPal describe their respective company's payment tools and markets; Mr. Vicente S. Aquino, Executive Director of the Philippines' Anti-Money Laundering Council Secretariat, described that nation's mobile payment systems; and Ms. Sheri Dunlop of the United States Secret Service presented a ML case study involving the use of digital precious metals. At other times, core project team members met with representatives from Visa and American Express and prepaid card program management firms in the United States.[6] Finally, project team members reviewed a variety of related media articles and public sector reports.

This report reflects the contributions of payment system and anti-money laundering and regulatory experts from a variety of countries. In many cases, the definitions and terminology used to describe similar payments systems or payments activities vary from country to country. To provide clarity and consistency within this report, the members of the working group have chosen to adopt, as much as practical, the terms and definitions applied to payments systems by the CPSS.[7] Whenever the terms or definitions used in this report diverge from this source, the variation is highlighted and explained.

The report is divided into six sections. Sections 1 and 2 provide an executive summary and a brief introduction. Section three describes how the new payment methods addressed in this study operate and are used.[8] Section four introduces a ML and TF risk matrix developed by the project team to assess the potential ML/TF risk of each NPM in this study. Section five addresses how the FATF Forty Recommendations and Nine Special Recommendations apply to NPM, and presents selected jurisdictional regulations. Section six summarizes the 38 responses to the FATF NPM questionnaire prepared by the project team.[9] Section seven offers conclusions and highlights areas for further consideration by the FATF.

2. Background

How payment system innovations emerge is associated with a number of factors specific to each country, including the underlying economic environment, technology, preferences, actual and perceived costs, along with regulations, policies, and practices of government and private entities with significant influence on the payments system. The fundamental trend, however, across all nations is the migration from paper to electronic payments.

Moving away from paper payments to standardized electronic transaction processing has had the effect of breaking down the payment system into distinct business segments. Hardware, software, communications lines, systems management, accounting, marketing, and distribution have all emerged as distinct business lines for distinct payment services. This segmentation, and the specialization that has resulted, has led to the entry of

[5] Another reliable source of information about the development and the state of the market of NPM's is the website of the electronic payment systems observatory (ePSO), managed by the European Central Bank: www.e-pso.info.

[6] NetSpend, Green Dot, and Wild Card Systems (now eFunds).

[7] See CPSS, "A Glossary of terms used in payments and settlement systems," BIS, March 2003, at http://www.bis.org/publ/cpss00b.htm.

[8] A detailed presentation of traditional credit and debit payment methods (on which most new payment methods are based) is contained in Appendix A.

[9] A detailed summary of the questionnaire responses can be found at Appendix B.

nonbanks as both outsourced service providers to the banking industry and sometimes competitors in the market for clearing services.[10]

While banks remain the core providers to end-users for most retail payment instruments and services, payment applications are now available from a wider range of service providers. The move from paper to electronic transactions has enabled non-bank service providers to customize their payment instruments and to package them with complementary products in order to serve niche markets.

Nonbanks now serve as Internet payment portals, transferring payments between payers, payees and their account-holding institutions. Nonbank intermediaries also transfer payments between buyers and sellers who transact through Internet retail storefronts and through online auction sites. Nonbanks, in fact, pervade the payments industry, processing transactions, maintaining databases, and even operating as value providers in e-money schemes. The result is that "the line between the direct provision of retail payment services to end users by non-banks and the provision of related support services to users and payment providers is much less clear than in the past."[11]

Traditional and Non-traditional Retail Payments

Traditional retail payments are generally low-value, consumer payments that do not require immediate settlement.[12] Traditional electronic payments include bank payment products and services and money transfers that are carried out through nonbank intermediaries such as Western Union, which generally work as credit transfers but do not rely directly upon the transfer of funds between bank accounts.

The FATF defines a money or value transfer system as a "financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer system belongs."[13]

Supplementing these traditional retail payments are newer, innovative payment products, or non-traditional retail payments. For the purposes of this report, we refer to these types of payments as "new payment methods", although they are also often referred to as "e-money" by international payments system experts. NPMs include a variety of innovative products that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems. NPMs also include products that do not rely on traditional payment systems to transfer value between individuals or organizations.[14] This report considers the following NPMs: prepaid cards, electronic purses, mobile payments, Internet payment services, and digital precious metals. Table 1 below provides for a schematic distinction, amongst NPMs, between those that are an extension of traditional payment instruments and those which are *strictu senso* new payment methods.

---

[10] Clearing and Settlement Arrangements for Retail Payments in Selected Countries, Committee on Payment and Settlement Systems, Bank for International Settlements, September 2000 (CPSS #40)

[11] Policy Issues for Central Banks In Retail Payments, Committee on Payment and Settlement Systems, Bank for International Settlements, March 2003 (CPSS #52)

[12] Paper non-cash retail payment instruments include checks, demand drafts, cashiers checks, money orders, traveler's checks, and other related bank drafts. Electronic non-cash retail payment instruments include credit and debit cards as well as credit transfers and direct debits completed through systems such as an automated clearinghouse (ACH). See Appendix A for detailed descriptions of traditional debit and credit card systems.

[13] Interpretative Note to FATF Special Recommendation VI: Alternative Remittance, February 2003.

[14] For the purposes of this study, we have excluded from consideration any non-traditional means of clearing and settling paper check payments or bank drafts through the use of electronic information or electronic check images, including their conversion to electronic funds transfers via ACH systems.

New Payment Methods (NPM)

Extensions of traditional retail electronic payment systems	New non-traditional retail electronic payment systems
Prepaid payment cards	Electronic purse
Internet payments based on bank accounts[15] *(not covered in this report)*	Internet payments not based directly on a bank account
Mobile payments based on bank accounts	Mobile payments not based directly on a bank account
	Digital precious metals

Table 1

Prepaid cards

Prepaid payment cards provide access to monetary funds that are paid in advance by the cardholder. While there are many different types of prepaid cards that are used in a variety of ways, they typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the funds prepaid for all cards issued. The cards may be issued by, and accounts may be held at, a depository institution or a non-bank organization; pooled accounts would be normally held by the issuer at a bank.

Prepaid cards can be issued for limited or multiple purposes. Limited-purpose or *closed system* prepaid cards can be used for only a limited number of well-defined purposes and their use is often restricted to specific points of sale or for specific services. Examples include merchant-issued gift cards, prepaid long distance service, and mass transmit system cards. These cards may either be limited to the initial value posted to the card (non-reloadable) or may allow the card holder to add value (up to a certain limit) and reuse the card (reloadable). The issuer of the card or its service provider typically operates the network on which the cards can be used. The value on the cards generally is linked to a prepaid account established by the issuer or service provider. Transactions are processed in a similar fashion to transactions involving debit or credit cards.

Multipurpose or *open-system* prepaid cards can be used across a broader range of locations for a wider range of purposes. Such cards may be used on a national or international scale but may sometimes be restricted to a certain geographical area. Multipurpose cards may be used by the person who purchased the card or by someone else. Examples include payroll cards and general purpose "cash cards" for individuals without bank accounts or a credit card. These cards are usually associated with a card payment network, such as Visa or MasterCard, which permits them to be used in the same manner as a debit card to make purchases or to get cash from an automated teller machine (ATM). Some issuers do not require the cardholder to have a depository account. These cards are distributed by merchants, depository financial institutions, and money/value transfer (MVT) systems for a variety of purposes. Most are reloadable.

[15] The expression "bank account" used in this box refers to accounts held at financial institutions that are subject to AML requirements.

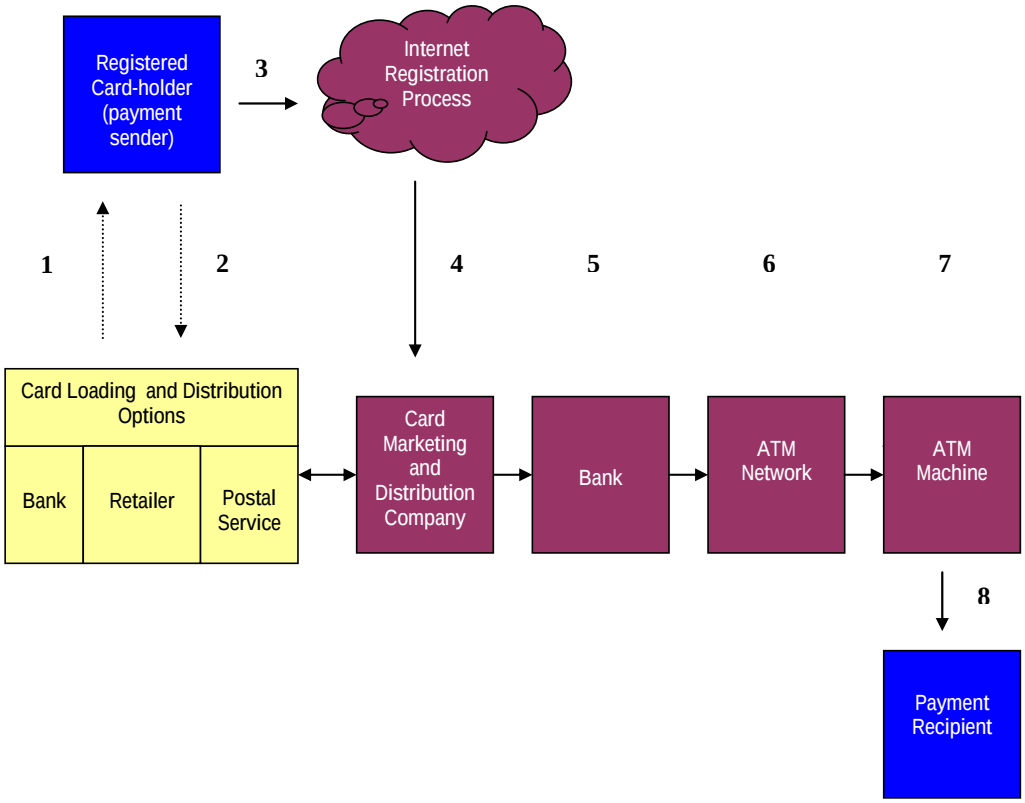


Figure 1 The process of issuing an open-system, magnetic strip, prepaid card varies by issuer. Steps (1), (2), and (3) above may occur in any order. In those three steps an individual completes the registration process for a prepaid card, prepays funds into the card account, and receives the card. Step (4) is the transfer of registration information to the service provider. When a card carries a bank association service mark (as in the case of MasterCard- or Visa-branded cards), the service provider must contract with a bank (5) in order to have access to the global ATM networks (6). Individual ATM machines (7) connect to local networks and often global networks allowing individuals in one country (8) to access funds held in another country.

Electronic purse

An electronic purse, or e-purse (also referred to as a "stored value card" as the value is stored on the card), is value stored electronically in a device such as a card with an integrated circuit chip (called a smart card or chip card).[16] Unlike a card with a magnetic stripe, which stores account information, an e-purse actually stores funds on the card's memory chip. The user is literally carrying his funds with him on the card (hence the name electronic purse).

In some e-purse programs value can be transferred from the card directly to participating merchants or another individual without the transaction going through an account at an intermediary. This may limit the amount of

[16] This definition augments slightly the normal CPSS usage of the term "electronic purse" to also encompass the term "electronic money". For the purposes of this report, the term electronic purse is "a reloadable, multi-purpose prepaid card which may be used for small retail or other payments instead of coins" where the "value is stored electronically in a device such as chip card."

identifying information available with such transactions. To obtain funds from an e-purse payment, however, the merchant or individual must redeem the value from an account held by the e-purse provider at the e-purse issuing institution. As the funds are on the card, no online connection and no cardholder identification are needed to make a payment. The electronic purse function was designed to substitute for cash in everyday situations. Today, electronic purses are mainly used for micropayments such as for public transportation, parking tickets or vending machines.

The development and use of card-based e-purses has declined considerably over the past decade so that very few e-purse systems remain in existence. In addition, these few remaining e-purse solutions are generally not interoperable regardless of the market in which they operate. Only one system, the German GeldKarte that operates in the border area of Germany and Luxemburg (See Figure 2), is known to be used in multiple national jurisdictions. Furthermore, e-purses usually have a limited storing capacity for funds (e.g. the German GeldKarte has a load limit of EUR 200).

Figure 2

Mobile Payments

Mobile payments refer generally to the use of mobile phones and other wireless communications devices to pay for goods and services. Payments are initiated from a mobile communications device using voice access, text messaging protocols (such as short/single messaging service or SMS), or wireless application protocols (WAPs) that allow the device to access the Internet. Authorization often occurs by keying in a unique personal identification number (PIN) associated with the customer or mobile device. Adoption of mobile payments varies from country to country. Use of mobile phones as a means to initiate payments is relatively widespread in Southeast Asia and in some European countries.[17]

Most mobile payment services simply use the phone as an access device to initiate and authenticate transactions from existing bank accounts or payment cards.[18] This is the equivalent of using the Internet to initiate a direct debit or credit transfer from a bank account, or a credit or debit card transaction. This is an extension of traditional payment methods.

New mobile payments: Where mobile payment services are not based on an underlying bank or payment card account, the telecom operator typically acts as a payment intermediary to authorize, clear, and settle the payment.[19] Telecom companies engaged in these activities may not be overseen by a country's central bank or other banking regulator but may be subject to AML/CFT measures.

The telecom operator may either allow the phone owner to charge certain transactions to the phone bill (post-paid) or may permit the phone owner to fund an account held by the telecom operator or other service provider for the purposes of making payments (prepaid). Prepaid mobile payments accounts operate in the same manner

[17] See CPSS, "Policy issues for central banks in retail payments," BIS, CPSS #52, March 2003, at http://www.bis.org/publ/cpss52.htm.

[18] See CPSS, "Survey of developments in electronic money and internet and mobile payments," BIS, CPSS #62, March 2004, at http://www.bis.org/publ/cpss62.htm.

[19] Telecom companies offering mobile payment services provide for the settlement of the payment transactions completed via their systems through normal banking channels.

as a prepaid card or an electronic purse. When the phone is used in the same manner as a prepaid card, the phone owner uses the phone as a payment system access device to authorize the deduction of value from the prepaid account. When the phone functions as an e-purse, the prepaid value is stored on the subscriber identify module or SIM card within the mobile phone.

Post-paid and prepaid card-like mobile payments are much more common than e-purse mobile payments. In the case of prepaid mobile payments, telecom providers often offer this service in conjunction with a bank. For example, in the Philippines two telecom companies offer mobile payment services, Globe Telecom and Smart Communications. Smart Communications' Smart Money is co-branded with Banco de Oro. The transactions and funds transfers Smart Money users initiate via their mobile phone are authorized against a prepaid account held at Banco de Oro. Smart Money users can also send cross-border remittances by providing relatives with a MasterCard-branded prepaid card linked to the Smart Money account that can be used to withdraw cash from an ATM.

Globe Telecom serves as the intermediary for funds transfers using G-cash and operates without a bank partner. As a result, Globe customers cannot withdraw funds from their prepaid accounts at ATMs but only over the counter at participating businesses. Figure 3 illustrates a G-Cash funds transfer from one Globe Telecom subscriber to another using SMS. Both G-Cash and Smart Money are subject to AML/CFT regulations (including suspicious transaction reporting) and supervision.

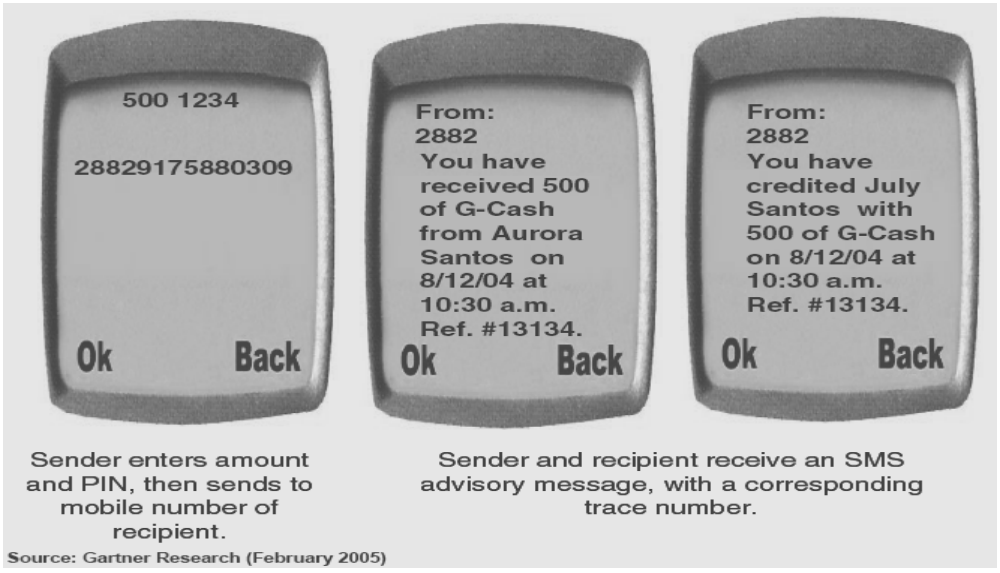


Figure 3 G-Cash Phone-to-Phone Remittance

Internet payment services

The expression "Internet payment services" is generally used to address: (i) payment services that rely on a bank account and use the Internet as a means of moving funds to or from a bank account; and (ii) payment services provided by non-bank institutions operating exclusively on the Internet and that are only indirectly associated with a bank account.

In the former case, Internet payment services refer to traditional payment methods where the Internet is only an innovative channel to exchange the information that is needed to move the funds from one account to another, which allows customers to access their bank accounts from home, 24 hours a day.

Where Internet payment services do not rely directly on a bank account, such as PayPal, individuals can transfer funds, shop online, or participate in online auctions, using a pre-funded account; however, the payment service provider may not be subject to the same AML/CFT measures that apply to banks. The service provider usually

will not have a face-to-face relationship with its customers. Depending upon the accessibility of the Internet payment service, these activities can involve payments or funds transfers across national borders.

Some non-bank Internet payment services allow customers to hold accounts with the payment service provider, while others offer only to send or receive individual payments using the customer's existing bank or credit card account. When non-bank Internet payment services offer customer accounts they may pool those customer funds in a single account at a bank. The account may be held in the name of the service provider. In that case, the bank holding the service provider's account may have no direct relationship with the service provider's individual customers.

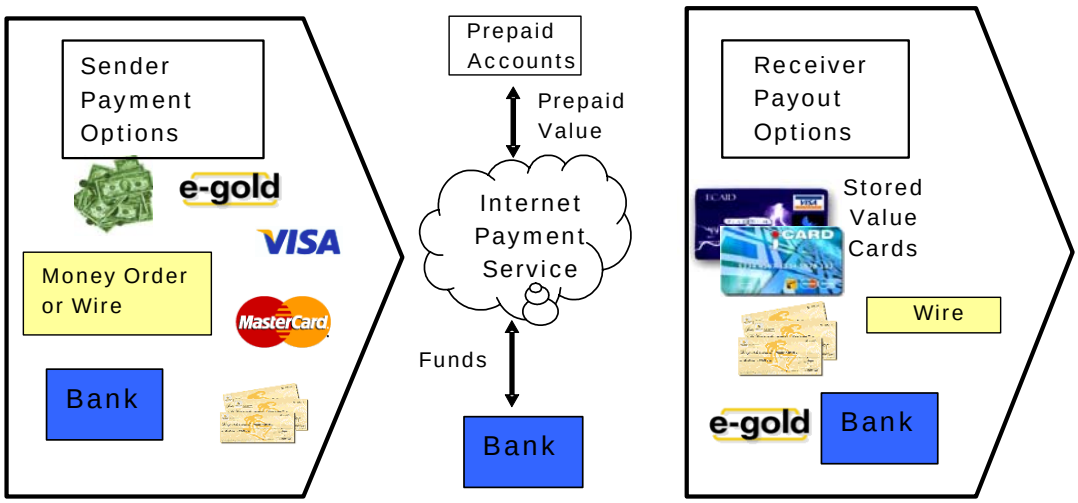


Figure 4

While a limited number of similar products exist in certain countries, PayPal appears to be the most widely used non-bank, Internet-based NPM. PayPal primarily functions as a payments intermediary for individuals and organizations that wish to trade with each other or transfer funds via the Internet. PayPal operates by allowing an individual to set up a pre-paid account in his name with PayPal that can be funded from a credit or debit card or a bank account via a credit transfer. Using those pre-paid funds, individuals can buy items or transfer funds to other PayPal account holders. The payment or transfer of funds occurs as a book-entry transaction between the PayPal accounts. When an individual wishes to access the funds in his PayPal account, he directs PayPal to credit his credit or debit card or bank account via a credit transfer or even a paper check.

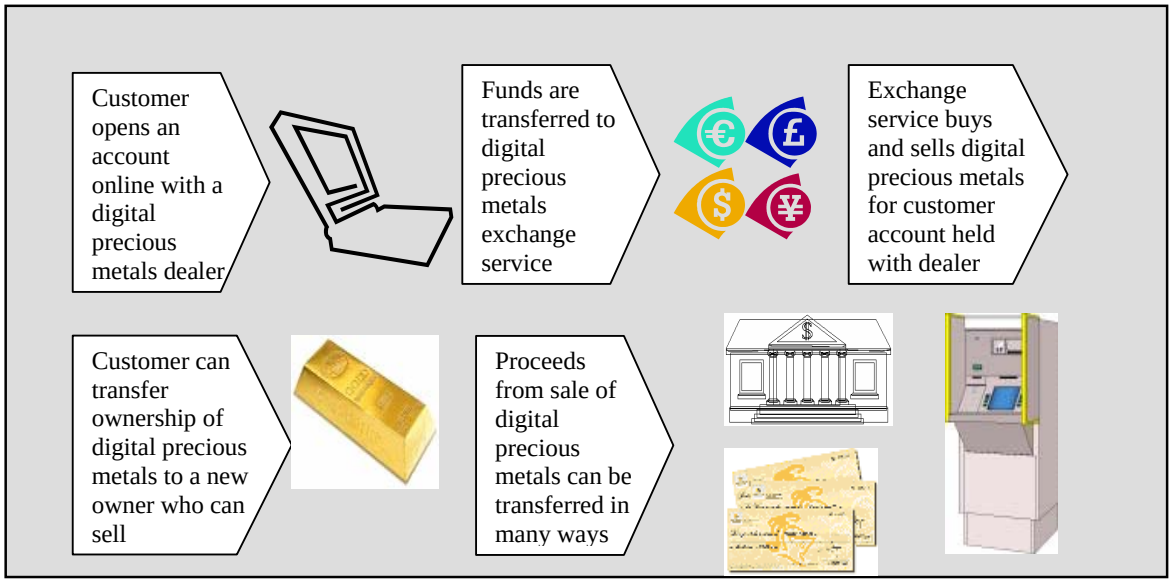
Service providers will differ as to the methods of payment they will accept to initiate a funds transfer, and the methods of payment they will use to distribute funds to the recipient. Figure 4 above illustrates how an individual can use a bank-issued credit card or other traditional payment methods to fund an Internet-based transaction account and subsequently make purchases or transfer all or a portion of the prepaid value to another account holder via book-entry by the service provider. The recipient can then use those funds to conduct additional transactions or withdraw the money via a traditional retail payment method. Online money transfer services set their own terms as what form of payment they will accept from senders and what forms of payment they make available to receivers.

Digital precious metals[20]

Digital precious metals are a relatively new online MVT system that involves the exchange of options or the right to purchase an amount of precious metals at a specific price. These derivatives can be exchanged, like traditional commodity or securities derivatives, between account holders in a digital precious metal service. Consumers purchase a quantity of virtual precious metal holdings based on the current price of the metal on the world commodity exchanges. Once a purchaser has acquired a quantity of the virtual precious metal, those holdings or a portion of them can be transferred either to another individual or a merchant in exchange for goods and services.

The oldest and best known of the digital precious metals dealers is e-gold Ltd., which claims to have almost 2 million accounts.[21] According to e-gold and other digital precious metals dealers, the rationale for using this store of value is to facilitate online transactions without regard for underlying currencies or access to foreign exchange. Transactions involving digital precious metals have immediate finality, which may appeal to online merchants that must pay high credit card interchange fees due to high fraud rates. Some digital precious metals dealers also allow users to maintain anonymous accounts. These traits are concerning to U.S. federal law enforcement agencies.

The transaction process associated with transferring the virtual holdings of precious metals between account holders can involve two separate service providers: the digital precious metals dealer, which maintains the accounts that contain the virtual holdings of precious metals; and the digital precious metals exchange service, which can act as a broker for the digital precious metals that the dealers buy or sell. Some dealers transact directly with account holders. Upon completion of a transaction, the selling account holder transfers ownership of his virtual precious metal holdings to the purchaser and can receive the proceeds of the sale through a variety of traditional and non-traditional payment methods (See Figure 5).



[20] The issuers of digital precious metals use the term "digital currency" to describe the barter arrangement they facilitate. Because of the potential confusion this common industry term would create with the term "e-purse" and "e-money", we have adopted the term "digital precious metals" for this report.

[21] E-dinar is a spin-off of e-gold and is affiliated with the Islamic Mint, a private organization working to revive the gold and silver currencies described in the Koran, the gold dinar and silver dirham. See: www.e-dinar.com.

Figure 5 Buying and selling digital precious metals typically involves working with two separate service provider categories: the digital precious metals exchange service and the digital precious metals dealer.

3. NPM Risk Assessment, Typologies, and Case Studies

The potential ML/TF risks posed by an NPM can vary from one service provider to another where there is no applicable AML/CFT law or regulation that establishes a uniform standard. To define high and low ML/TF risk characteristics of NPM operations, the project team developed a risk evaluation matrix (Table 1). The matrix identifies the essential risk criteria, applies those criteria to cash, representing the extreme high risk example, and provides generic NPM high and low risk scenarios.[22] Each NPM then is evaluated individually against the ML/TF risk criteria and wherever possible case studies and typologies are presented. The individual NPM risk assessments are summarized in Table 2.

To assess an NPM's ML/TF risk accurately, all of the risk factors have to be weighed in relation to the needs of the target market and applicable risk mitigating laws, regulations, and industry rules and practices. Taking all these factors into account, a particular NPM can be effective for all legitimate purposes while rendered ineffective or at least inconvenient for illegitimate purposes [23]

Few countries have identified criminal cases or typologies indicating ML or TF directly related to new payment methods. While this appears to indicate that NPMs are little used by criminals or terrorists, it may also indicate a more limited awareness of these NPMs within the AML/CFT community. The following typologies, therefore, should not be considered exclusive to any jurisdiction.

Payment Method Risk Factors			
Criteria	Cash	NPM High Risk	NPM Low Risk
Identification	Anonymous	Anonymous accounts with no identification or verification requirements	Payment methods that conduct verification of full customer identification
Value Limits	No limit	Any anonymous payment method without funding or transfer limits	Specific limits are placed on funding and transaction values[24]
Methods of Funding	Anonymous, no intermediary, no transaction record	Using an anonymous funding source (e.g. cash or money orders) to fund or receive funds from an NPM account that also can be used anonymously to	Using funding, pay out and value transfer methods that require verification of customer identification and maintain transaction records for each value transfer.

[22] Physical cash is often the ideal method of value transfer for criminal activity because it is anonymous, untraceable, requires no intermediary, is widely accepted, and provides for immediate settlement. The money laundering (ML) or terrorist financing (TF) risks posed by the new payment methods discussed in this report can be measured by how closely these alternatives match the attributes of cash. The main problem with cash for money launderers is its bulk, which creates difficulty moving the currency across borders. Criminals turning to cash alternatives, including NPMs, can eliminate the problem of moving large quantities of currency, but may encounter other limitations.

[23] In practice, no single category of the ML/TF risk criteria determines the relative ML/TF risk of a particular NPM. In addition to evaluating the NPMs considered in this report, the risk matrix presented may provide a useful framework for analyzing the level of risk associated with other payment systems or commercial activities.

[24] Account limits may not be necessary when full customer identification is verified and a transaction record is maintained, otherwise limits may be appropriate

		transfer value to an anonymous recipient	
Geographical Limits	Some currencies are accepted more widely than others	Payment methods that can be used to send and/or receive funds across national borders	Payment methods that can only be used to send and/or receive funds domestically
Usage Limits	No limit	Payment tool can only be used to access cash or can be exchanged for cash	Payment tool can only be used to acquire goods and/or services

Table 2

Prepaid Cards: Open System

Identification. Open-system prepaid cards may be used to support anonymous cross-border funds transfer (See Figure 6). When cards are issued without a bank account and applications are accepted online, via fax, or over the counter at retailers and check cashing outlets, insufficient customer due diligence in the application process may increase the potential ML/TF risk. This risk may be mitigated by account and transaction limits. Some service providers tier the customer identification process to the value held in the account and the frequency or value of account activity. Although prepaid cards have a unique account number and create an electronic transaction record, without adequate cardholder identification the transaction trail alone may be insufficient to help law enforcement trace the cardholder. Depending on the jurisdiction, offshore card issuers may pose additional ML/TF risks.

Value limits. Open-system prepaid card programs often target distinct market segments (e.g. children; teenagers away from home; adults without a bank account; and adults unable to qualify for a credit card). Each market segment may have distinct needs, which may be reflected in the funding and value limits which are set by the card-issuing bank. These limits include how much value can be held in a card account, how much can be prepaid at one time, and how often value can be added or withdrawn. The more money that can be moved through a card account, either at one time or through a series of ATM transfers, the greater the risk, relative to the other risk criteria.

Method of funding. Prepaid cards draw on a prepaid account that can be funded in a variety of ways. The card-issuing bank and its partners determine how card accounts can be funded. Some methods, such as credit transfers from a bank account or credit card, involve payment sources that: (i) independently verify the identity of the prepaid cardholder; (ii) will maintain a record of the funds transfer to the prepaid card; and, (iii) will usually have AML policies and procedures that include monitoring transactions for suspicious activity. Other methods of account funding, such as cash and money orders, are anonymous and leave no paper trail, increasing the potential ML/TF risk independent of the other risk criteria.

Geographic limits. Open-system prepaid cards that have the capability to provide access to cash at automated teller machines (ATMs) increase the potential ML/TF risk independent of the other risk criteria and risk mitigation. Access to cash through the ATM networks, however, usually requires the use of a personal identification number (PIN) that must be pre-set with the issuing institution. The requirement of the PIN may not, however, provide sufficient information within the transaction record to identify with full certainty the recipient.

Usage limits. Open-system prepaid cards can have usage limits. Physical cards may be limited to point-of-sale (POS) networks, allowing only the purchase of goods and services and barring access to cash via ATMs. Virtual cards provide the cardholder only an account number to be used for online and telephone transactions; there is no physical card to access cash via ATMs. However, most open-system prepaid cards are physical cards and facilitate access to POS and ATM networks. In some countries, physical cards may also be used to withdraw cash at retailers whereby an amount higher than the price of goods purchased is paid to the retailer and the difference between the price of the goods and the amount paid is given in cash to the cardholder. For the reasons

discussed previously, cards that can provide access to cash via ATMs on a global basis may increase the potential ML/TF risk independent of other risk criteria and risk mitigation.

Typology. The transfer of illicit proceeds from one country to another using debit cards associated with personal bank accounts and the ATM networks is an established method of ML. Instances of ML have been identified as having occurred even when a customer identification program is in place at the time the bank account is opened. This can occur when a customer uses false identification documents. Some open-system prepaid cards offer similar ATM access without requiring the cardholder to open a bank account or verify identification, creating the potential for greater use of this typology.

Case Studies.

A. In 2001, a suspicious activity report (SAR) filed in the United States detailed the acquisition of more than 300 prepaid cards by a single individual who used them to transfer almost $2 million to Colombia. No further information is available to the public.

B. In 2001, the El Dorado Task Force[25] in New York, identified a significant trend in the number of individuals who appeared to be using ATMs as a means of laundering money through cash withdrawals in foreign countries. Analysis identified more than fifty SARs involving the structured deposit of cash into New York area accounts with subsequent ATM withdrawals in Colombia, Mexico, Peru, Ecuador, and Panama. A similar study conducted by the Financial Crimes Enforcement Network (FinCEN, the U.S. financial intelligence unit) over a four-year period found the most common withdrawal locations were Colombia, Venezuela, Mexico, Argentina, and Brazil. In almost all of the SARs, the banks described the suspected violation as ML-related.

C. In 2004, German tax investigators discovered a case of ML through prepaid cards. Two participants of a criminal fraud/embezzlement scheme had transferred parts of their shares of the criminal proceeds onto several prepaid cards. They used the funds on the cards for cash withdrawals (domestic only, not in foreign countries) and payments for goods. The card accounts were kept only for short periods (6 – 24 months) after which they were closed again and new ones were opened. In this case more than 350.000 EURO were hidden and laundered this way.

[25] Created in 1992 to target money laundering in New York, the El Dorado Task Force became one of the nation's most successful money laundering task forces. It is led by the Immigration and Customs Enforcement federal law enforcement agency and includes representatives from 29 federal, state, and local law enforcement agencies.

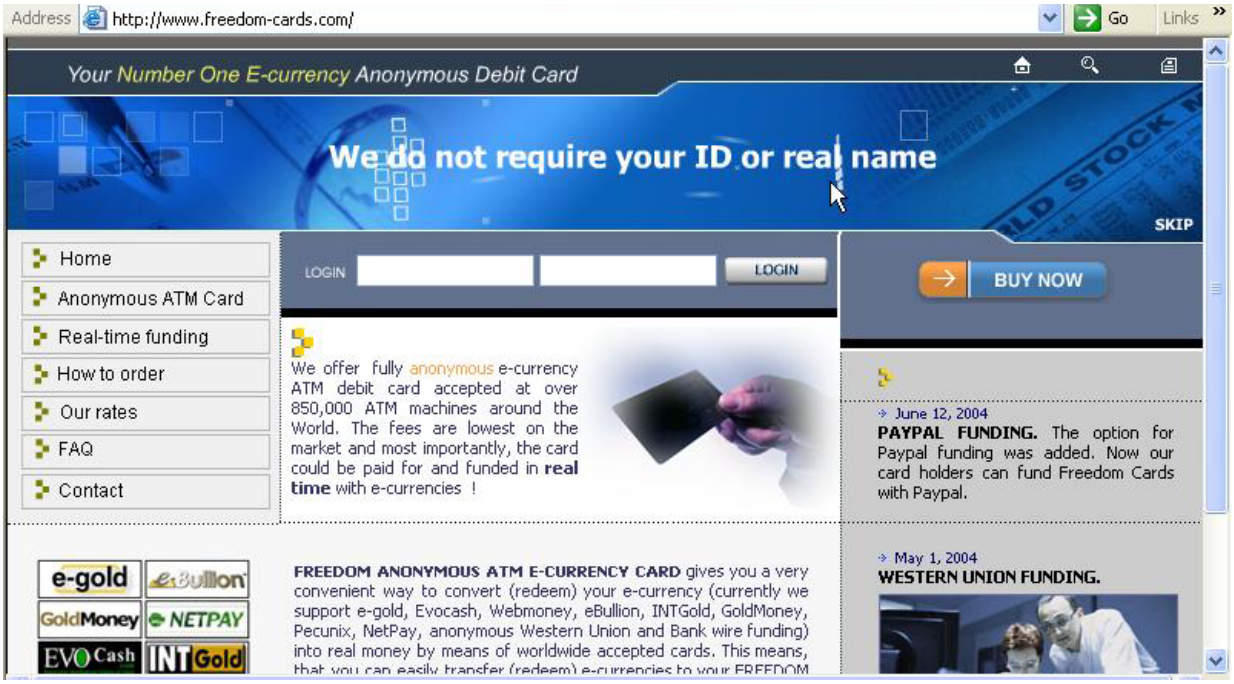


Figure 6

Prepaid Cards: Closed System

Identification. Anonymous, closed-system prepaid cards may be resold for cash, which could facilitate ML and TF. This risk, however, is mitigated by the demand for the goods and services that can be purchased with the card as well as the geographic scope of a card's acceptance.

Value limits. A high-value, closed system prepaid card that can be resold may be a convenient substitute for cash when moving value across borders. The higher the value limit on a closed system prepaid card the greater the potential ML/TF risk, independent of other risk criteria and risk mitigation.

Method of funding. As with open-system prepaid cards, closed-system cards draw on a prepaid account that can be funded in a variety of ways determined by the merchant selling the card.

Geographic limits. The resale potential of a closed-system prepaid card depends upon the availability of resale markets and the level of demand for the card. The greater the geographic scope in which the card is accepted, the greater the potential ability to resell it, which may increase its potential use as an ML/TF tool.

Usage limits. Closed-system stored value cards are by definition limited in their potential usage. Generally, these cards can only be used to buy goods and services sold by the card issuer. As noted above, the greater the availability of resale markets and the level of demand for the card, its potential ML/TF use may be increased. Unlike open-system prepaid cards, closed-system cards cannot be used to access cash via ATMs, although they can potentially be resold for cash and can be purchased for cash.

Typology. The wholesale distribution of prepaid long distance calling cards is, according to the U.S. Federal Bureau of Investigation, a $4 billion a year cash-intensive industry that can provide cover for ML. At the retail level, closed-system prepaid cards can potentially be purchased anonymously in large quantities for cash,

transported across borders, and resold. Unlike currency, the value held on prepaid cards is not apparent to customs and border officials, although the quantity of cards may be.

Case Studies.

A. In 2001, FinCEN reported that more than 160 Suspicious Activity Reports were filed on telephone card businesses with dollar amounts that ranged between $300,000 and $50 million.[26] The FBI reported in 2005 that a review of the Suspicious Activity Report database revealed that financial institutions are increasingly reporting suspicious activity related to the prepaid calling card industry.

B. In 2005, U.S. Immigration and Custom Enforcement initiated an investigation into an employee of a state agency in Ohio selling fraudulent drivers' licenses and identification cards in exchange for prepaid telephone cards.[27]

Electronic Purse

Identification. A cardholder with an electronic purse linked to a bank account is identified through the account-opening process. There are other chip card programs, however, not linked to a bank account, which may not require customer identification and provide no transaction record. Independent of other risk factors and risk mitigation methods, insufficient customer identification may increase the potential ML and TF risk.

Value limits. Although chip card technology does not prohibit electronic purses from holding unlimited value, current card programs are generally used for small value transactions and therefore tend to have low value limits. Germany's *GeldKarte*, for example, has a value limit of €200.

Method of funding and receipt of funds. Electronic purses linked to a bank account can only have funds added through the account. Some e-purse programs also allow for card-to-card value transfers. An e-purse that is not linked to a bank account may have the ability to add value via cash. Independent of any risk mitigation methods, a card with a high value limit, anonymous card-to-card transfers, and cash as an option for loading and withdrawing value could pose a significant ML and TF risk.

Geographic limits. The lack of significant cross-border capability associated with any electronic purse program significantly reduces the ML/TF risk posed by these payment tools.

Usage limits and receipt of funds. Electronic purses generally are limited to small value retail transactions, although some programs do allow for card-to-card and card-to-cash functionality.

Typology. There are no observed ML/TF typologies associated with the current use of electronic purses.

Case Studies. There are no observed ML/TF cases associated with current use of electronic purses.

Mobile Payments

Identification. Most mobile payment systems use the mobile phone as a device to access a bank account or credit card. These systems establish customer identification when the underlying bank or credit card account is opened. A similar customer identification process takes place when a telecommunications service provider,

---

[26] Department of the Treasury, FinCEN, SAR Bulletin, June 2001.

[27] U.S. Immigration and Customs Enforcement, News Release, Ice Arrests 9 in Ohio Fraud Driver's License Scheme, available at: http://ice.gov/graphics/new/newsreleases/articles/drivers022405.htm.

rather than a financial institution, holds the mobile payment account and extends credit to the account holder. If mobile phone service is prepaid and the funds used to facilitate mobile payments are also prepaid, the service provider may not be motivated to fully identify customers because of the absence of credit risk.

Value limits. Where mobile phones are access devices to underlying bank and credit card accounts, limits may not be necessary. In the Philippines, Globe Telecommunication requires prepayment for transactions through its G-Cash mobile payment program and imposes a maximum per transaction of 10,000 pesos ($182, €145), a maximum per day of 40,000 pesos ($728, €580), and a maximum transfer per month of 100,000 pesos ($1,825, €1455).

Method of funding. Mobile payment programs that draw on a prepaid account can be funded in a variety of ways. Payment sources that have independently verified the identity the phone owner and that maintain a record of the funds transfer to the mobile payment account present a low risk. The use of cash to fund a mobile payment account, independent of other risk factors or risk mitigation strategies, may present some limited ML/TF risk.

Geographic limits. Mobile payment systems currently do not facilitate cross-border transactions due to incompatible systems. An attempted joint venture (SIMPAY) of several European telecommunications service providers failed in 2006.

Usage limits. Payments can only be received by a participating merchant or fellow service subscriber.

Typology. There are no observed ML/TF typologies associated with the current use of mobile payment systems.

Case Studies. There are no observed ML/TF case studies associated with the current use of mobile payments systems.

Internet Payment Systems

Identification. Internet payment systems may permit anonymous accounts.

Value limits. Individual service providers usually determine the limits on account or transaction value, which affects the relative ML/TF risk.

Method of funding. Internet payment systems set their own terms regarding what methods of payment they will accept to fund accounts and how funds transfers are paid out to recipients. Service providers accepting cash and money orders or transfers from anonymous prepaid cards may present a greater ML/TF risk than service providers that limit funding sources to a bank account or credit card.

Geographic limits. Offshore Internet payment systems may facilitate transactions that are illegal in the payer's home jurisdiction. The online payment service acts as an intermediary, receiving funds that are passed on to a final recipient. In some cases, where direct funds transfers to the final recipient would be blocked under a jurisdiction's domestic laws, the payer can transfer the funds through an offshore online payment system operating under a different regulatory regime

Usage limits. Individual service providers determine the usage limits for the service.

Typology. Internet payment systems offer the potential for anonymous cross-border funds transfers. The risk is greatest when the service provider operates offshore in a jurisdiction with a weak anti-money laundering and counter TF regime. Even when customer due diligence is undertaken, where the customer relationship exists entirely online, the extent to which service providers attempt to verify customer identification determines the ML/TF risk relative to the other risk criteria and risk mitigation efforts.

Case Studies. There are no observed ML/TF cases associated with current use of Internet payment systems.

Digital Precious Metals

Identification. Digital precious metals dealers may permit anonymous accounts.

Value limits. There may be no value limits on digital precious metals accounts other than the amount of funds that can be placed into the online account through the use of traditional or non-traditional payments systems.

Method of funding. Each service provider sets its own terms as to what methods of payment it will accept. The serve provider's ability to accept any specific method of payment will also be limited by the willingness of the providers of these other payment services to offer digital precious metals brokers or dealers access to their services.

Geographic limits. Service providers may operate globally with no geographic limitations, although natural limits do exist based upon access to the Internet. Some governments, such as China and others, and may also place limits on the types of services to which they permit their citizens access. Web hosting and other Internet service providers may also place limits on the types of web sites and businesses they are willing to support.

Usage limits. Digital precious metals accounts may have no usage limits. Each service provider sets its own terms as to how it will disburse the funds, but its ability to do so also depends on the willingness of the providers of other payment services to offer precious metal brokers or dealers access to their services.

Typology. Digital precious metals offer the potential for anonymous cross-border funds transfers. The risk is greatest when the service provider operates offshore in a jurisdiction with a weak anti-money laundering and counter terrorist financing regime. Even when CDD is envisaged, where the customer relationship exists entirely online, the extent to which service providers attempt to verify customer identification determines the ML/TF risk relative to the other risk criteria and risk mitigation efforts.

Case Studies.

A. In March 2004, an Oklahoma man admitted to a financial fraud scheme involving an online investment fund. Thousands of people lost almost $9 million. According to the U.S. Federal Bureau of Investigation, the online investment scheme, E-Biz Ventures, laundered investor money through e-gold Ltd. The Oklahoma man who created this criminal enterprise may have been targeting tax evaders and other criminals because he "allegedly highlighted his reliance on e-gold to appeal to his victims' fear of the federal government and their desire for anonymity."[28]

B. In October 2004, the United States Secret Service shut down ShadowCrew.com, one of the largest illegal online centres for trafficking in stolen identities and payment cards. There were 21 arrests, and to date 12 of the defendants have pleaded guilty. ShadowCrew.com had approximately 4,000 members from all over the world dedicated to malicious computer hacking and the sale of stolen and counterfeit identification and credit and debit card numbers.[29] Those who pleaded guilty "acknowledged that ShadowCrew members sent and received payment for illicit merchandise and services via Western Union money transfers and digital currencies such as e-gold and Web Money."[30] One, "who used the nickname Voleur -- French for thief -- boasted in a chat room that he moved between $40,000 and $100,000 a week," was receiving Western Union money orders from accomplices, which, for a fee, he laundered through e-gold accounts.[31]

---

[28] Grow, Brian, Gold Rush, Business Week, January 9, 2006, accessed at: http://www.businessweek.com/magazine/content/06_02/b3966094.htm.

[29] http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm

[30] http://www.usdoj.gov/criminal/cybercrime/mantovaniPlea.htm

[31] Grow, Op. Cit.

C. Estonia reports a case involving the laundering of illicit proceeds from unauthorized bank account withdrawals through the use of digital precious metals. Account information was gathered through the use of fraudulent e-mails that claimed to be sent on behalf of the recipient's bank which sought to confirm the information. If the recipient responded with the account information, the criminals initiated unauthorized withdrawals. The money was laundered through a series of steps involving cross-border transactions via Western Union and Money Gram, and ultimately Web Money, a digital precious metals service.

Off-shore provision of NPMs

A potential risk factor that may be common across many types of NPMs is that of jurisdiction. In some cases, NPM issuers or service providers may be located in an offshore financial centre and therefore subject to a less robust system of laws and regulation. Additionally, processes related to NPMs often flow through multiple jurisdictions, which has the effect of making the product more complex. The involvement of multiple jurisdictions and resulting segmentation of various parts of the chain of transactions increases the difficulties of designing effective supervisory strategies for NPMs. When NPMs are provided over the Internet, the jurisdiction risk is increased due to the potential difficulties in identifying to which jurisdictions the service providers belong, where they are incorporated, which authorities are responsible for their supervision and what AML/CFT regime is applicable. In this case it becomes extremely complicated for any of the jurisdictions where the NPM is accessible to national customers to intervene and stop illegal activities that are taking place. International cooperation among authorities may be an essential tool to face these situations, especially where efficient and effective exchange of information systems are in place. In this regard, the Early Warning System proposed by Germany at the ASEM symposium which took place in Berlin at the end of 2003 and described in the box below, could represent a good example.

Germany's Proposal for an Early Warning System

Offshore card issuers and payment services, whether acting through an agent or via the Internet, do not always follow the law in the countries where they seek to do business. Germany introduced the „Early Warning and Information Sharing System" at the ASEM Symposium in Berlin in October 2003 to promote coordination and information sharing between jurisdictions in the context of Alternative Remittance Systems and Underground Banking. The ASEM[32] experts „agreed to nominate a point of contact from the competent law enforcement or supervising body or FIU in each ASEM country in order to promote coordination including exchange of information and, when possible, joint action between relevant domestic and foreign authorities to deter illegal activities or abuse. Experts from ASEM countries agreed that this kind of early warning system would help to disrupt illegal international transactions simultaneously in all affected countries and would enable law enforcement and supervisory authorities to take the necessary co-ordinated action within their own jurisdictions. The experts welcomed the involvement of other countries in this process."[33]

The Early Warning and Information Sharing System was later approved and joined by several FATF members to whom it was introduced during the FATF Seminar on TF in Paris in February 2004.

Although originally intended for fighting Underground Banking, the Early Warning System could also be a very effective tool for the fight against the abuse of new payment systems. These NPM, especially those making use of the Internet, have an international structure very much like Underground Banking Networks. New payment methods can be used to transfer funds worldwide. The Early Warning System therefore is a very useful and effective tool to not only take co-ordinated actions against the abuse of such NPM but also to raise awareness of such abuse not only in singular jurisdictions, but worldwide.

---

[32] The acronym ASEM stands for Asia-Europe Meeting, an informal forum for dialogue between European and Asian jurisdictions. For more information on ASEM and its members see www.aseminfoboard.org

[33] Final conclusions of the Berlin Symposium on Alternative Remittance Services and Underground Banking 30-31 October 2003, sec. IV.

NPM Money Laundering and Terrorist Financing Risks

Payment Method	Potential Risk Factors	Current and Potential Risk Mitigants
Prepaid cards: open-system	• Anonymous card holder • Anonymous funding (inflow) and anonymous access to funds (outflow) • High card value limit and/or no limit on the number of cards an individual can acquire • Access to cash globally through ATMs • Offshore issuers may not observe laws in all jurisdictions	• Verify cardholder identification • Limit funding options • Limit card value and/or the number of cards that an individual can acquire and/or value per transaction • Limit cross-border access to cash • Monitor transactions and report suspicious activity • Implement a card/account block • Limit access to network by undesirable merchants and ATM providers/networks
Prepaid cards: closed system	• Anonymous card holder • Anonymous funding • High card value limit • Substitute for bulk cash smuggling • No limit on the number of cards an individual may purchase	• Verify cardholder identification • Limit card value and/or the number of cards any one purchaser may acquire • Limit funding options • Monitor transactions and report suspicious activity • No direct cash access via ATM • Implement a card/account block
Electronic Purse	• Anonymous card holder • Anonymous funding and receipt of funds • High card value limit • No transaction record	• Verify cardholder identification • No card-to-card transfer capability • Limits on the amounts that can be spent/stored • Limited cross-border functionality • Limit funding options • Monitor transactions and report suspicious activity • Implement a card/account block
Mobile payments	• Anonymous accounts • Anonymous funding and receipt of funds • High or nonexistent account funding limit	• Account holders are identified when phones are used as an access device to a bank or credit card account or when the telecom verifies phone owner identification • Limited cross-border functionality • Limited account and transaction value • Limit funding options • Monitor transactions and report suspicious activity • Implement a card/account block • Limit access to network
Digital precious metals	• Anonymous accounts • Anonymous funding and receipt of funds • High or nonexistent account funding limit • Offshore service providers may not observe laws in other jurisdictions	• Identify account holder • Maintain transaction record with payer and recipient • Monitor transactions and report suspicious activity • Limit funding options • Implement account block • Limit access to service
Internet payment systems	• Anonymous accounts • Anonymous funding and receipt of funds (ATM) • High or nonexistent account funding limit • Offshore service providers may not observe laws in other jurisdictions	• Identify account holder • Maintain transaction record identifying payer and recipient • Monitor transactions and report suspicious activity • Limit funding options • Implement account block • Limit access to the service

Table 3

5. Application of FATF Recommendations and Special Recommendations; and Selected Regulatory Approaches[34]

The FATF 40 Recommendations and nine Special Recommendations highlight potential ML and TF risks associated with new payment methods and provide guidance for regulating domestic service providers.

Recommendation Five addresses anonymous accounts, which is the principal ML/TF vulnerability identified in the new payment methods analyzed in this report. Recommendation five states: "Financial institutions[35] should not keep anonymous accounts or accounts in obviously fictitious names."

Recommendation Eight specifically addresses the ML/TF risks that may be associated with new payment methods: "Financial institutions should pay special attention to any ML threats that may arise from developing technologies that may favour anonymity, and take measures, if needed, to prevent their use in ML schemes."

Recommendation 23 underscores the need for all providers of financial services to be subject to adequate regulation and supervision. With regard to the broad category of money or value transfer services, Recommendation 23 states: "At a minimum, businesses providing a service of money or value transfer, or money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat ML and TF."

Special Recommendation VI amplifies Recommendation 23, stating in part: "Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions."

Special Recommendation VII specifies the information that should accompany domestic and cross-border wire transfers, but allows wide latitude in how financial institutions and jurisdictions may interpret and react to the completeness of the wire transfer information received.

Recommendation 21 signals the potential need to close off "business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations."

The FATF Glossary includes among the activities that are performed by financial institutions as a business for or on behalf of their customers "issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)".

Regulatory Approaches

Determining either the volume or nature of transactions that use the new payment methods described in this report is difficult because few countries appear to be either aware of these payment tools or to be monitoring their use. The Bank for International Settlements (BIS) notes: "With technology facilitating the breakdown of traditional banking services into multiple components and the addition of analytical tools and other capabilities into traditional banking services, more unlicensed non-bank entities are likely to provide bank-like services via the

[34] The regulatory approaches mentioned in this section have been verified with the jurisdictions concerned. Some measures were not adopted specifically for anti-money laundering purposes but rather by financial supervisors or monetary authorities to protect other financial interests.

[35] The term "financial institutions" refers to service providers that transfer money or value in both the formal and informal sectors.

Internet, including those that are extended cross-border. Differences in definitions as to what constitute a "bank" among jurisdictions would likely be magnified and will increasingly challenge how bank supervisors deal with financial entities with no home supervision."[36] The BIS notes: "Over time some technology companies offering "e-banking-like" services might relocate into jurisdictions where their specific mix of products and services does not require a banking license just as offshore centres developed previously."[37]

"The trend toward a broader range of service providers and to greater networking in end-user markets has raised some regulatory questions. The regulatory approaches taken by different countries to the overall efficiency, risk and consumer concerns associated with new payment instruments, providers and market arrangements have differed somewhat. In some European countries a response to the challenge has been to limit the provision of some payments services to financial institutions. In other countries the provision of payment instruments and services has not been restricted."[38]

Germany's Regulatory Provisions With Regard to Prepaid Cards

In a prepaid card scheme, German financial supervisory authorities focus on the card issuer (mainly banks) and the card broker (the intermediary service provider between the bank and the cardholder). By acting as an agent to arrange customer relationships between the card issuer and a customer/cardholder, a card broker is considered to be conducting deposit brokering. This is because, in Germany, taking in funds to issue a prepaid card is considered to be the same as taking in deposits. As a consequence, a full banking license is required to issue prepaid cards. The card issuer is considered as a credit institution and therefore subject to full AML compliance including customer identification.

As regards those prepaid card schemes where the card issuer is located abroad, the card issuer may rely on an intermediary service provider (so-called "card-broker) to promote the card in the targeted market. By acting as an agent to arrange customer relationships between the card issuer and a customer/cardholder, a card broker is considered to be conducting "deposit brokering". This business type of deposit brokering does not require a license if the deposit taker (in this case the card issuer) is domiciled within the European Economic Area.

If however a card broker is acting as an agent for a card issuer domiciled outside the European Economic Area, the card broker is considered a financial services institution and is required to be licensed. As a financial services institution, a card broker is subject to full AML compliance including customer identification.

The EU Regime for e-money

In the EU, there are currently two pieces of legislation which regulate e-money: Directives 2000/46/EC[39] (the e-money institutions Directive)[40] and 2005/60/EC (third money laundering Directive); the latter shall be transposed by Member States into national legislation by December 2007.

Whilst it is widely accepted that the definition of e-money covers prepaid cards, e-purses and internet payments such as PayPal, there is some controversy as to whether pre-paid mobile payments are covered. In the whole EU, there are only 6 "purebred" e-money issuers, as the majority of entities issuing e-money are banks conducting other banking business as well.

---

[36] Management and Supervision of Cross-Border Electronic Banking Activities, Bank For International Settlements, July 2003. Accessed at: http://www.bis.org/publ/bcbs99.pdf

[37] Ibid.

[38] CPSS #33

[39] Official Journal L275, 27/10/2000

[40] Official Journal L 309, 26/10/2005

Following the flexibility provided for by the Directive on e-money institutions as regards the application of AML/CFT provisions, EU Member States (MS) currently apply different regimes to e-money: a majority of MS applies the same AML/CFT provisions as for banks, some apply a lighter regime but the situation is expected to change after the third Money Laundering Directive is transposed by MS in their national legislation.

In particular, the third AML Directive gives the possibility to EU MS to allow e-money issuers not to apply customer due diligence in respect of e-money, where, if the device cannot be re-charged, the maximum amount stored in the device is no more than EUR 150 or where, if the device can be recharged, a limit of EUR 2500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1000 or more is redeemed in that same calendar year by the bearer.

Simplified CDD applies to other products or transactions carrying a low risk of ML or TF, in accordance with technical criteria identified to help assess whether situations represent a high or a low risk of ML or TF.

Notwithstanding the technical criteria identified, simplified CDD shall not apply in the case where there is information available that suggests a product is subject to a high risk of being misused for ML or TF purposes.

Regulating Internet Payments, and Other New Payment Systems, in the United States

The comprehensive AML/CFT regime in the United States requires "financial institutions" (as defined in the Bank Secrecy Act and in implementing regulations) to, among other things, establish and maintain anti-money laundering programs, file cash transaction, suspicious activity and other reports, perform CDD, and obtain and retain records regarding customer identification and verification. Within this framework, non-depository financial institutions that provide payment services tend to belong to some category of "money services businesses" (MSBs). MSBs are defined to include five distinct types of financial services providers: currency dealers or exchangers; check cashers; issuers of traveller's checks, money orders, or stored value; sellers or redeemers of traveller's checks, money orders, or stored value; and money transmitters. The five types of financial services are complementary and are often provided together at a common location. Money services businesses have grown to provide a set of financial products that one would traditionally look to banks to provide.

As noted above, money transmitters and issuers, sellers or redeemers of "stored value" are MSBs subject to the US AML/CFT regime, which requires certain MSBs to register with FinCEN (the FIU), as well as to establish an AML programs and to comply with various reporting and recordkeeping requirements. Many types of MSBs also are required to be licensed on the state level. Whether a particular online payment service, stored value provider, digital precious metals service or other value-service provider or payment system or digital currency service meets the definition of an MSB under the regulations is a fact-specific determination. That determination is dependent upon such factors as the structure, location, operations and services of the particular business. If the service or business is found to be an MSB under these regulations, then it would be subject to all of the programmatic, reporting and record-keeping requirements described here. Many payment systems, particularly online payment system providers, are based outside the United States and are not subject to U.S. jurisdiction. U.S. federal banking agencies, FinCEN, and others also routinely provide guidance to depository institutions regarding potential risks associated with non-bank payment service providers and available means to mitigate those risks.[41]

[41] For example, sections of the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual relating to electronic cash, prepaid products and third-party payment processors were updated in July 2006 to outline risk factors in these products and to recommend steps that depository institutions should take to mitigate those risks.

Use of "Special Measures" in the United States

The United States can take action against an NPM based outside the country that poses a ML threat to the U.S.[42] In the United States, the Secretary of the Treasury is authorized – in consultation with the Department of Justice, the State Department, and the appropriate Federal financial regulators – to designate a foreign jurisdiction, institution, class of transactions, or type of account as being of primary ML concern.

There are a range of options available to target the specific ML concern most effectively. Through the imposition of various "special measures," the Treasury Secretary can gain more information about the jurisdictions, institutions, transactions, and accounts that are of concern, and take appropriate action to safeguard U.S. financial institutions.

The special measures available to the Secretary include requiring of domestic financial institutions: (1) Recordkeeping and reporting of certain financial transactions; (2) collection of information relating to beneficial ownership; (3) collection of information relating to certain payable-through accounts; (4) collection of information relating to certain correspondent accounts; and (5) prohibition or conditions on the opening or maintaining of correspondent or payable-through accounts.

India Forbids Use of Digital Precious Metals

In October 2002, India's central bank, the Reserve Bank of India, forbid the use of "e-gold" as violating national rules requiring only sovereign currencies be used in domestic transactions. The central bank stated in a news release: "An impression is sought to be created among the members of public by some agencies/persons that transactions involving e-gold, purportedly an electronic currency, are freely permitted in India and that e-gold has the status of a foreign currency… The Reserve Bank clarifies for the information of [the] public that 'e-gold' is not a currency of any sovereign state."[43]

Australia: Unlicensed Digital Precious Metals Sites

In 2004 the Australian Securities and Investments Commission (ASIC) identified several online digital precious metals dealers including some based outside the country as conducting business without a proper license: "Following an examination of electronic currency trading websites, ASIC became aware of three Australian-based businesses that were operating such sites or were acting as agents for similar businesses based overseas. These businesses exchanged conventional currencies to electronic currencies and vice-versa, and charged a commission for their services… ASIC believes that such products can be defined as non-cash payment systems and that people who deal in such products with Australian consumers must hold an Australian financial services licence (AFSL)." The identified businesses "all withdrew their websites and closed down their businesses voluntarily."[44]

6. NPM Questionnaire Results and Analysis

Objectives and methodology

This section gives an overview of the responses to the questionnaire issued by the project team to which there were 37 responses. Most respondents identified NPMs in their jurisdiction. In some countries, respondents have either not identified NPMs (e.g. Argentina, Cambodia and Slovenia) or have only provided information about

---

[42] Some online payment systems may be licensed in one country and maintain operations (including staff, computer systems, and customers) in various other countries without a physical retail presence anywhere.

[43] http://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx

[44] http://www.asic.gov.au/asic/asic_pub.nsf/byheadline/04-366+ASIC+acts+to+shut+down+electronic+currency+trading+websites?openDocument

traditional means of payment (e.g. Qatar, Latvia, Macao and Slovakia), or even traditional means of payment which can be accessed in new ways such as Internet banking (Azerbaijan). Some respondents privately indicated to the project team there were unsettled cases and investigations underway regarding NPMs, but that these cases could not be disclosed.

Summary findings from the questionnaires are presented below for each payment method with more detailed information presented in Appendix B in the following fields of information: NPM category, market size, regulation of access to activity, AML/CFT provisions and AML/CFT cases as well as the existence of illegal operators. Conclusions are provided at the end of this section as well as for each category of NPM.

Prepaid cards

Fourteen countries, approximately one-third of respondents, report the presence of prepaid cards, both closed-system and open-system cards are reported. With regard to open-system cards, ATM functionality is often present and sometimes allows transferring funds worldwide.

Little information was reported regarding market size, but where such information is available it often indicates a small or emerging market.

Most of the reported types of prepaid cards are submitted either to registration or licensing requirements or under supervision (exceptions are Palau and New-Zealand). The picture is mixed concerning AML/CFT provisions, as for less than half[45] of the countries, no AML/CFT provisions have to be applied (ex. USA and Czech Republic). It is interesting to note that all the payment methods which are not under CFT/AML regulation have a limit to the transferred amount.

Except for the USA and New-Zealand, no AML/CFT cases are reported. The same goes for illegal operators, but with no exceptions.

Payments initiated by means of a mobile phone (and linked to a bank-account)

Four countries reported mobile phones are used to access bank accounts (Korea, Finland, New-Zealand and China). As the payment method is based on bank accounts, registration/licensing apply, as well as supervision and AML/CFT provisions.

No AML/CFT cases or illegal operators are reported.

E-purse

Four countries (Belgium, Switzerland, Germany and the Netherlands) reported e-purses are issued in their jurisdiction. In all cases, e-purse issuers are required to be licensed and supervised and AML/CFT provisions apply. In all cases, there are limits to transferred amounts. There is no evidence of ML or examples of law enforcement actions in any of those countries.

Internet payments

This is the largest group of new payment methods, as they are reported by 15 out of 37 countries (40%). Systems differ per country; some of them (e.g. Paypal, Neteller) operate in several jurisdictions.

Most countries apply registration/licensing requirements and supervision or are working towards putting in place such regulations. Most countries also apply AML/ CFT provisions (sometimes even when registration/licensing/supervision are not applied).

Amongst countries where no AML/CFT provisions apply (NL, ES, CN), only CN has found evidence of ML/TF. Examples of law enforcement cases can be found in the USA, ET, and CA.

[45] "Half" is only correct when taking into account that Palau and New Zealand both indicate that even though they apply AML/CFT requirements, they have no registration or licensing requirements nor supervision.

One of the problems reported regarding this NPM is the possibility for payment service providers to offer their services offshore and therefore circumvent the destination country's registration/licensing rules as well as supervision and AML/CFT requirements.

Mobile Payments

Only five countries (about 10% of the countries responding to the questionnaire) reported this NPM. In those countries, this NPM seems to be used for micro-payments. The picture is mixed as regards regulatory framework and application of AML/CFT requirements.

None of the countries reported evidence of ML/TF or law enforcement cases.

Digital precious metals

This NPM does not seem to be widespread, as only 2 countries (Estonia and the USA) report its presence in their jurisdiction. Not much information is provided by Estonia,. In the USA case, a significant number of operators are active, but are not necessarily based, in the jurisdiction of the USA and numerous accounts are held. The applicable regulatory framework and AML/CFT provisions depends upon which state the payment method is located. However, most of the digital currency services are based outside the USA and are not subject to US law although they can be used by US-citizens. Law enforcement cases have been reported.

7. Conclusions and Issues for Further Consideration

The answers provided by countries to the questionnaire that was sent at the beginning of this study, reflected a legitimate market demand served by each of the payment methods analyzed, yet some actual and potential ML and TF vulnerabilities do exist. The FATF 40+9 Recommendations seem to allow for the pursuit of payment system innovation and AML/CFT, since they provide for the needed degree of flexibility in the application of AML/CFT standards to new emerging technology-based payment methods.

Among the main risk factors identified, specifically, this study notes that providers of new payment methods that are located outside the jurisdiction of a given country may pose additional risks compared with domestic service providers, especially when: (i) the distribution channel used is the Internet; (ii) no face-to-face contact with the customer takes place; and (iii) the NPM operates through an open network that can be accessed in a high number of jurisdictions.

The extent to which the new payment methods identified in this study are used for illegitimate purposes is difficult to determine at this time. The responses to the questionnaire issued by the project team provide only a limited number of typologies and show that the level of development and/or awareness of new payment methods is not uniform across the world. In this regard it should be noted that new payment methods are developing quickly and considerably; law enforcement cases may consequently increase as well in the near future.

As previously noted, it is believed that the FATF Forty Recommendations and Nine Special Recommendations provide an appropriate framework to address the vulnerabilities associated with these new methods of payment that have been identified by the project team. However, given the different characteristics and development that new payment methods may have in each jurisdiction, the study does highlight an opportunity for further examination of specific measures that could be adopted by countries to limit identified risks. In the case of new payment methods, technology plays a twofold role: on the one hand, it may increase typical ML/TF risks (i.e. anonymity, global use, speed of transfers, legal arbitrages, offshore provision of services) and on the other hand, help prevent or limit such risks (e.g. usage and spending limits, electronic record of transactions, etc.). Such additional measures could be applied in addition to or instead of traditional AML provisions (for example, CDD could be replaced by spending and loading limits on a payment instrument, which would represent thresholds, or by usage limits – such as non-reloadability or geographic limitations in the use of a payment instrument).

In light of the findings of this project, it is recommended that the WGTM considers the following possible future actions on this topic:

a) Providing guidance to jurisdictions as to what preventive measures may be taken to limit the risk of NPMs being used to launder money and/or finance terrorism (this could occur under FATF Recommendation 8);

b) Updating this study on the development of new payment methods as well as the relative typologies and risks analyses after a period of two years;

c) Proposing the inclusion of new payment methods as a specific issue to be monitored – during the two years period mentioned under letter b) above - under the project on ML and TF trends and indicators.

Appendix A: Description of Traditional Credit and Debit Card Networks

Network description

There are at least six global credit card networks: Visa (market leader), MasterCard, American Express, Diners Club, JCB, and Discover. Proprietary credit card networks, which may also be global in scope, also exist for the limited purpose of purchases at associated merchants. In addition, there are a variety of networks that support debit card and ATM transactions: Plus (Visa), Cirrus (MasterCard), Electron (Visa), and Maestro (MasterCard) operate internationally; Interact (Canada), STAR (U.S.), and others operate within one or more countries or regionally within a country. Historically, the card and EFT/POS network services have been somewhat distinct, not only in terms of the differences in credit and debit as products but also in terms of the authorization approach for those products. Credit cards grew from a point-of-sale (POS), charge card model and initially used "off-line" or signature-based authorization approaches. EFT/POS networks grew from an "on-line" or Personal Identification Number (PIN)-based card and dedicated automated teller machine (ATM) model. More recently, particularly in Europe and other regions outside the United States, the use of PINs and chip-based card infrastructures have become common for both credit and debit cards.

Infrastructure

The supporting infrastructure of the major credit card and EFT/POS networks has been migrating from proprietary networks and platforms to open systems. As these networks annually process billions of electronic payment transactions, the standards and security adopted by these organizations affect the future technology available to the payments industry. The traditional electronic connection between the merchant and the association, and the connection between the banks in the association for the card networks is typically a proprietary one.

The card associations/companies have proprietary, centralized backbone payment networks that connect retail merchants and associations, and banks within the association using special software and hardware. Regional or national EFT/POS networks provide similar access to other financial institutions and the ability to perform ATM and POS transactions. These networks can offer financial institutions a full range of switching (routing), authorization, clearing, and settlement services, including related back-office operations. Others only maintain a switch, relying on third-party processors to handle much of the data processing related to these services. Financial institutions affiliated with these networks may choose among the menu of options offered by these networks.

Clearing and Settlement

There are three phases within a credit card transaction: authorization of the underlying payment and purchase request, clearing of the accounting entries among the parties, and settlement among the parties in actual funds along with the payment of various interchange and other transaction-related fees.[46] Authorization and clearing of credit and signature-based debit transactions occurs through a "double message" process that involves two separate electronic transmissions; PIN-based debit transactions, by contrast, are "single message" processes in which authorization and clearing occurs during a single transmission. Credit and debit transactions involving PINs and chip-based card infrastructure may follow either of these authorization and clearance routes.

Credit cards

The first transmission within a credit card or signature debit transaction is the near real-time authorization request at the time of purchase. Payment information from the card and the merchant is sent from the merchant terminal to the acquiring bank and switched to the credit card processing network, which routes it to the issuing bank. The

[46] The exact processes involved in all three phases can vary significantly depending upon the individually negotiated arrangements between member banks and the card networks or the specific characteristics of the transaction and the parties involved. The remainder of this discussion is meant only to provide a general overview of these processes.

issuing bank responds with an "OK," indicating that the customer's credit card account is valid and that the customer has not surpassed his credit limit. The issuing bank then reduces the cardholder's "open-to-buy" credit line balance by the purchase amount. A stand-in processor may also provide the authorization as an alternative to the issuing bank. Certain PIN and chip-based credit cards may operate similarly.

Later in the day (though this may vary as well), either at multiple pre-determined times or once at the end-of-the-day, the merchant initiates a second batch-file clearing message of all the transaction data processed to his acquiring bank since the last such transmission. The acquiring bank reconciles the data against the authorization information. Once reconciled, the acquiring bank posts a credit to the merchant's account for the amount of the transactions, minus a merchant discount fee. The bank transmits a separate file of all merchant transaction data to the credit card association.

Final settlement generally begins with the credit card association using the member banks' aggregated transaction information to compile each member's net settlement position. The credit card association provides this information to members through proprietary settlement software or an "advisement" message that produces an audit trail and converts the data to a format interpretable by the bank. To settle these net positions, each issuing bank in a net debit position (or its correspondent bank) initiates a credit transfer to the credit card association's settlement bank and its special settlement account. The card association retains some of this payment to cover interchange, foreign exchange, or other association fees. The settlement bank then initiates a credit transfer from the settlement account to the acquirer's account with the remaining amount, minus its association fees. Member banks must maintain collateral with the credit card associations' settlement banks in the case of default. Banks can also settle both credit and debit card transactions directly with each other, through regional settlement bank, or by other net settlement arrangements. There can be significant variation in the settlement process depending upon the member involved.

Signature debit

A signature-based debit transaction is authorized similar to a credit card transaction, except that the issuing bank validates against the cardholder's demand deposit account or a stand-in authorizing system run by the card network. The clearing process is the same as a credit card transaction. Credit and signature-based debit transmissions may be sent separately. Settlement largely occurs in the same fashion as a credit card transaction. Some EFT/POS networks also process signature-based debit transactions with final settlement involving either credit transfers or direct debits. Overall, the card networks view signature-based debit and credit card transactions as almost identical for processing, clearing, and settlement. Certain PIN and chip-based credit cards may operate similarly.

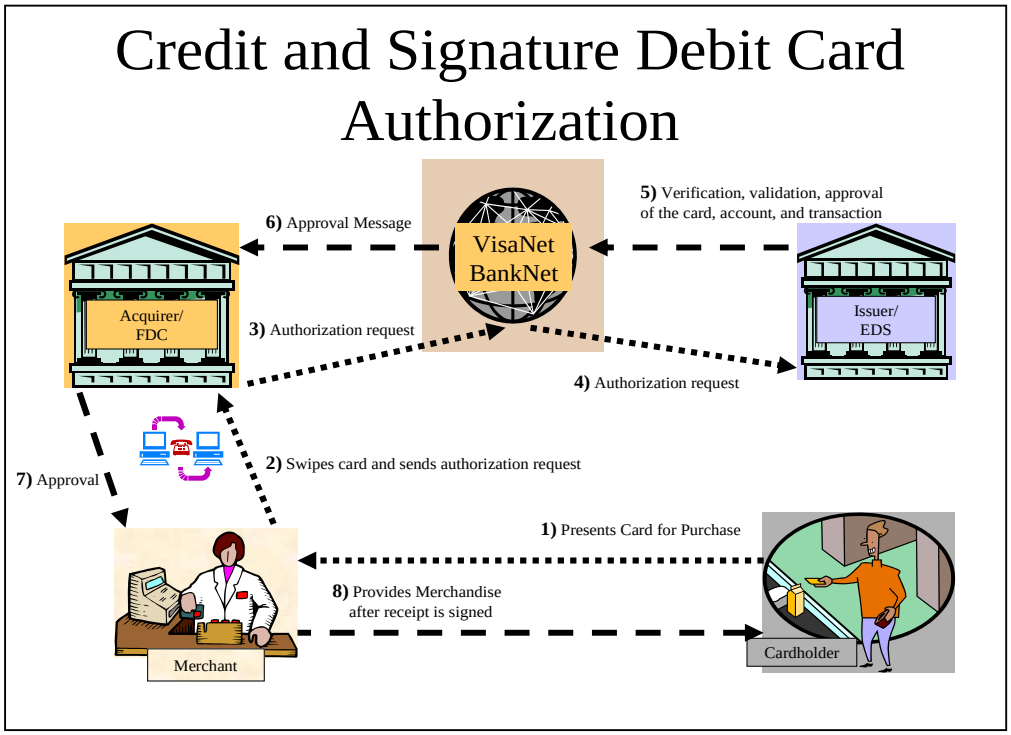


Figure 7

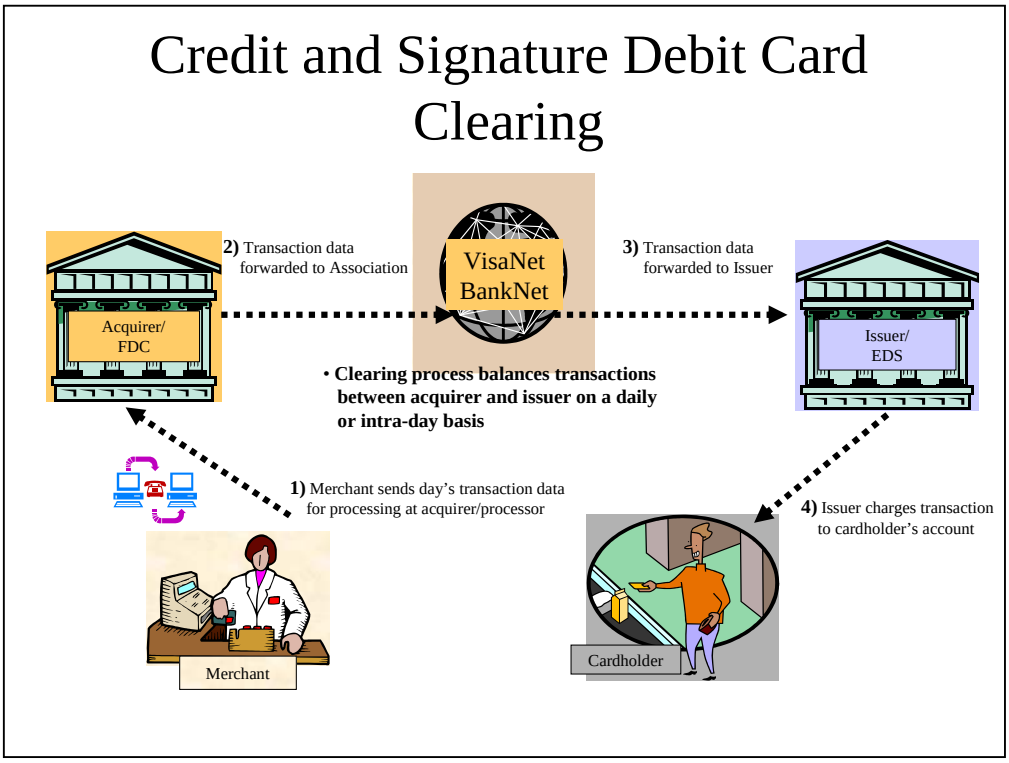


Figure 8

PIN-based debit

In the U.S., the card networks consider PIN-based debit fundamentally different and separate from signature-based debit and credit card transactions. This is not the case in other countries where PINs and chip-based cards are common. For PIN-based debit, the authorization and clearing of the transaction occurs within a single transmission. It can be routed through either an regional EFT/POS network, such as STAR, or a national or international PIN-based debit networks, such as Interact (POS or ATM) or Maestro and Interlink if it is a POS transaction and Cirrus and PLUS if it is an ATM transaction.[47] A stand-in processor may also be used. The authorization process at the issuing bank is the same as the authorization for signature-based debit, save that the consumer must enter a PIN at the merchant terminal or at the ATM. The issuing bank typically debits the cardholder's account immediately as the final amount of the transaction is confirmed at the time of purchase. The acquiring bank or its processor also obtains a full transaction record as a result of the transmission, clearing the transaction between the banks. The acquiring bank typically credits the merchant for the amount of the transaction at that time.

Final settlement among EFT/POS members can occur in a number of different ways, just as it can with the card networks. One way involves book-entry net settlement at the EFT/POS network's chosen settlement bank. Each member bank funds a settlement account at the EFT/POS network's settlement bank. The EFT/POS network and its settlement bank debits and credits the issuing and acquiring members' accounts to finalize the transfer of funds. This includes both the actual transaction amount and any network-related fees. A second option is for members to have their processing agent set up a settlement account at a settlement bank other than the EFT/POS network's or for the member to hold the account. In this case, the EFT/POS network originates a direct debit of the issuing member's settlement account (authorization for this is given as part of the requirements of network membership) to credit the acquiring member's account (or the EFT/POS network's settlement account at

[47] Where transactions can flow over either regional, national, or international EFT/POS networks, the regional network normally take precedence according to their regional routing rules. However, the merchant and acquiring bank may be able to prioritize that routing order to some extent.

its settlement bank in the case of network fees). Depending upon the EFT/POS network, the daily settlement process may include just the individual transaction amounts or there may be separate settlements of the day's transactions and their associated network fees. Some EFT/POS networks will delay the settlement of the network fees until the end of the month.

Alternatively, if the transaction flows through a card network, the clearing among the banks and the national network occurs later, through a similar net settlement process as that used with signature-based debit and credit card transactions. Settlement may use traditional national direct debit or credit transfer systems. Settlement is based on the issuing bank's positive response to the authorization request. The issuer rather than the acquirer pays the network interchange fees for PIN-based ATM transactions.

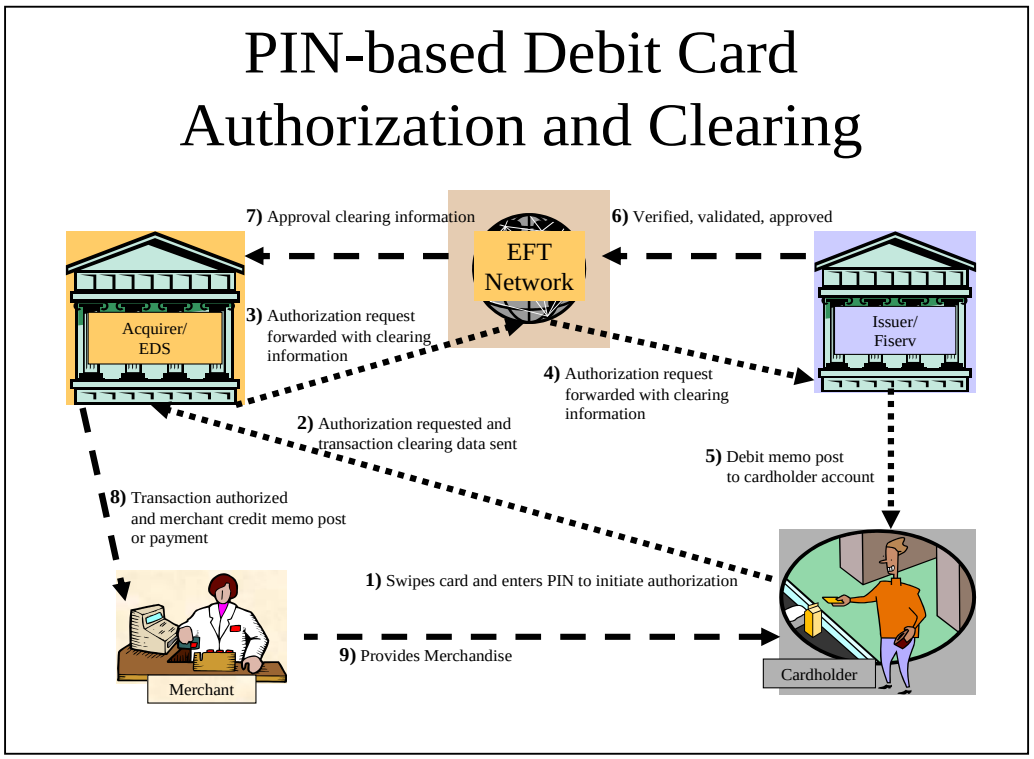


Figure 9

Appendix B: Supplemental NPM Questionnaire Results and Analysis

Table A: Short description of the NPM.

Table B: The two main indicators for market size are the estimated number of domestic service providers and the estimated number of accounts held or cards issued.

Table C: Information on regulatory provisions. The distinction between registration (R) and licensing (L) is noted. The main difference between these two categories is that licensing pre-supposes authorization to provide payment services (subject to conditions such as prudential rules, etc), whereas registration is not subject to conditions. As regards supervision, different approaches are also possible, and whenever detailed information is provided, it is reported under "additional information".

Table D: AML/CFT provisions can derive from regulations in place or from business practice (a typical example of business practice being limits to transferred amounts).

Table E: Reports of AML/CFT cases or if any illegal operators have been found (illegal operator means those which are not registered or licensed).

Prepaid or prepaid payment cards

A. Description of the NPM

Countries	Short description of the NPM
Ireland (IE)	"Virtual visa voucher" – offered by permanent TSB bank in association with Visa and 3V transaction services – available since September 2005 – customer registers online, voucher is printed upon request at a participating retailer, and a "disposable" pre-paid card is issued; this card can be used to purchase goods on the internet or by mail/telephone order.
Turkey (TR)	"Pre-paid debit cards" are mentioned, but no detailed information is provided.
Lebanon (LB)	Prepaid cards are mentioned but insufficient information is provided (e.g. in relation to Visa/ Mastercard branded networks)- "Liters plus" referred as limited-purpose pre-paid card)
Palau (PA)	Reference to pre-paid debit cards that can be used in ATM networks, no additional information is provided.
Lithuania (LT)	Reference to pre-paid debit cards issued by banks or shops, but no detailed information is provided.
New Zealand (NZ)	"Visa Cash passport" (available for purchase in NZ and for ATM cash withdrawal in NZ and overseas); other store-value cards used in NZ for purchases in closed systems (transport operators, educational institutions, etc.)
Cyprus (CY)	Pre-paid card issued by a bank; it can be used at venues where Visa electron is accepted and for internet payments; the information is limited
Czech Republic (CZ)	E-tickets for the payment of public transport; this service is not cross-border.

Italy (IT)	Rechargeable prepaid cards require full CDD, and AML provisions fully apply. Prepaid cards that may not be recharged may not exceed the amount of 500 EUR and do not require CDD to be applied, they may thus be anonymous. Such cards are issued by financial institutions (i.e. banks and e-money institutions). In some cases the customer originally holds a credit with a telephone company (the card is at this stage a telephone card) and then converts such credit into a credit with a financial institutions which is legally the prepaid card issuer (at this stage the card is a payment instrument).
Austria (AT)	Pre-paid debit cards (2 systems) which do not require a bank account and which can be used for cash withdrawals at an ATM or for purchases at a point of sale; funding methods include cash and credit transfers. No information on market size.
USA	Different types of prepaid cards are identified, covering a variety of uses and technologies, both operating within either an "open" or "closed" system.
Spain (ES)	Hal-Cash; it is based on a pre-paid account which allows ATM cash withdrawal cross-border; mobile phone is issued as an access device and as a messaging system; this product is mainly offered to un-banked, immigrant populations.
Switzerland (CH)	A pre-paid multi-purpose debit card. Micro-payments can be made through the internet and/or mobile phone by online merchants. Users scratch off a panel on the card to access a code which corresponds to their pre-paid credit amount. When executing the payment of products or services ordered over the internet or by means of a mobile phone, users have to indicate the card's code, which gives access to the pre-paid account held in the issuer's server. The amount is then deducted from the actual card balance.

B. Market size

Estimated number of Domestic Service Providers		Estimated number of Accounts Held Cards Issued	
≤ 3	> 3	≤ 1000	> 1000
IT,IE, PA, NZ, CH	CZ, USA, ES	NZ (per anum)	CZ, IT, USA

C. Access to activity

Registration/Licensing		Supervision		Additional information
Yes	No	Yes	No	
AT, CZ, IT, IE(L), LB (L), CH	PA, NZ, HK, ES (?), USA	IE, LB, AT, CZ, IT, CH	PA, NZ, HK, ES (?)	IE, LB: providers are banks.

D. AML/CFT Provisions

Customer Due Diligence		Record-keeping		Suspicious Transaction Reporting		Other AML Policies & Procedures		Limit to transferred amount if any	
Yes	No	Yes	No	Yes	No	Yes	No	≤ 500	> 500
AT, IT IE, LB, PA, NZ, CH	DE, IT, USA, HK, ES	IE, LB, PA, NZ, IT, AT, USA, CH	IT , HK, ES	IE, LB, PA, NZ, AT, IT, CH	USA, HK, ES	IE, LB, PA, AT, IT, USA, CH	NZ, HK, ES	AT, CZ, IT, IE(350), LB, NZ (25.000 NZ$); NZ yes but depends on ATM network	USA, ES, PA no limit

E. AML/CFT Cases - illegal operators

Evidence of Money Laundering		Examples of Law Enforcement		Illegal Operators	
Yes	No	Yes	No	Yes	No
NZ	AT, CZ, IT, USA, IE, LB, ES, CH	USA, NZ	AT, CZ, IT, IE, LB, ES, CH		AT, CZ, IT, USA, IE, LB, NZ, ES, CH

Payments initiated by means of a mobile phone (and linked to a bank-account)

A. Description of the NPM

Countries	Short description of the NPM
Finland (FI)	"Mobiiliraha" – linked to a bank account; no detailed information is provided.
New Zealand (NZ)	Mobile phone banking, meaning access to a bank account by means of a mobile phone device.
China (CN)	Mobile phone banking, meaning access to a bank account by means of a mobile phone device.
Korea (KO)	The use of mobile phones or PDA's for cross-border payments from a bank-account to a (foreign) bank-account.

B. Market size

Estimated number of Domestic Service Providers		Estimated number of Accounts Held Cards Issued	
≤ 3	> 3	≤ 1000	> 1000
	KO, FR		KO

C. Access to activity

Registration/Licensing		Supervision		Additional information
Yes	No	Yes	No	
KO, FI, NZ, CN, FR		KO , FI, NZ, CN, FR		

D. AML/CFT Provisions

Customer Due Diligence		Recordkeeping		Suspicious Transaction Reporting		Other AML Policies & Procedures		Limit to transferred amount if any	
Yes	No	Yes	No	Yes	No	Yes	No	≤ 500	> 500
KO, FI, NZ, CN		KO, FI, NZ, CN		KO, FI, NZ, CN		KO, FI, NZ, CN			KO

E. AML/CFT Cases - illegal operators

Evidence of Money Laundering		Examples of Law Enforcement		Illegal Operators	
Yes	No	Yes	No	Yes	No
	KO, FI, FR		KO, FI, FR		KO, FI, FR

E-purse

A. Description of the NPM

Countries	Short description of the NPM
Germany (DE)	Geldkarte: The funds of the card are on the card itself; in general, the funds are loaded from a bank account and no online connection and no cardholder identification are needed to make a payment; this card has almost no cross-border

	operability. Geldkarte is actually a common technological standard for chipcards; many banks issue their own Geldkarte cards. However, as all these cards are fully inter-operable, for the purpose of this report Geldkarte can be considered as a singular payment instrument.
Netherlands (NL)	Chipknip: The money is loaded from a bank-account and can be used as an independent electronic purse.
Switzerland (CH)	CASH system: The money is loaded form a bank-account and can be used as an independent electronic purse.

B. Market size

Estimated number of Domestic Service Providers		Estimated number of Accounts Held Cards Issued	
≤ 3	> 3	≤ 1000	> 1000
DE, NL	CH		DE, NL, CH

C. Access to activity

Registration/Licensing		Supervision		Additional information
Yes	No	Yes	No	
DE, NL, CH		DE, NL, CH		

D. AML/CFT Provisions

Customer Due Diligence		Recordkeeping		Suspicious Transaction Reporting		Other AML Policies & Procedures		Limit to transferred amount if any	
Yes	No	Yes	No	Yes	No	Yes	No	≤ 500	> 500
CH, NL,	DE[48],	CH, DE, NL		CH, DE, NL		CH, DE, NL		DE, NL, CH	

E. AML/CFT Cases / illegal operators

Evidence of Money Laundering		Examples of Law Enforcement		Illegal Operators	
Yes	No	Yes	No	Yes	No

[48] In Germany, e-purses can be legally issued only by credit institutions which are subject to full AML policies and procedures with only one exception: due to the low loading limit, customer identification/CDD is not deemed necessary.

	DE, NL, CH		DE, NL, CH		DE, NL, CH

Internet payments

A. Description of the NPM

Countries	Short description of the NPM
Canada (CA)	Many providers, including offshore.
Belgium (BE)	Paypal (which is regulated by the FSA in the UK, and provides its services in Belgium under the license of e-money institutions granted by the UK's FSA, which provides for the possibility to operate all across the EU). It is therefore not under Belgian, but UK's supervision.
Finland (FI)	"Digiraha" described as “digital purse for internet payments”. No detailed information.
Estonia (ET)	Fogott, Paypal, Netteller- no detailed information is provided.
New Zealand (NZ)	Paypal
Austria (AT)	Emerging server-based system for purchases on the Internet.
China (CN)	Different emerging e-business enterprises and third party intermediaries are providing their own business and online payment intermediaries.
Czech Republic (CZ)	Internet shopping; the user has a virtual account on the website and the provider debits this account at the moment of purchase; limited information is provided.
France (FR)	Neosurf: customer exchanges funds for a scratch card (of various amounts), which gives a code to pay on the internet. This system is active in France, Belgium and Switzerland.
Germany (DE)	Paypal (which is regulated by the FSA in the UK, and provides its services in Germany under the license of e-money institutions granted by the UK's FSA, which provides for the possibility to operate all across the EU). It is therefore not under German, but UK's supervision.
Indonesia (ID)	Online payment for on-line merchants and person-to-person money transmission; the services can be used for local and cross-border payments; these payment methods are still under construction and do not operate yet.
Italy (IT)	1) Moneta On Line: This is a scratch card issued by a bank to make low-value purchases over the internet at merchants adhering to the VISA circuit; the users are not identified; 2) BankPass Web: This is an electronic wallet to pay on the internet.
Netherlands (NL)	Several providers, including Paypal
Spain (ES)	1) Paypal: Spain seems to have imposed stricter AML/CFT provisions on

	Paypal than Germany and the Netherlands. 2) Click & Buy: This is an internet billing mechanism for enterprises; it can be used to buy at merchants in different parts of the world.
Switzerland (CH)	Click and buy micro-payments through the internet at online merchants other than the issuer of the card.
USA	There are several domestic online payment services, including PayPal, and others offshore that access the U.S. market.

B. Market size

Estimated number of Domestic Service Providers		Estimated number of Accounts Held Cards Issued	
≤ 3	> 3	≤ 1000	> 1000
CZ, FR, DE, ID, ES(1), ES(2), CH, BE	NL, IT, USA, CA	CZ, ES(1)	NL, FR, DE, USA

C. Access to activity

Registration/Licensing		Supervision		Additional information
Yes	No	Yes	No	
AT, GE, ID, IT, NL, ES(1), CH, USA, BE	CN, ES(2), NZ, CA, ET	AT, DE, ID, IT, NL, ES(1), CH, CA (for AML purposes), USA, BE	CN, ES(2), NZ, ET	CN is working on regulation- ET will soon enforce the EU e-money Directive.

D. AML/CFT Provisions

Customer Due Diligence		Recordkeeping		Suspicious Transaction Reporting		Other AML Policies & Procedures		Limit to transferred amount if any	
Yes	No	Yes	No	Yes	No	Yes	No	≤ 500	> 500
AT, ID, IT, ES(1), CH, USA, NZ, CA, ET, DE, BE	CN, NL,ES(2)	AT, ID, USA, IT, ES(1), CH, USA, NZ, CA, ET, DE, BE, NL	CN, ES(2)	AT, ID, IT, ES(1), CH, USA, NZ, CA, ET, DE,	CN, ES(2)	AT, ID, IT, ES(1), CH, USA, CA, DE, BE	CN, NL, ES(2), NZ, ET	AT, FR, CH, CA (has a limit, but amount depends on business practice)	DE, IT, NL, ES(1), ES(2), CN

				BE, NL					

E. AML/CFT Cases - illegal operators

Evidence of Money Laundering		Examples of Law Enforcement		Illegal Operators	
Yes	No	Yes	No	Yes	No
CN, ET, CA, USA	AT, FR, DE, ID, IT, NL, ES(1), ES(2), CH, NZ, BE	USA, ET, CA	AT, CN, FR, DE, ID, IT, NL, ES(1), ES(2), CH, NZ, BE	CN, ID, USA	AT, FR, DE, IT, NL, ES(1), ES(2), CH, BE

Mobile Payments

A. Description of the NPM

Countries	Short description of the NPM
France (FR)	Post-paid and pre-paid payment service are offered by telephone companies.
Belgium (BE)	Mobile payments (SIM reload only) are estimated to be available in Belgium on a reduced scale for at least 2 years.
Lithuania (LT)	Information provided suggests use of mobile phones to pay for limited purposes (parking, tickets for concerts or other events) from prepaid balance or mobile phone bill; but no detailed information is provided.
Germany (DE)	1) Crandy is a pre-paid mobile payments system, which allows person-to-person transfers and payments at POS; funds can be transferred from a bank account. 2) Pre-paid scratch cards for payment by mobile phone
Netherlands (NL)	Payment services by telephone company for payments using a mobile phone (for example for purchasing of ring-tones).

B. Market size

Estimated number of Domestic Service Providers		Estimated number of Accounts Held Cards Issued	
≤ 3	> 3	≤ 1000	> 1000
	FR, DE, NL		FR, DE, NL

C. Access to activity

Registration/Licensing		Supervision		Additional information
Yes	No	Yes	No	
DE (L)	NL	DE	NL	

D. AML/CFT Provisions

Customer Due Diligence		Recordkeeping		Suspicious Transaction Reporting		Other AML Policies & Procedures		Limit to transferred amount if any	
Yes	No	Yes	No	Yes	No	Yes	No	≤ 500	> 500
	NL, DE, BE	DE, BE (but not required by Law)	NL	DE	NL, BE	DE	NL, BE	DE, NL,BE (fixed by the telecom operator)	

E. AML/CFT Cases - illegal operators

Evidence of Money Laundering		Examples of Law Enforcement		Illegal Operators	
Yes	No	Yes	No	Yes	No
	FR, DE, BE		FR, DE		FR, DE

Digital precious metals

A. Description of the NPM

Countries	Short description of the NPM
Estonia (ET)	"Icegold" No detailed information is provided.
USA	A number of digital precious metals dealers are accessible online. Funding accounting and withdrawing funds is accomplished through “an exchange service.” Each exchange service sets its own terms as to how it is willing to receive and remit funds. Some may only accept transfers from bank or credit card accounts, while others will accept cash and money orders.

B. Market size

Estimated number of Domestic Service Providers		Estimated number of Accounts Held Cards Issued	
≤ 3	> 3	≤ 1000	> 1000
ET	USA		USA

C. Access to activity

Registration/Licensing		Supervision		Additional information
Yes	No	Yes	No	
USA		USA		In the United States, money transmitters are among money services businesses that are required to register with the FIU (FinCEN), they also are subject to AML reporting and recordkeeping requirements and are often required to be licensed on the state level. Whether an online payment system or digital precious metals dealer meets the definition of a money transmitter pursuant to the relevant regulations, though, depends upon its location and the ways in which it participates in or conducts transactions. Many online payment systems are based outside the United States and are not subject to U.S. jurisdiction.

D. AML/CFT Provisions

Customer Due Diligence		Recordkeeping		Suspicious Transaction Reporting		Other AML Policies & Procedures		Limit to transferred amount if any	
Yes	No	Yes	No	Yes	No	Yes	No	≤ 500	> 500
	USA	USA			USA		USA	USA: established by each issuer	USA: established by each issuer

E. AML/CFT Cases - illegal operators

Evidence of Money Laundering		Examples of Law Enforcement		Illegal Operators	
Yes	No	Yes	No	Yes	No
USA		USA		USA: offshore	

Appendix DD:

FATF, *FATF Report: Money Laundering Using New Payment Methods*
(Paris: FATF, 2010)

FATF • GAFI
FINANCIAL ACTION TASK FORCE GROUPE D'ACTION FINANCIÈRE

FATF Report

Money Laundering Using New Payment Methods

October 2010

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

ACKNOWLEDGEMENTS

The FATF would like to thank Vodafone, Moneybookers and the Consultative Group to Assist the Poor (CGAP) for presentations provided to the project team during the 2009/2010 annual typologies experts' meeting in the Cayman Islands and MasterCard Europe for their presentation on prepaid cards at the project team's intersessional meeting in Amsterdam in 2010. In addition, comments received from the GSMA and Western Union, during the FATF private sector consultation, were also much appreciated.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. After the 2006 New Payment Method (NPM) report, the growing use of NPMs and an increased awareness of associated money laundering and terrorist financing risks have resulted in the detection of a number of money laundering cases over the last four years.

2. The project team analysed 33 case studies, which mainly involved prepaid cards or internet payment systems. Only three cases were submitted for mobile payment systems, but these involved only small amounts. Three main typologies related to the misuse of NPMs for money laundering and terrorist financing purposes were identified:

- Third party funding (including strawmen and nominees).
- Exploitation of the non-face-to-face nature of NPM accounts.
- Complicit NPM providers or their employees.

3. While the analysis of the case studies confirms that to a certain degree NPM are vulnerable to abuse for money laundering and terrorist financing purposes, the dimension of the threat is difficult to assess. The amounts of money laundered varied considerably from case to case. While some cases only involved amounts of a few hundred or thousand US dollars, more than half of the cases feature much larger amounts (four cases involved over 1 million US dollars mark, with the biggest involving an amount of USD 5.3 million).

4. The project team retained and updated the 2006 report´s approach to assessing money laundering and terrorist financing risk associated with NPMs and assesses the risk of each product or service individually rather than by NPM category.

5. Anonymity, high negotiability and utility of funds as well as global access to cash through ATMs are some of the major factors that can add to the attractiveness of NPMs for money launderers. Anonymity can be reached either "directly" by making use of truly anonymous products (*i.e.*, without any customer identification) or "indirectly" by abusing personalised products (*i.e.*, circumvention of verification measures by using fake or stolen identities, or using strawmen or nominees etc.).

6. The money laundering (ML) and terrorist financing (TF) risks posed by NPMs can be effectively mitigated by several countermeasures taken by NPM service providers. Obviously, anonymity as a risk factor could be mitigated by implementing robust identification and verification procedures. But even in the absence of such procedures, the risk posed by an anonymous product can be effectively mitigated by other measures such as imposing value limits (*i.e.*, limits on transaction amounts or frequency) or implementing strict monitoring systems. For this reason, all risk factors and risk mitigants should be taken into account when assessing the overall risk of a given individual NPM product or service.

7. Across jurisdictions, there is no uniform standard for the circumstances in which a product or service can be considered to be of "low risk". Many jurisdictions use thresholds for NPM transactions or caps for NPM accounts in order to define "low-risk scenarios"; but the thresholds and caps vary

significantly from jurisdiction to jurisdiction. Likewise, different views may be taken on the relevance of certain risk factors or of the effectiveness of certain risk mitigants, due to respective legal and cultural differences in jurisdictions.

8. Some jurisdictions allow firms to apply simplified CDD measures in cases of predefined low-risk scenarios. Again, there is no uniform standard across jurisdictions on the definition of "simplified CDD measures". Some jurisdictions even grant a full exemption from CDD measures in designated low-risk scenarios.

9. Not all NPM services are subject to regulation in all jurisdictions. While the issuance of prepaid cards is regulated and supervised in all jurisdictions that submitted a response to the project questionnaire, the provision of Internet payment and mobile payment services is subject to regulation and supervision in most, but not all jurisdictions (FATF Recommendation 23; Special Recommendation VI).

10. The project team also identified areas where the current FATF standards only insufficiently account for issues associated with NPMs:

- Where NPM services are provided jointly with third parties (*e.g.*, card program managers, digital currency providers, sellers, retailers, different forms of "agents"), these third parties are often outside the scope of AML/CFT legislation and therefore not subject to AML/CFT regulation and supervision. The concept of agents and outsourcing is only marginally addressed in the FATF 40 Recommendations and 9 Special Recommendations (in Recommendation 9 and Special Recommendation VI). More clarification or guidance from FATF on this issue would be welcome, especially as a few jurisdictions are considering a new approach on the regulation and supervision of agents.

- Many NPM providers distribute their products or services through the Internet, and establish the business relationship on a non-face-to-face basis, which, according to FATF Recommendation 8, is associated with "specific risks". The Recommendations do not specify whether "specific risks" equates to "high risk" in the sense of FATF Recommendation 5; if so, this would preclude many NPM providers from applying simplified CDD measures. While FATF experts have recently come to the conclusion that non-face-to-face business does not automatically qualify as a high risk scenario in the sense of Recommendation 5, it would be helpful if this could be confirmed and clarified within the standards.

11. It would be desirable if other Working groups within FATF decided to pick up the discussions described above to provide more clarity on the interpretation of the FATF Recommendations involved. Such work would not only be relevant and helpful for the issues of money laundering and terrorist financing, but also for the issue of financial inclusion.

12. NPMs (as well as other financial innovations) have been identified as powerful tools to further financial inclusion. Many of the challenges mentioned above (*e.g.*, discussion on simplified CDD in cases of low risk, full exemption from CDD, or the regulation and supervision of agents) are of high relevance for the entire discussion around financial inclusion, going beyond the issue of the vulnerability of NPMs to ML/TF purposes alone.

CHAPTER 1: INTRODUCTION

The 2006 report

13. In October 2006, the FATF published its first report on New Payment Methods (NPMs). The report was an initial look at the potential money laundering (ML) and terrorist financing (TF) implications of payment innovations that gave customers the opportunity to carry out payments directly through technical devices such as personal computers, mobile phones or data storage cards.[1] In many cases these payments could be carried out without the customer needing an individual bank account.

14. As these NPMs were a relatively new phenomenon at the time, only a few ML/TF case studies were available for the 2006 report. In addition, clear definitions of various NPM products and how they should be regulated were just beginning to be addressed by a limited number of jurisdictions. Therefore the report focused on raising awareness of these new products and the potential for their misuse for ML/TF purposes.

15. The 2006 report found that ML/TF risk was different for each NPM product and that assessing the ML/TF risk of NPM categories was therefore unhelpful. Instead, it developed a methodology to assess the risk associated with individual products.

16. The report concluded that it should be updated within a few years, or once there was greater clarity over the risks associated with these new payment tools. This report updates the 2006 report on NPMs and provides an overview of the most recent developments.

Objectives of the present report

17. Since the publication of the 2006 report, NPMs (prepaid cards, mobile payments and Internet payment services) have become more widely used and accepted as alternative methods to initiate payment transactions. Some have even begun to emerge as a viable alternative to the traditional financial system in a number of countries.

18. The rise in the number of transactions and the volume of funds moved through NPMs since 2006 has been accompanied by an increase in the number of detected cases where such payment systems were misused for ML/TF purposes. The NPM report in 2006 identified potential legitimate and illegitimate uses for the various NPMs but there was little evidence to support this. The current report will compare and contrast the "potential risks" described in the 2006 report to the "actual risks" based on new case studies and typologies. Not all potential risks identified in 2006 were backed up by case studies. This does not mean that those risks are no longer of concern, and jurisdictions should continue to be alert to the market´s development to prevent misuse and detect cases that went unnoticed before.

19. The report will also develop red flag indicators which might help a) NPM service providers to detect ML/TF activities in their own businesses and b) other financial institutions to detect ML/TF

[1] Including different storage media such as magnetic stripe cards or smart card electronic chips.

activities in their business with NPM service providers, in order to increase the number and quality of suspicious transaction reports (STRs).

20. Although more case studies are now available, issues surrounding appropriate legislation and regulations for NPMs are still a challenge for many jurisdictions. Consequently, the report also identifies the unique legal and regulatory challenges associated with NPMs and describes the different approaches national legislators and regulators have taken to address these. A comparison of regulatory approaches can help inform other jurisdictions' decisions regarding the regulation of NPM.

21. Finally, this report considers the extent to which the FATF 40+9 Recommendations continue to adequately address the ML/TF issues associated with NPMs.

Steps taken by the project team

22. The project team analysed publications about NPMs and ML/TF[2]. It also analysed the responses to questionnaires which covered the spread of domestic NPM service providers[3], the role of regulation in relation to NPMs and case studies detected in jurisdictions (the latter also including foreign service providers). Thirty-seven jurisdictions and the European Union Commission submitted a response.[4]

23. The majority of the respondents identified NPMs within their jurisdiction. Prepaid cards were the most common (34 of the countries have such providers), followed by Internet payment services (IPS) providers with 17 countries and mobile payment services with 16 countries offering each NPM respectively. Case studies were provided for the three NPMs: 18 cases involving prepaid cards, 14 cases involving Internet payment services and three cases involving mobile payment services.[5] A detailed summary is attached in Appendix A.

24. The project team also consulted with the private sector in several ways. During the 2009-2010 annual typologies experts´ meeting in the Cayman Islands, representatives from NPM service providers, including the Internet payment sector, the mobile payments sector and a representative from the Consultative Group to Assist the Poor (CGAP), provided presentations to the project team. At the project team´s intersessional meeting in Amsterdam in March 2010, a representative from a card technology provider in Europe gave a presentation on prepaid cards. A more wide-ranging private sector

---

2 See Appendix C for a list of publications used for this report.

3 Including a description of the biggest or most significant products and service providers.

4 The FATF and the NPM project team would like to thank all jurisdictions and organisations that have contributed to the completion of this report by providing experts to participate in the project team and by submitting responses to the project questionnaire, including (sorted alphabetically): Argentina, Armenia, Australia, Austria, Belarus, Belgium, Brazil, Bulgaria, Canada, Cayman Islands, Colombia, Denmark, Estonia, European Commission, France, Germany, Gibraltar, Italy, Japan, Jersey, Lebanon, Luxembourg, Macao, Mexico, Netherlands, Norway, Oman, Peru, Philippines, Poland, Portugal, Russia, Singapore, Slovak Republic, South Africa, St. Vincent & the Grenadines, Sweden, Switzerland, UK, Ukraine, USA, and the World Bank. The project team would also like to thank the secretariat of the Egmont Group for circulating the questionnaire among its members, thus increasing the outreach of the entire project.

5 Various reasons have been proposed for the low number of cases, including that transaction value and volume remains very small for mobile payments, or that these systems may not be attractive to money launderers, or that mobile providers and law enforcement have failed to detect criminality or that criminals, or indeed law enforcement are unfamiliar with the technology.

consultation was also conducted through the FATF electronic consultation platform where a draft of this report was presented for consultation.

Structure of the present report

25. This report is based on the FATF 2006 report. It attempts to avoid repetition as much as possible. The report therefore does not describe the general working mechanisms of NPMs.[6] Instead, it focuses on recent developments, updates the risk assessment and introduces new case studies.

26. The report is divided into 4 sections:

- Section 1 (chapters 1 and 2) introduces the project work as well as the key overarching issues. It also provides an overview of recent developments;
- Section 2 (chapters 3 and 4) addresses the risks and vulnerabilities of NPMs and presents case studies and typologies.
- Section 3 (chapter 5) addresses regulatory and supervisory issues, exploring the different national approaches to AML legislation as well as the prosecution of illicit NPM service providers.
- Section 4 (chapter 6) concludes the report and identifies issues for further consideration.

6 Relevant sections of the 2006 report (including definitions) are cited as excerpts in Appendix B.

CHAPTER 2: BACKGROUND

"New Payment Methods" and their development since 2006

27. In 2006, bank-issued payment cards and transactions via the internet or over the telephone were not really new. Depository financial institutions have offered remote access to customer accounts for decades. What was new about these technologies in 2006 was their use by banks outside of traditional individual deposit accounts and by non-banks, some of which did not fit traditional financial service provider categories and therefore sometimes fell outside the scope of regulation despite providing financial services such as the carrying out of payments or holding accounts. Indeed there are still several jurisdictions where NPM service providers are not subject to prudential and/or AML regulation.

28. The development of NPMs has created new opportunities for criminals to misuse such technologies for the purposes of ML and TF. This has, in turn, resulted in new typologies and created new challenges for law enforcement authorities.

The promotion of NPMs through jurisdictions and government agencies

29. NPMs have developed as a result of the legitimate need of the market for alternatives to traditional financial services. In some cases, this was driven by the demand for more convenient or safer ways to pay for online purchases; in other cases, their development was fostered by a desire to provide access to financial services for those who were excluded from traditional financial services (*e.g.*, individuals with poor credit ratings, minors, but also inhabitants of under-banked regions),[7] and the assumption that NPMs may have a positive effect on national budgets as well as overall national and global economic development.[8]

Box 1.

United States: Four million people who receive Social Security benefits lack bank accounts. To reduce reliance on paper checks, the United States began distributing these benefits using prepaid cards, which beneficiaries can use to purchase goods or get cash. Previously, beneficiaries cashed checks at non-banks and conducted transactions using cash or money orders.*

Pakistan: Fighting forced more than a million people from their homes in 2009. The Government of Pakistan

7 The World Bank, the Consultative Group to Assist the Poor (CGAP), the G-20 Access Through Innovation Sub Group and other organisations have also identified NPMs, mobile payment services in particular, as a possible tool for financial inclusion of the poor and/or the under-banked and launched initiatives to promote and support the implementation of NPMs in jurisdictions concerned.

8 This is due to efficiency gains in terms of transaction speed, finality of payments, security features of technology based payment methods and their lower costs compared to paper payment instruments. Another important characteristic of NPMs that explains policy-makers' support for their sound development is their accessibility: especially pre-paid cards and mobile payments grant easy access to the payment system by the whole population, including the unbanked. Given these potentialities, central banks in their capacity of payment system overseer have long since devoted specific attention to the development of NPMs. Ultimately, the Bank for International Settlements has launched an initiative to study the innovations in retail payments.

needed a way to deliver financial assistance to these displaced individuals quickly. Rather than distributing cash, the Government of Pakistan partnered with a bank to distribute prepaid cards with access to 25,000 Pak rupees (about USD 300). At the same time, a Pakistani bank and a payment card company installed wireless point-of-sale terminals at retailers where people could buy basic supplies. By using cards rather than cash, the Government of Pakistan provided immediate assistance to nearly 300,000 families through transparent distribution channels.**

* Direct Express Media (2008)
** Visa Corporate Site (2010)

30. As a result, some jurisdictions have adapted their regulatory framework to actively promote NPMs within their domestic market.

Box 2. The EU Commission openly encourages and promotes the development of NPMs and concluded in its Explanatory Memorandum to the original E-Money-Directive of 1998:*

"Electronic money has the potential to develop into an efficient and effective means of payment; it can play a significant role in the development and improvement of electronic commerce; and it can be an important tool in the completion of the single market and monetary union. The Commission is of the view that it is in the interests of both business and consumers alike that electronic money develops within a regulatory environment that instils trust and confidence in this new and developing payment instrument. At the same time it is vital that development is allowed to take place unimpaired by strict technological rules which will hamper innovation and restrict competition.

The Commission proposal (…) introduces the regulatory regime necessary to ensure the financial integrity of non-bank issuers without stifling developments in the domain of electronic money and will help to cultivate an environment in which the development of this new means of payment is promoted in the interests of business and consumers."

In a review of the original E-Money-Directive, the Commission kept up the aforementioned goals and intentions:**

"The general objective of the review of the EMD is to promote the emergence of a true single market for electronic money services in Europe. Contribute to the design and implementation of new, innovative and secure electronic money services. Provide market access to new players and real and effective competition between all market participants, thereby generating significant benefits to the wider European economy."

Accordingly, recital (4) of the amended E-Money-Directive*** reads:

"(4) With the objective of removing barriers to market entry and facilitating the taking up and pursuit of the business of electronic money issuance, the rules to which electronic money institutions are subject need to be reviewed so as to ensure a level playing field for all payment services providers."

* Commission of the European Countries (1998)
** Commission of the European Countries (2008)
*** Official Journal of the European Union (2009)

Other studies on NPMs and ML/TF risks and vulnerabilities

31. NPMs have attracted a significant amount of press coverage. They have also been the subject of an increasing number of public and private sector research initiatives. In addition, there are a number of recent or ongoing typologies projects of FATF and FSRBs that touch upon this subject.[9] This shows that the awareness of the opportunities and risks associated with NPMs has increased since the publication of the 2006 report.

32. These studies have often focussed on one category of NPMs only. This report is different as it will provide a broader comparative analysis of these issues and identify the commonalities shared by all types of NPMs. It will also identify the specific challenges within each category of NPMs.

9 Recent or ongoing typologies projects include: FATF typologies report on *Money Laundering and Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems* (FATF (2008)); MONEYVAL workshop on Cybercrime (ongoing); EAG workshop on internet payments (ongoing).

2.1 Recent Developments Related to Prepaid cards

33. Prepaid cards can be split into two broad categories, open-loop cards and closed-loop cards.[10] This report focuses mainly on open-loop cards[11] because closed-loop cards only have a very limited negotiability. This does not mean that the ML/TF risk in closed-loop prepaid cards is very low: in fact, a few case studies involved closed-loop cards. However, in most of these case studies closed-loop cards were not used as a payment instrument, but as a mere intermediary store of value. This can be illustrated by the following two case examples:

Box 3. Stolen credit card information used to purchase closed-loop cards

In 2007, two defendants were prosecuted for purchasing closed-loop prepaid gift cards with stolen credit card account information. The defendants used the gift cards to purchase merchandise, which they then returned to the store in exchange for new gift cards, or they sold the merchandise for cash. Because the new prepaid cards were not linked to the stolen credit card account numbers, they were not affected when the theft of the credit card information was discovered. The defendants were convicted and ordered to pay USD 82 000 in restitution. One defendant was convicted of conspiracy and fraud and sentenced to 45 months imprisonment and three years supervised release. The other defendant was convicted of conspiracy and money laundering and sentenced to five months imprisonment and three years supervised release.

Source: United States.

Box 4. Suspected use of a closed-loop card company for money laundering and terrorist financing

Law enforcement information indicated that the owner of a prepaid phone card company was suspected of money laundering and having links to a terrorist organisation.

The owner conducted many large cash deposits into personal and business bank accounts and when questioned would indicate that prepaid phone cards were sold to retailers and convenience stores, and cash payments were received instead of cheques. This was apparently due to the fact that the owner was not confident that cheques would be honoured.

Some of the deposits were also conducted into accounts held by prepaid phone card suppliers.

Electronic funds transfers were also ordered by the owner to the benefit of individuals in Europe and the Middle East, sometimes through accounts which previously had not seen much activity. The owner was also the beneficiary of funds ordered by the same individuals.

Source: Canada.

34. During the June 2010 FATF plenary in Amsterdam, the plenary asked the project team to provide information regarding the nature and inherent risks of closed-loop prepaid cards.[12] However, beyond the two case examples above, the project team does not have sufficient data to assess the risk of such cards, as the questionnaire circulated at the beginning of the project explicitly excluded closed-loop cards from the scope of this project. Nevertheless several of the risk factors as well as the corresponding

10 For more details see the definition of prepaid cards as given in the FATF 2006 report (included as Appendix B to this report).

11 For the purposes of this report, the term prepaid cards includes the types of cards that were named "e-purses" in the FATF 2006 report.

12 The issue had come up after the mutual evaluation of Brazil; the assessment team had criticised Brazil for applying reduced CDD measures to such cards without having conducted a thorough risk assessment to determine the risk of such products first (FATF (2010)).

risk mitigants evaluated in this report that apply to open-loop cards may also apply to closed-loop cards (*e.g.*, regarding CDD measures or value limits).[13]

35. The overall volume of prepaid card transactions can only be estimated, as in most jurisdictions data on annual transaction volume for prepaid cards is not reported separately by the leading payment card networks, card-issuing banks, or non-bank issuers and service providers.[14] For the US, the total funds loaded onto prepaid cards in 2009 are estimated to have been USD 120.2 billion, according to research commissioned by MasterCard, Inc. and conducted by the Boston Consulting Group (BCG).[15]

36. While about 17% of U.S. consumers have a prepaid card,[16] outside the U.S. the percentage of consumers with a prepaid card tends to be lower and the market potential may be lower as well.[17]

37. Prepaid cards have been introduced in a number of countries, but in most countries the use of prepaid card appears to be less prevalent compared to the US. The BCG study mentioned above (see footnote 21) forecasts that the US will account for 53% of the global prepaid card market in 2017, and that UK and Italy will remain the largest markets for prepaid cards in Europe, with the UK accounting for 25% and Italy 20% of the entire European market by 2017.[18] The BCG study roughly supports a 2009 survey sponsored by the international payments processing firm First Data that found that Italy was the "most advanced prepaid market in Europe," while the UK market was described as "established," and the markets in Germany and Austria were described as "embryonic." [19] As a general trend it is safe to say that the usage and spread of prepaid cards has grown in recent years. According to the Basel Committee on Payment and Settlement Services (CPSS)[20] the number of issued "cards with an

---

13 Based on the discussion during the evaluation of Brazil and the indicators available, it may be worthwhile to analyse the money laundering and terrorist financing vulnerabilities of closed-loop prepaid cards in a separate typologies project.

14 MasterCard and Visa mix prepaid card transaction volume in with their debit card data. For the 12 months ending 30 June 2009, Visa reported 935 billion USD of consumer debit transactions for purchases of goods and services, with just over 84% of that volume taking place in the United States (United States Securities and Exchange Commission (2009a)). For MasterCard, in the year ending 31 December 2009, total debit card transaction volume was $814 billion, with 55% taking place in the United States (United States Securities and Exchange Commission (2009b)).

15 Payment News (2010)

16 Foster K., Meijer E., Schuh S., and Zabek A. (2010).

17 According to United Kingdom-based PSE Consulting: "US prepaid products rely on displacing check wage payments, and often the less well off are obliged to spend c.$50 - $60 per month on 'check cashing', paying their utility bills or sending money home to their families. In Europe the greater prevalence of electronic salary payments and government benefits plus free 'basic banking' products means the unbanked population is significantly smaller than in the US and consumers are unused to paying such high charges." (see: www.pseconsulting.com/pdf/articles/sep06/pse_repaid_press_release_110806.pdf)
This view is supported at least within the UK by the UK Payments Council, which in its new report, The Way We Pay 2010, finds that 89% of workers in the UK are paid by direct deposit to individual bank accounts with the remainder paid by check or cash. The report does not mentions prepaid cards. (Payments Council (2010)).

18 Master Card (2010)

19 First Data (2009)

20 Bank for International Settlements (2009)

e-money function"[21] has grown from 107.6 million in 2004 to 275.28 million in 2008 in selected CPSS countries.[22]

38. The project questionnaire asked jurisdictions for an estimate of prepaid cards issued by domestic payment service providers. Out of those jurisdictions that provided an estimate, the eight jurisdictions with the most cards issued are listed in the following table:

Jurisdiction	Cards issued (estimate)	Jurisdiction	Cards issued (estimate)
Japan	100 million	**Slovak Republic**	4 million
Singapore	15 million	**Mexico**	2.6 million
Italy	8 million	**Russia**	2 million
Norway	6 million	**France**	1.3 million

39. Since the first report was published in 2006, there have been no significant technical developments, most open-loop prepaid cards still rely on magnetic stripes. Where so-called "smart cards" are used featuring an electronic chip, this chip is usually used for processing additional customer information. Prepaid card systems that use the chip to store the funds on the card ("e-purses")[23] are usually still limited to domestic use and often have rather low value limits.

40. As described in the FATF 2006 report, prepaid cards can be an alternative to a variety of traditional banking products and services, such as debit or credit cards or traveller cheques. Many prepaid cards enable customers to make international payments, and some are increasingly offering features similar to conventional bank accounts: such card products may allow the customer not only to make payments, but also to receive payments from third parties. They may also allow cross-border remittances, *e.g.*, by issuing several "twin" or "partner" cards to one customer, which they can pass on to remittance receivers anywhere in the world. These "twin" or "partner" cards grant their holders access to the original card holders´ funds through the global ATM network.[24]

41. Some providers of Internet payment services and mobile payment services are known to provide their customers with an additional prepaid card to facilitate access to cash through the use of ATMs domestically and worldwide. This link was identified for mobile payments in the 2006 report, but has now been associated with IPS as well.

2.2 Recent Developments Related to Internet Payment Services

42. Internet payment services (IPS) can be provided by financial institutions and firms outside the financial services sector. They can rely on a bank account or operate independently from a bank account.

---

21 These are defined as "Reloadable multi-purpose prepaid cards which can be used at the sites of several service providers for a wide range of purposes and which have the potential to be used on a national or an international scale, but may sometimes be restricted to a certain area", Statistics on payment and settlement systems in selected countries – Figures for 2008 (December 2009), p. 312.

22 Statistics on payment and settlement systems in selected countries – Figures for 2008 (December 2009), table 10, p. 262. These figures include data from Belgium, France, Germany, Italy, Japan, Netherlands, Singapore and Switzerland; they do not include Canada, Hong Kong, Sweden, UK and the US ("nav"-data was not available).

23 See definition of e-purses in the FATF 2006 report on NPM, added to this report in Appendix B. For the purposes of this report, e-purses are included in the category "prepaid cards" (also see glossary s.v. "electronic purses").

24 See also: 5.2., *Identification of secondary card holders*, para. 196 ss.

43. Internet payment methods fall into one of three categories:

- Online banking, where credit institutions offer online access to traditional banking services based on an account held at the credit institution in the customer's name. Online banking is outside the scope of this document.
- **Prepaid Internet payment products**, where firms who may not be credit institutions allow customers to send or receive funds through a virtual, prepaid account, accessed via the Internet;
- **Digital currencies**, where customers typically purchase units of digital currencies or precious metals which can either be exchanged between account holders of the same service or exchanged against real currencies and withdrawn.

44. The market for prepaid Internet payment products has diversified and grown steadily since 2006 in parts of the world, possibly as a result of increased Internet usage and acceptance of Internet payments by online merchants. They are also increasingly being used to support person-to-person (p2p) transfers.

45. Recent years have seen the emergence of electronic currencies linked to **virtual worlds**, where users convert real currencies into virtual currencies in order to complete purchases within the virtual world environment. Within that same environment, p2p transfers are often conducted among users (*i.e.*, users sending virtual currencies to fellow users). These virtual currencies are not confined to a particular online game, as they can be traded in the real world and be converted into real currencies.

46. **Cash vouchers** have gained popularity in some markets. These vouchers can be bought anonymously at retailers, petrol stations etc. and are usually sold in units ranging from as low as 10 EUR up to 500 GBP (approx. 750 EUR).[25] Cash vouchers are originally designed for person-to-business (p2b) payments on the Internet, but can also be used for p2p transactions where they are accepted as a funding method by other NPM service providers (*e.g.*, prepaid card issuers or digital currency exchangers), or where they can be used for online gambling.

47. **Internet payment services are increasingly interconnected with different new and traditional payment services**. Funds can now be moved to or from a variety of payment methods, ranging from cash, money remittance businesses (*e.g.*, Western Union), NPMs, bank wire transfers, and credit cards. Furthermore, some IPS providers have started to issue prepaid cards to their customers, thus granting them access to **cash withdrawal through the worldwide ATM networks**.

48. As indicated previously, 15 of the jurisdictions responding to the questionnaire indicated that IPS providers were operating in their respective jurisdiction. Statistics regarding the number of such providers and active client accounts were not consistently provided. However for countries providing such statistics, the estimated number of providers varied between one and 23. As for the estimated number of active IPS accounts, it varied between 45 000 and over 80 million accounts.

---

25 Cash vouchers share some characteristics with prepaid cards and are therefore considered to be prepaid cards by some, rather than IPS. As this report examines all NPMs, it is not necessary to make a final decision whether these should be considered prepaid cards or IPS.

2.3 Recent Developments Related to Mobile Payment Services

49. For the purposes of assessing risks and vulnerabilities it is essential to differentiate between "mobile payments" based on individual bank accounts or securities accounts for each customer (and recipient) held at a financial institution that is subject to adequate AML/CFT regulation and supervision, and those services offered separately from such accounts.[26] In this respect, it may be helpful to use the four categories of mobile payment systems described by the World Bank:[27] [28]

- Mobile financial information services: Users may view personal account data and general financial information, but there is no capability for any financial transaction and therefore may be considered low risk.

- Mobile bank and securities account services: Users may transact, in a similar fashion to internet banking. The service will be tied into individual bank or security accounts and is therefore (like internet banking) not considered a NPM in the strict sense of this report. Mobile bank and securities account services are likely to be regulated and supervised.

- **Mobile payment services**: Allows non-bank and non-securities account holders to make payments with mobile phones. However, payment service providers may be non-traditional financial institutions with widely varying controls and supervision measures.

- **Mobile money services**: Subscribers are able to store actual value on their mobile phone. They may use phone credits or airtime as tender for payment. Such systems offer versatility but may often fall out of regulation and prudential supervision altogether.

50. The scope of this report covers the last two categories only. However, some of the issues discussed in this report may apply for mobile bank and securities account services as well (*e.g.*, the issue of outsourcing business activities or using agents; or simplified due diligence measures; or non-face-to-face account opening).

51. Advances in mobile phone technology since the 2006 report should reasonably have been expected to facilitate a marked increase in the use of mobile payments systems. The expected proliferation of such systems was regarded as symptomatic of the trend for migration from paper to electronic payments common to all payment systems innovations.

52. Despite a predicted marked increase in the use and spread of mobile payments,[29] only a few providers have managed to run a successful and profitable business model[30] in the long term so far.[31]

---

26 These services may as well rely on the involvement of banks; however, in these business models the technical handling of payment transactions does not rely on individual bank accounts for each customer and recipient.

27 World Bank (2008)

28 Other terms and definitions may exist in the mobile payment service market such as "mobile wallets", "mobile money transfer" (indicating person to person payments) or "mobile payment" (indicating person to business, *i.e.*, retail or bill payment). In this report, these definitions are not used in this sense.

29 Estimates varied; it was suggested that 1.4 billion people will use cell phones to remit money domestically and across borders by 2015 (Michael Klein, World Bank (2008)). Other sources suggest that mobile phone transaction services will grow at 68% per year reaching almost USD 250 billion in 2012

53. As indicated previously, 15 of the jurisdictions responding to the questionnaire indicated that mobile payment service providers were operating in their respective jurisdiction. Statistics regarding the number of such providers and active client accounts were not consistently provided; not all responding jurisdictions made a clear distinction between mobile payments in the sense of this report and mobile banking. For countries providing such statistics, the estimated number of providers varied between one and 21 (including mobile banking models). As for the estimated number of active mobile payment service accounts, it varied between 26 000 and 15 million accounts.

54. Technological developments in mobile payment systems have included the fusing with other payment methods, including traditional payment methods as well as other NPMs:

- Some mobile payment service providers offer open-loop prepaid cards that are connected to the accounts of their customers; through this originally domestic providers may offer cross-border services, as this grants customers or third persons who were handed over the prepaid card access to the global ATM network.
- Some providers even allow for ATM withdrawals without the need for a card. Customers can initiate p2p transactions by passing on a certain code to third parties, who can enter the code into an ATM in order to receive the amount of money linked to that specific code.[32]
- Some providers cooperate with traditional money remittance services (*e.g.*, Western Union); the remittance service enables third parties that are not customers of the mobile payment service provider to send or receive to or from a customer, also across borders.

(Arthur D Little (2009)). These estimates do not only refer to mobile payments services in the sense of this report, but also include mobile banking services.

30 This observation only refers to mobile payments business models in the sense of this report, which does not include "bank based" models (*i.e.*, business cooperation models between banks and telecom companies where each customer needs to have an individual bank account).

31 There are several potential reasons for this, including the following: profit margins in mobile payments services are rather small; in order to make profits, a large number of customers and accepting merchants must be acquired; technological and security issues must be overcome to win the trust of customers. Prudential regulation as well as AML/CFT regulation has also been identified as a potential impediment for market success of NPMs in general, and mobile payment service providers in particular (see chapter 5 for more detail).

32 These non-card ATM withdrawals are currently restricted to domestic ATMs in the provider´s jurisdiction, and only to ATMs of the specific cooperating bank.

CHAPTER 3: RISK ASSESSMENT OF NPMS

NPMs: risk vs. opportunity

55. On the one hand NPMs, like all financial services and products, can be abused for ML/TF purposes. Most jurisdictions have therefore subjected NPM service providers to AML/CFT obligations and regulation.

56. On the other hand, where NPM providers are subject to AML/CTF obligations and appropriately supervised for AML/CTF purposes, NPMs can make payment transactions more transparent and help prevent corruption or other abuses. NPMs can shift customers from the unsupervised or even illegal sections of the payments market (*e.g.*, *hawaladars*, underground banking services) into the formal sector. This means that where providers are subject to AML/CTF legislation and supervision, more transactions are monitored and suspicious transactions are identified and reported to a competent authority. Ultimately, this should result in better oversight of payment activities within a jurisdiction.

Box 5.
Example: Afghan police officers and US soldiers in Afghanistan

In May 2002, at the request of the Afghan Government, United Nations Assistance Mission for Afghanistan and the United Nations Development Program established the Law and Order Trust Fund for Afghanistan (LOTFA) to enable the Afghan police to return to work throughout the country with the first priority being the provision of police salaries. Working with the Afghan ministries of the Interior and Finance, and the United States Military Combined Security Transition Command Afghanistan, LOFTA opened more than 62 000 bank accounts for Afghan police officers and facilitated electronic funds transfers to make salary payments. In addition, the UN, Afghan, and U.S. authorities have been using M-paisa, launched in 2008 by the Roshan mobile company, in collaboration with First Micro Finance Bank, to make salary payments through mobile cell phones. Mobile payments were used in order to avoid police officers having to leave their posts to collect their salaries. Using electronic funds transfer rather than cash disbursement also helped to avoid corruption and bribery.*

Source: United States.

* United Nations Development Programme Afghanistan (2009)

57. Contrary to cash, NPMs can provide additional investigative leads for law enforcement agencies. This is because a transaction carried out through a NPM will always generate an electronic record, whereas cash does not. Even where CDD measures are not applied (*i.e.*, where the customer remains anonymous), the electronic record can, in some cases, still provide law enforcement with at least minimal data such as an IP address or the place where a payment was executed or funds withdrawn; this can potentially support the location or identification of a user suspected of money laundering or terrorist financing.[33] [34]

[33] For example, law enforcement might be able to obtain images of a suspect by analysing CCTV (video surveillance) data at point of sale or in locations where the product was used (ATMs, internet cafes etc.).

[34] Critics challenge the usefulness of the electronic traces rendered by anonymous services or products, pointing out that IP-addresses may be forged; or may be from public places such as “hot spots” or internet

58. This report refers to a number of cases where NPMs were used for money laundering purposes where cash or other traditional payment methods could instead have been chosen. It can therefore be assumed that some criminals consider NPMs to be a better option than cash for ML/TF purposes. This especially applies to cases where NPMs are a substitute for bulk cash to carry, or where the non-face to face nature of the business relationship facilitates the use of straw men or fake identities.[35]

NPMs and Terrorist Financing

59. Based on the case material submitted to the project team, this report focuses mainly on money laundering. Where terrorist financing issues are concerned, this will explicitly be noted in the text; otherwise most findings relating to money laundering apply to terrorist financing *mutatis mutandis*.

60. Out of the 33 case studies analysed in this report, only one has an obvious link to terrorist financing (see section 4: "Typologies", ***case 4***).

Common risks of NPMs

61. The 2006 report identified a number of characteristics shared by most NPMs. These include the absence of credit risk, speed of transactions and (often) non- face to face nature of the business relationship:

- Absence of credit risk

  Funds for use with NPMs are generally prepaid. This absence of credit risk means that service providers may have fewer incentives to obtain full and accurate information about the customer and the nature of the business relationship.

- Speed of transactions

  NPM transactions can be carried out and funds withdrawn or converted much quicker than through more traditional channels. This can complicate monitoring and potentially frustrate efforts to freeze the funds.

- Non-face to face business relationship

  Many (but not all) NPM providers' business model relies on non-face to face business relationships and transactions, which FATF Recommendation 8 identifies as presenting "specific"36 ML/TF risks due to increased impersonation fraud risk and the chance that customers may not be who they say they are.

---

cafes; in such cases, the information is of little use to law enforcement in jurisdictions where public and private video surveillance is less prevalent.

35 See *4.4.1, Cross-border transport of prepaid cards* and Chapter 4.2, *Case 20: Use of "ghost employees" to launder illicit funds through prepaid cards* for "cross-border transport of cards and "ghost employees" examples in the typologies sections.

36 If read in conjunction with the Interpretative note to Recommendation 5 (para. 7) and the Basel CDD paper (section 2.2.6, para. 48), "specific" risk appears to mean "higher" risk: "48. In accepting business from non-face-to-face-customers (…) there must be specific and adequate measures to mitigate the higher risk". See also para. 165 ss.

Assessing individual providers and products, not NPMs as such

62. One of the findings of the 2006 report was that ML/TF risks and vulnerabilities varied significantly among service providers and products, even within one and the same category of NPMs such as prepaid cards. This is due to the fact that the different products have different features that will affect their risk profile.

The Risk Matrix

63. The 2006 report developed a risk matrix which featured several risk factors to assess the risk associated with individual NPM products.[37] This matrix has been updated as follows:

- "Identification" has been renamed "CDD" and now encompasses identification, verification and monitoring.
- "Record keeping" has been added as an additional risk factor.
- "Value limits" and "usage limits" have been broken down into more detail; and
- "Segmentation of services" has been integrated into the risk matrix. Segmentation of services had already been identified as a challenge for regulators and law enforcement in the 2006 report, but had not been included in the risk matrix then.

64. Some of the risks (such as anonymity, methods of funding, value limits etc.) are the direct result of product design, while others result from the providers´ CDD measures (such as verification and monitoring procedures).

65. The risk factors listed in the following matrix should not be looked at in isolation but as a whole; a "high risk" rating in one risk factor does not necessarily mean an overall rating of "high risk" for the product. It is important to look at the whole picture not only including all risk factors, but also all risk mitigants implemented in order to effectively assess the risk associated with a particular NPM product.

Box 6.
Example: Risk factor "Usage limits / utility"

The risk matrix considers services that facilitate person-to-person (p2p) payments to be of a higher risk than services that facilitate person-to-business (p2b) payments only. This consideration is based on the fact that the p2p functionality enables a user to transfer funds to a much higher number of potential recipients, and without the need for an underlying purchase or any other "reason" for a transaction.

However, the p2p functionality of an NPM service does not automatically lead to an overall risk assessment of "high risk" for that service. Likewise, NPM services that are restricted to p2b payments cannot automatically be regarded as "low risk" services. Instead, the other risk factors listed in the risk matrix must be taken into account as well (*e.g.:* Are there identification/verification measures? Are there value limits? …)

Payment Methods Risk Factors				
Criteria		Cash	NPM High risk	NPM Low risk
CDD	Identification	anonymous	Anonymous	Customers are identified
	Verification	anonymous	Customer's identity (where obtained) is not verified on	Customer's identity is verified on the basis of reliable,

[37] Other publications on risk assessment have developed different approaches, using different risk factors, which are not adopted here. See for example World Bank Working paper (2008), p. 17 ss.

Payment Methods Risk Factors				
Criteria		**Cash**	**NPM High risk**	**NPM Low risk**
			the basis of reliable, independent source documents, data or information (*cf.* Recommendation 5)	independent source documents, data or information (*cf.* Recommendation 5)
	Monitoring	none	None	Ongoing Monitoring of business relationships
Record keeping		none	Electronic transaction records are generated, but not retained or not made accessible to LEA upon request	Electronic transaction records are retained and made accessible to LEA upon request
Value Limits	Max. amount stored on account / accounts per person	no limit	no limit	Amount limit (cf. para. 112 ss.)
	Max. amount per transaction (incl. loading / withdrawal transactions)	no limit	no limit	Amount limit (cf. para. 112 ss.)
	Max. transaction frequency	no limit	no limit	Transaction limit (cf. para. 112 ss.)
Methods of funding		n.a.	Anonymous funding sources (*e.g.,* cash, money orders, anonymous NPMs); also multiple sources of funds, *e.g.,* third parties	Funding through accounts held at a regulated financial or credit institution, or other identified sources which are subject to adequate AML/CTF obligations and oversight
Geographical limits		Some currencies are accepted more widely than others; currencies can be converted through intermediaries	Transfer of funds or withdrawal across national borders	Transfer of funds or withdrawal only domestically
Usage Limits	Negotiability (merchant acceptance)	Generally accepted	High number of accepting merchants / POS (*e.g.,* through usage of VISA or MasterCard standard)	Few accepting merchants / POS
	Utility	p2b, b2b, p2p, no online usage possible	p2b, b2b, p2p, online usage possible	p2b, b2b, online usage possible, but no p2p
	withdrawal)	n.a.	Anonymous and unlimited withdrawal (*e.g.,* cash through ATMs)	limited withdrawal options (*e.g.,* onto referenced accounts only); limited withdrawal amounts and frequency (*e.g.,* less than a certain fixed sum per calendar year)
Segmentation of services	Interaction of service providers	n.a.	Several independent service providers carrying out individual steps of the transaction without effective oversight and coordination	Whole transaction carried out by one service provider
	Outsourcing	n.a	Several singular steps are outsourced; outsourcing into other jurisdictions without appropriate safeguards; lack of oversight and clear lines of responsibility	All processes completed in-house to a high standard

66. Some types of NPMs are more affected by certain risk factors than others, but most risk factors apply to all types of NPMs to a certain degree. The following discussion of **risk factors (section 3.1)** will therefore be presented in a consolidated section for all NPMs together.

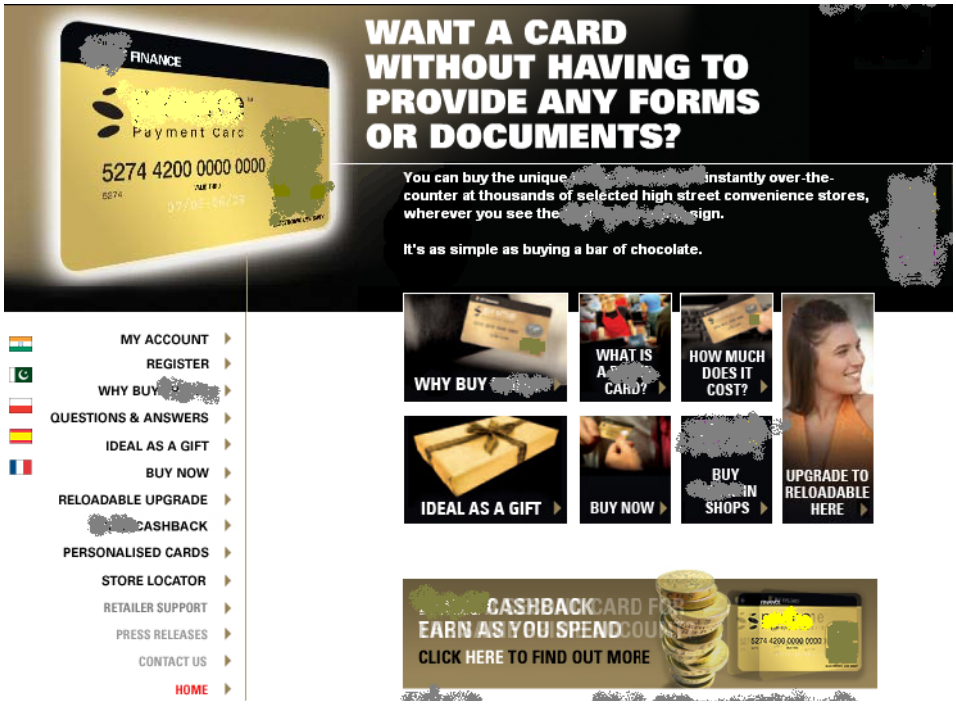
67. The ML/TF risks associated with NPMs can effectively be mitigated by firms' own AML/CTF policies and procedures and regulatory oversight. Like risk factors, the **risk mitigants** appear to be similar for all types of NPMs and are therefore presented in a consolidated **section 3.2.**

3.1 Risk factors

Customer Due Diligence

68. **Prepaid cards** can be designed to afford the customer absolute anonymity while maintaining a high degree of functionality. For example, some prepaid card issuers attract customers with anonymous prepaid cards with no or high loading and transaction limits.

Figure 1. Example of a prepaid card



Source: Internet screenshot July 2010

69. Prepaid cards can also easily be passed on to anonymous third parties who in some cases will be the beneficial owner. Where additional "twin cards" or "partner cards" are issued that are specifically designed and advertised for being passed on to third parties to allow remittances, these third parties/beneficial owners are often not identified. This emphasizes the significance of identifying at least the primary account holder /card holder.[38]

[38] There is always the potential for any payment card (including traditional debit or credit cards) to be shared with third parties who remain anonymous to the card issuing institution; but if the institution has adequately identified the primary card holder, law enforcement has a point of contact to associate with reports of suspicious transactions.

70. For many NPM providers, customer contact is often minimal as a result of business relationships being conducted on a non-face to face basis. As recognised by FATF Recommendation 8, this increases risks like identity fraud, impersonation fraud or the use of the product by third parties for illicit purposes. Absence of face to face contact is particularly common among **IPS providers** who generally conduct most of their business activities online. It may also be relevant for other types of NPMs (*e.g.*, online purchase of prepaid cards).

71. Most IPS providers ask for their customers´ names, but the levels of customer verification vary significantly, ranging from no verification at all (some providers only require a pseudonym) to sophisticated verification measures (see section 3.2 "risk mitigants").

72. The verification of the customers´ identity may be further hampered or impossible in jurisdictions that have no national identity card scheme, or other appropriate alternative forms of identification; this is a challenge often encountered by NPM providers operating in underbanked regions, especially **mobile payment services providers**. For this reason, the World Bank has recommended to jurisdictions intending to promote financial inclusion (*e.g.*, through mobile payment service providers) that if the jurisdiction´s "national identification infrastructure and other private databases lack coverage, integrity, or are not easily and cost-effectively accessible to financial institutions for verification purposes, the state should address these deficiencies".[39] Where customer data cannot be reliably verified, it may be appropriate to apply alternative risk mitigation measures (*e.g.*, imposing low value limits in order to qualify as a "low risk" product and be allowed to apply simplified CDD measures; see also below section 3.2, "value limits" as a risk mitigant (para. 112 ss.).

73. Where no identification or verification based on reliable and independent sources takes place, NPM providers run the risk of customers' holding multiple accounts simultaneously without the provider noticing.

Record keeping

74. According to FATF Recommendation 10, both identification data as well as transaction records should be maintained for at least five years. Transaction records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. While neither Recommendation 10 nor the Interpretative Note to Recommendation 10 provides a definition of the term "transaction records", examples of necessary transaction records are provided by the FATF Methodology (10.1.1):

> *"Examples of the necessary components of transaction records include: customer´s (and beneficiary´s) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction."*

75. These examples do not explicitly list the IP addresses of customers initiating a payment transaction through a personal computer. Only in a few cases have jurisdictions, regulators or industry have issued guidance that it can be advisable to do so.[40]

---

39 World Bank (2009a), Annex 1 (A 1.1), p. 173 ss.; these World Bank recommendations are based on and quoted from: Bester, H., D. Chanberlain, L. de Koker, C. Hougaard, R. Short, A. Smith and R. Walker (2008), p. xi,; p. 39, 40.

40 For example, the *UK JMLSG Guidance (2007)* Part II Sector 3, explains how IP addresses can form part of a customer´s identity.

76. Law enforcement agencies have reported investigative cases where providers had not kept record of IP addresses at all, or not sufficiently, or had already deleted them before law enforcement agencies could access them. The increased ML/TF risk with providers that have no robust record keeping policy regarding all relevant transaction data lies in the fact that weak record keeping impedes criminal prosecution.

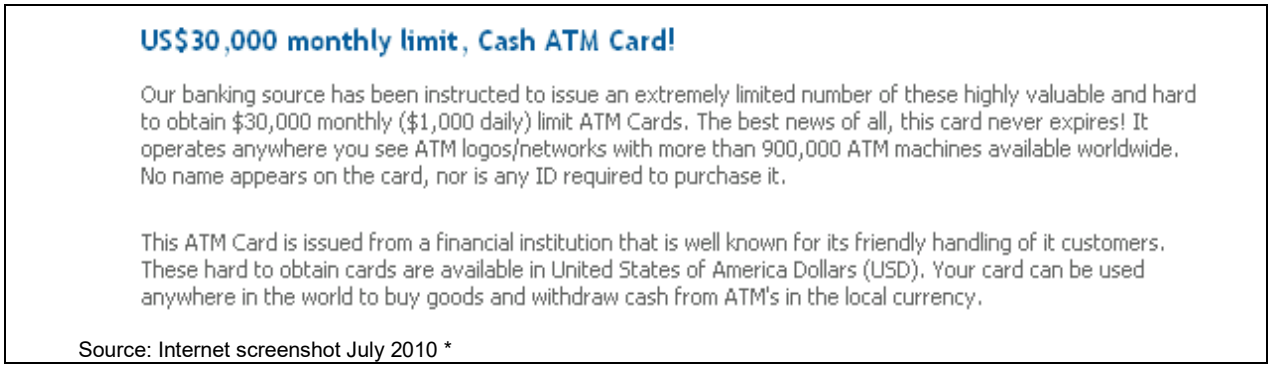
Value limits

77. The term "value limits" refers to limitations on the maximum amount that can be held in a NPM account or product; or limitations on the maximum amount per single payment transaction; or limitations on the frequency or cumulative value of permitted transactions per day/week /month/ year; or a combination of the aforementioned limitations. Also the number of accounts or cards allowed per customer can be considered a type of value limit.

78. Where value and transaction limits are not imposed, the availability of funds is limited only by the amount loaded onto the account. This increases the product's appeal to would-be money launderers and consequently the ML/TF risk the product is exposed to.

79. The higher the value and/or frequency of transactions, the greater the money laundering and terrorist financing risk. Similarly, high, or no, account limits increase the risk as well.

80. Most **Mobile payment service providers** impose rather low (*i.e.*, strict) value limits on their products, whereas a wide variety of approaches can be found for **Internet payments services and prepaid cards providers.** For example, prepaid cards may be designed as a non-reloadable card with a rather low account cap (such as USD 100); on the other hand, there are reloadable cards with no or rather high account caps such as USD 30 000 per month.



US$30,000 monthly limit, Cash ATM Card!

Our banking source has been instructed to issue an extremely limited number of these highly valuable and hard to obtain $30,000 monthly ($1,000 daily) limit ATM Cards. The best news of all, this card never expires! It operates anywhere you see ATM logos/networks with more than 900,000 ATM machines available worldwide. No name appears on the card, nor is any ID required to purchase it.

This ATM Card is issued from a financial institution that is well known for its friendly handling of it customers. These hard to obtain cards are available in United States of America Dollars (USD). Your card can be used anywhere in the world to buy goods and withdraw cash from ATM's in the local currency.

Source: Internet screenshot July 2010 *

* As mentioned above, some offers of anonymous prepaid cards are fraud. The project team did not investigate whether the product advertised by this screenshot is fraudulent or not.

81. Providers of products with high or no value limits are often based in jurisdictions where NPM providers are not or insufficiently regulated and supervised for AML/CTF purposes, but sell their product internationally (through agents or over the Internet). However, such providers of anonymous prepaid cards with high or no limits have also been found to operate in jurisdictions whose regulatory regimes and supervision are generally considered robust.[41] Such anonymous cards are often not promoted by the issuing institution itself, but by intermediaries some of which have specialised in founding and selling companies abroad, preferably in tax havens, thus providing a complete "privacy

[41] In 2007, the German *Bundeskriminalamt* (BKA) conducted a special investigation on payment cards; during that investigation, the BKA detected six cases of anonymous prepaid cards sold via the internet; the issuing banks were located in Europe and Central America.

package" to their customers. Some of those anonymous prepaid cards however have been discovered to be fraudulent.

82. Value limits may be linked to the product´s CDD requirements (*i.e.*, strict limits where the level of CDD measures is low, and higher or no limits where the level of CDD measures is high; see also below section 3.2 "risk mitigants", value limits).

Methods of funding

83. NPMs can be funded in different ways - including anonymously through sources such as cash, money orders or funds transfers from other anonymous NPM products. Anonymous funding methods may result in no or insufficient paper trails regarding the funding transaction and the origin of the funds.

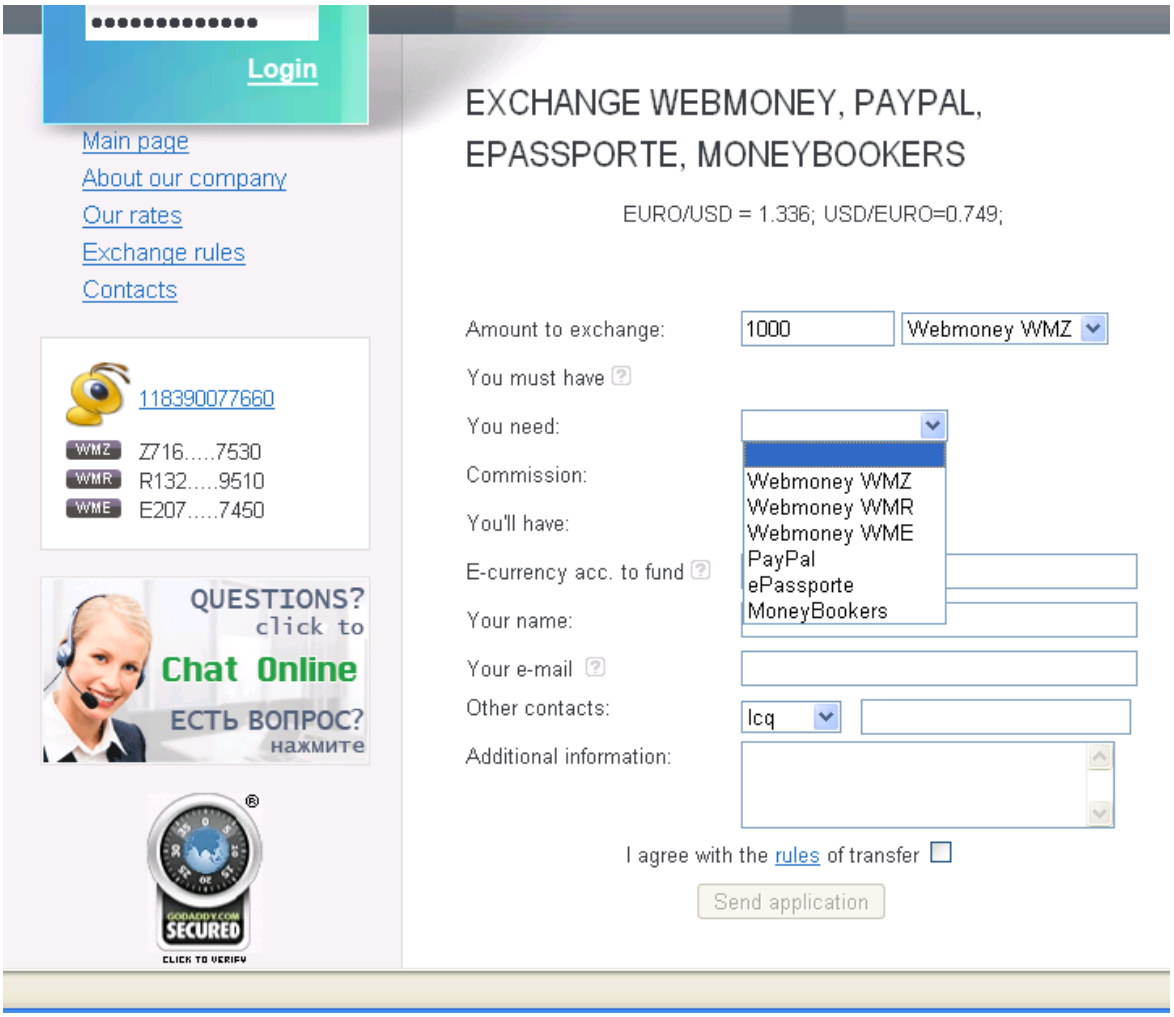
84. Cash funding is especially popular with NPM providers that sell pre-funded products through distribution agents (*e.g.*, prepaid cards and cash vouchers sold by retailers, or mobile prepaid funds sold by phone shops.)[42] Cash funding through distribution agents can increase ML/TF risk, especially where the distributing staff have no CDD obligations and/or no sufficient training in AML/CFT compliance.

85. Other than funding through anonymous sources, the ML/TF risk will increase where the funds can stem from different sources, including third parties. For example, where there is a co-operation with money remittance businesses, these may be used to not only fund the customer's own personal account, but also to fund the account of third persons.

86. As most IPS and mobile payment services are account-based, another possibility of "indirect funding" arises when the service provider allows for person-to-person (p2p) transactions within the system. In such cases the provider's funding restrictions may be circumvented by funding an account in cash through a digital currency exchanger (or other third parties), who will then transfer the funds into the customer´s account.

[42] In under-banked regions where few customers have bank accounts, and where the NPM service (often mobile payment services) is supposed to substitute for the lack of bank accounts, there may be few alternatives to cash funding.

Figure 2. Example of online exchange of currency



Source: Internet screenshot May 2010.

87. As different NPM providers have different funding and withdrawal methods, exchangers enable customers to circumvent these procedures by simply converting the funds into a more suitable provider's currency.

Geographical limits

88. The wider the geographical reach of a NPM product, the higher the ML/TF risk will be. Cross-border functionality renders a service more attractive to launderers; it also enables payment service providers to conduct their business from jurisdictions where they may not be subject to adequate AML regulation and supervision, and where they may be outside the reach of foreign law enforcement investigations.

89. While many payment service providers who offer cross-border services may cooperate well with their domestic supervisors and law enforcement agencies, some providers may refuse to provide information to foreign agencies or may face legal obstacles for doing so. Formal legal assistance requests can be very time-consuming and often have only little chance of success. As a result, some agencies may refrain from requesting legal assistance and close the investigation instead. This

phenomenon is exacerbated if the service is provided by several providers interactively who are located in several different jurisdictions (see "segmentation of services", para. 96 ss.).

90. Open-loop prepaid cards can be used to quickly move cash around the world by using the ATM network to withdraw funds, with no face-to-face transaction required. The global network providers (VISA, MasterCard) can limit the use of prepaid cards to certain jurisdictions or regions, but most open-loop prepaid card business models are designed to function globally. Although the ATM network was not designed to be used as a person-to-person money transmission system, it is now also being marketed as one.

Figure 3. Example of internet transfer

Source: Internet screenshot August 2010.

91. Internet payment services providers can be headquartered or licensed in a jurisdiction different from where the customer is located, and because IPS can use a variety of funds transfer methods, payments can potentially be initiated and received from anywhere in the world. Most IPS providers offer their services globally, thus facilitating cross-border transactions.

92. Most mobile payment service providers were originally designed for domestic transactions only. An increasing number of providers offer the possibility to effect cross-border payments between specific countries, opening so-called payment corridors (*e.g.*, from the UK to Kenya, or Philippines to Malaysia). While there have been attempts to implement multinational business models for mobile payments, currently there still is no truly global mobile payment service provider yet.

93. However, some mobile payment service providers have extended their outreach by connecting with the global ATM network (by providing their customers with prepaid cards) or by cooperating with

global money remittance businesses. Through this, an originally domestic service provider can effectively carry out cross-border transactions into and out of its original jurisdiction.

Usage limits

94. The usage limits for NPM products can differ by product and by service provider. NPM products with limited functionality are exposed to fewer AML/CFT risks than those that allow customers to use the product more widely.

95. Open-loop prepaid cards, especially when they are based on a well established and widespread technical standard (VISA, MasterCard) generally have the least usage limits, as they can rely on an existing extensive infrastructure for payment transactions, including the global ATM network and a very high number of accepting merchants / point-of-sale (POS).

- Negotiability(merchant acceptance)

  Visa and MasterCard branded prepaid cards are accepted by domestic and foreign merchants that are part of VISA or MasterCard's payment networks. As the standards used for prepaid card payments typically are largely identical[43] with those of regular debit or credit card payments, such prepaid cards are accepted as a means of payment almost everywhere where a credit card would be accepted for payment (as long as the prepaid funds are sufficient for the intended payment), including online shops.

  When using IPS and mobile payment services providers, payment transactions can often only be carried out between customers of the same IPS provider. Payments services that are widely accepted will be more attractive to money launderers than those that allow funds to be spent with a limited range of merchants only.

  In some markets, mobile payments services are used exclusively for micropayments (*e.g.*, mass transport tickets, vending machines, and ringtones); the number of accepting merchants is limited. In other markets where mobile payment services may be used as a substitute for bank accounts and wire transfers, the negotiability is often much higher, resulting in greater risk.

- Utility

  In order to carry out a classic prepaid card payment, the receiver/payee needs to have the necessary technical equipment (card reader, online access to system). Therefore, most card payment receivers are businesses (p2b-payments). However, where prepaid cards are designed to receive payments / funds from external sources, or where the cards or specific partner cards can be passed on to third parties or used to fund other NPM accounts, p2p payments are also facilitated.

  Most IPS and mobile payment services feature p2p-payments, but some are designed to facilitate p2b payments for underlying shopping transactions only (*e.g.*, cash vouchers), which generally decreases the ML/TF risk. However, where "merchants"[44] accepting such payments

---

43 There are controls that countries or institutions can apply that prevent cards from being used for certain purchases; or in ATM machines; or that limit the transaction value etc. Because of this, the functionality of prepaid cards can vary and does not necessarily equal that of credit cards.

44 Which is a wider term and encompasses more than the classic online shop.

are being used for financial services provision (*e.g.*, money transmission service accepting these payment methods as a funding method) or criminal purposes (*e.g.*, illicit online gambling providers accepting this payment method), the ML/TF risk remains high.

- Funds withdrawal

  Cash can be withdrawn from many open-loop prepaid cards via the ATM networks. In addition, in several jurisdictions merchant points of sale may be easily used to withdraw cash by overpaying purchased merchandise and receiving the overpaid amount in cash ("cash back").[45] Easy cash access and high negotiability, coupled with the fact that prepaid cards[46] are much easier to transport than bulk cash (an ISO standard financial transaction card can be considerably more compact than currency[47]), may make prepaid cards a convenient substitute for cash in bulk cash smuggling ML schemes,[48] assuming a high account limit and/ or no verification of customer identification.

  Most IPS and mobile payment services providers restrict the possibility of redeeming money in the same way they restrict the funding methods. For example, redemption of funds may be restricted to a transfer of funds into an account held in the customer's name at a credit or financial institution.

  Where cash is used as a method of funding, it is usually also possible to withdraw cash from the mobile payment account, *i.e.*, through agents. This not only increases the ML/TF risk, but may also create additional challenges for the mobile payment service provider. For example, there have been reports about fraudulent agents, or problems with the cash supply for requested withdrawals.

  Providers may facilitate cash payouts through cooperation with money remittance businesses or brick-and-mortar exchangers that will trade electronic funds for cash. Some IPS and mobile payment providers also offer to load the funds onto a prepaid card, thus granting their customers access to cash withdrawal through the worldwide ATM network. One mobile payment provider (in cooperation with a domestically operating bank) even enables access to the cooperating bank´s ATMs without the customer needing to have a bank account or a prepaid card: upon request, the customer is provided with a one-time authorisation code which he (or a third party) can enter into the ATM, together with the customers phone number and the amount he wishes to withdraw.[49]

Segmentation of services

96. NPMs can be more exposed to risks where several parties are involved in performing the payment service jointly, such as card issuers, program managers, exchangers, distributors and other

---

45 This "cash back" method of withdrawing funds has originally been developed for and is commonly applied with regular credit or debit cards.

46 The card often acts as an access device to withdraw the funds and initiate payments.

47 The volume of an ISO standard "financial transaction card" is 3 525.8 cubic millimetres. The volume of a 20 EUR note is 1 435.6 cubic millimetres. The volume of a 20 USD bill is 1 129 cubic millimetres. Thus, a payment card with access to just 100 EUR or 100 USD is already considerably more compact than five 20 EUR notes or five 20 USD bills.

48 See *4.4.1. Cross-border transport prepaid cards.*

49 *Cf.* Finextra (2010).

types of intermediaries or agents. The number of these parties generates potential risks of segmentation and loss of information. This may be exacerbated if important services are outsourced to potentially unregulated third parties without clear lines of accountability and oversight, or which are located abroad. Payment schemes with a high degree of segmentation may raise issues for supervisors in terms of competences, international cooperation, powers and means to supervise and to safeguard them effectively.

97. Providers often use **agents** not only for cash acceptance and cash withdrawals, but also to establish new customer relationships. In most jurisdictions agents who are not credit or financial institutions are not themselves subject to AML/CFT obligations. The legal and regulatory responsibilities for complying with relevant AMLCFT legislation or regulation remain with the NPM provider. This means that the NPM provider will be liable for any failure by the agent to meet the provider´s AML/CFT obligations on its behalf ("agent's risk").[50] The provider therefore has to be satisfied that the agent carries out their function effectively. Given the vast number of agents that some providers have to rely on (*e.g.*, hundreds of branches of a big retailer), this may be difficult – even more so where agents are based in a foreign jurisdiction, or potentially, where the agent makes use of further agents ("sub-agents").[51]

98. Where a provider cooperates with money remittance businesses, these are generally used to accept cash for funding and/or pay out cash for withdrawals. This can to some extent add an additional level of AML/CFT compliance, as in most jurisdictions money service remitters are subject to AML/CFT regulation and supervision themselves. However, the regulatory requirements may be different: for the money service businesses, the customer´s transaction usually being a one-off transaction, whereas for the NPM provider the transaction is part of an ongoing customer relationship. Furthermore, the risk may increase if the cooperating money remittance business is located in a jurisdiction that does not enforce equivalent AML/CFT standards.

99. A special phenomenon of segmentation of services is associated with a certain type of IPS, so-called digital currency providers (DCP), which use "exchangers" as an integral part of the payment transaction chain. DCP do not directly issue their "digital currency" to their customers / account holders, and as a consequence do not receive an equivalent incoming flow of money from their customers. Instead, customers have to purchase their digital currency from exchangers, who will then transfer the purchased amount of digital currency into the customers DCP account. Some exchangers are subsidiaries of DCP, but many are legally independent businesses or natural persons. Exchangers may be brick-and-mortar businesses (*i.e.*, exchanging cash and other traditional payment methods for digital currency and vice versa) or pure online businesses (exchanging electronically transferred money for digital currencies, or exchanging digital currencies for other digital currencies or IPS funds).

3.2 Risk mitigants

100. Like any financial product, the AML/CTF risk associated with NPMs is high in the absence of appropriate safeguards. However, there are effective risk mitigants that can significantly reduce the identified risks.

---

50 The term "agents risk" comes from the FATF paper "*Risk Based Approach: Guidance for Money Service Businesses*", FATF (2009a), pages 32 ss.

51 While this phenomenon of sub-agents has not yet been observed with NPM service providers, it has become apparent in the latest typologies report on money service businesses.

101. The following risk mitigants should not be looked at separately but as a whole; some of them are intertwined or affect more than just one specific risk factor. It is important to look at the whole picture including all risk factors and all risk mitigants in order to effectively assess the risk associated with a particular NPM product.

Identification and verification measures

102. Identification and verification measures allow firms to understand who their customer and, where relevant, the beneficial owner is. This is important in that this information forms the basis for ongoing monitoring of the business relationship. It also allows firms to verify that the customer is who they claim to be, identify whether a customer is associated with multiple accounts (or cards; or cash vouchers), and create a paper trail for law enforcement.

103. For products and services that rely on the internet, the internet protocol address (IP-address) should be part of the identification data collected and retained by the provider. The IP-address can help minimise the potential for a customer to access multiple accounts, even if those are anonymous.

104. Some jurisdictions exempt providers from applying customer due diligence measures where the ML/TF risk is considered very low. Sometimes, these exemptions are conditional on the imposition of low value and transaction thresholds. Some jurisdictions also allow NPM providers to benefit from a one-off transaction exemption from CDD. In those situations, it is important that institutions have systems in place to detect if a customer holds multiple cards or accounts, which can be an indicator for a customer circumventing the CDD procedures by structuring the funds into several "low risk" products.

105. Where verification takes place on a non-face to face basis, it is important that firms employ anti-impersonation fraud checks to be satisfied that their customer is who they claim to be. Anti-impersonation checks include, but are not limited to: correspondence with the customer at their verified home address; requiring the first payment to be carried out through an account in the customer's name with a regulated credit institution from a FATF-equivalent jurisdiction; and requiring copy documents to be certified by an appropriate person.[52] Accompanying anti-fraud checks, such as using dynamic codes which change with each single transaction or access to an IPS, or checking of biometric data (such as fingerprint and voice recognition systems),[53] can add to the AML policies of a provider and help prevent a single customer from opening multiple accounts unnoticed.

106. Where a payment service provider uses third parties to establish customer contact and to accept and pay out cash (*e.g.*, retailers or money remittance businesses), firms can mitigate risk by ensuring that these are appropriately trained and qualified in AML/CFT compliance, preferably subject to regulation and supervision themselves in a jurisdiction with equivalent AML/CFT regulatory standards.

107. Where NPMs can be used for p2p remittances, providers can mitigate risk by ensuring that the recipient of the payment does not remain anonymous and that safeguards are put in place, which are similar to those expected from firms executing wire transfers.

---

52 Basel Committee on Banking Supervision (2001), section 2.2.6; Joint Money Laundering Steering Group Guidance (2010), Part I Chapter V;

53 *Cf.* World Bank (2009b)

Monitoring

108. NPMs are based on computer technology and therefore provide good prerequisites for effective monitoring and reporting procedures. Transactions carried out through NPM services always leave electronic footprints which can be monitored and analysed, even where NPMs benefit from exemptions from customer due diligence (*i.e.*, the customer remains anonymous). This means that providers can block accounts where they detect abnormal transaction patterns or otherwise become suspicious that their product might be abused for ML/TF purposes.

109. Monitoring systems can be a very effective tool to mitigate an NPM product's financial crime risk.

To be effective, such systems must at a minimum allow the provider to identify:

- Discrepancies, for example between submitted customer information and the IP address.
- Unusual or suspicious transactions.
- Cases where the same account is used by multiple users.
- Cases where the same user opens multiple accounts.
- Cases where several products are funded by the same source.

110. Where products benefit from customer due diligence exemptions, systems should detect where a customer approaches a limit (on one product/transaction or cumulatively) beyond which full customer due diligence has to be applied.

111. Effective monitoring systems are also the basis for effective reporting of obligated NPM providers.

Value limits

112. Account balance and transaction limits as well as restrictions in the frequency of transactions may prevent criminals from having continuous access to large amounts of money for illicit purposes. Applying a risk-based approach, value limits can be tailored to reflect the needs and risks attached to each market segment and NPM product. For example, there may be effectively no transaction limits when the service is linked to a fully identified and verified bank or credit card account, but a reduced transaction limit or service where there is a reduced ID requirement.

113. Where NPM providers are subject to AML/CFT regulation and supervision, in application of a risk-based approach their products often do not require the full application of customer verification measures ("simplified CDD" or "reduced CDD"), ranging from reduced normal CDD to total exemptions from the CDD requirements. [54] Value limits are often a decisive factor whether a product can be considered to be of "low risk" and therefore apply for simplified CDD or not.

114. Value and transaction limits can be a very powerful risk mitigant as they render a product less attractive to money launderers, especially when coupled with effective monitoring systems and procedures that prevent multiple purchases of low-value cards or multiple low-value accounts for a

[54] See *5.2, Exemptions from AML obligations.*

single customer. For example, the restrictive value limits implemented by most mobile payment service providers are thought to be one of the main reasons that so few ML case studies involving mobile payments have been detected so far.

115. One of the challenges for applying value limits is to define an appropriate threshold which can be considered low risk. Different jurisdictions and service providers have come to different conclusions as to what thresholds they consider to be "low risk".[55] Furthermore, low transaction amounts that may deter Money launderers might still be attractive for the purpose of terrorist financing, which is generally thought to involve much smaller amounts than ML.

Methods of funding

116. The ML risk associated with anonymous funding methods can be mitigated by restricting funding methods to sources where providers can rely on another institution´s CDD measures, such as previously identified bank accounts, credit or debit cards or other personalised payment methods.[56] While excluding cash or other anonymous sources as a funding method significantly reduces risk, it may not be feasible in such markets where NPM service providers are the only access to the financial system for a good part of the under-banked population (*e.g.*, mobile payment services in jurisdictions with weak banking infrastructure).

117. Issuers with restricted funding methods should be in a position to detect indirect funding through third parties (*e.g.*, exchangers) by attentive monitoring. They can further reduce ML/TF risk by not only restricting the funding method, but also restricting the number of parties allowed to fund the product (*e.g.*, regarding cards: the cardholder alone, or the employer in the case of payroll cards), thus limiting the possibility of third party funding.

---

55 See 5.2, *The definition of low risk cases*, para. 161.

56 This does not constitute reliance as per FATF Recommendation 9, and is unlikely, by itself, to satisfy Recommendation 5´s requirement for using a reliable and independent source to verify a customer´s ID.

CHAPTER 4: TYPOLOGIES AND CASE STUDIES

118. In 2006 when the FATF New Payment Methods report was released, the potential for the misuse of NPMs was already apparent. However, at that time there was little evidence to support this. Since then, both the availability and adoption of NPMs have grown significantly as has evidence of misuse (especially with prepaid cards and IPS), as demonstrated by the following case studies. It should be noted that most case studies concern money laundering and there are only a few isolated cases with suspected links to terrorist financing, even though NPMs have been identified as being vulnerable to terrorist financing.[57]

119. The case studies demonstrate the following typologies: *1)* Third party funding (including strawmen and nominees); *2)* Exploitation of the non-face-to-face nature of many NPM accounts; and *3)* Complicit NPM providers or their employees. The typologies are presented in an order based on whether or not all NPMs, or two of them or at least one NPM has been used in such a way.

120. The project team came to the conclusion that it was not appropriate to present a fourth typology on "anonymity". While many case studies involved taking advantage of the possibility of remaining anonymous, only three cases (***cases 8,10 and 31***) involved NPM products that provided "direct" anonymity, *i.e.*, the product did not require ID/VER at all. Numerous other cases that involved products that may provide "indirect" anonymity, are dispersed over the other three typologies identified (*e.g.*, strawmen, stolen or fake customer data or online data manipulation). "Anonymity" as such may be a general and overarching issue with NPMs, but it is too vague to construct a separate typology.

4.1 Typology 1: Third party funding (including straw men and nominees)

121. NPM accounts can be funded anonymously where the specific business model permits.

122. Prepaid cards can be funded by cash, bank transfers, and person-to-person (p2p) transfers. Customers of most IPS providers can also conduct p2p transfers. These funding methods may allow complicit third parties to fund the prepaid cards or the IPS accounts willingly (*e.g.*, by paying for the sale of illicit merchandise or for gambling, refer to ***cases 1-3, 6***),[58] or may be used by fraudsters to get funds from unwilling victims of their illegal activities. In such cases the distinction between the predicate offence and the subsequent placement phase of money laundering may be difficult. Nine case studies illustrate how prepaid cards and IPS accounts can be funded through third parties for the purpose of money laundering.

123. Similar to IPS providers and prepaid cards, mobile payment services allow third-party funding which can be exploited by criminals. In three cases, criminals used the p2p payment feature of a mobile payment service provider to fund their accounts. In all cases, the third parties were defrauded or tricked

---

57 UN Counter-Terrorism Implementation Task Force (2009), p. 14; also confer World Bank (2009b).

58 EUROJUST has also indicated that NPM are often used to buy or sell child obscenity/child pornography images online to avoid attention from public authorities. Presently the EFC (European Financial Coalition against the Commercial Sexual Exploitation of Children Online) is in contact with a certain number of such NPM providers.

into sending money to the criminals, making the use of the mobile payment service provider also part of the predicate offence. It should be noted that the amounts involved in these cases were small.

124. There is also evidence that even robust identification and verification requirements can be circumvented by the use of third parties such as straw men or financial agents/financial mules.

a. Prepaid Cards:

Case 1: Laundering of proceeds gained through illegal online steroid sales

In 2007, there were three cases with a total of seven defendants who were charged with selling athletic performance enhancing drugs, such as human growth hormone and anabolic steroids, illegally online and laundering the proceeds. All three cases involved loading the defendants' prepaid cards as an optional payment method for completing the online sale of the illegal substances. In one case, the defendant earned USD 60 000 in 11 months from his online steroid business. In another case, the defendant laundered about USD 125 000 in 21 months using prepaid cards. All three cases were resolved with guilty pleas. Defendants received prison sentences.

Source: United States.

Case 2: Laundering of illegal gambling proceeds through prepaid cards

In 2007, a number of defendants were charged with facilitating illegal gambling. The organisation involved onshore agents in the United States who recruited gamblers, collected losses, and distributed winnings, and an offshore organisation that operated an Internet site that processed bets and set odds.

Among the methods used to transfer the illicit gambling proceeds between the onshore agents and offshore organisers was to open and load U.S. prepaid card accounts and then send the card information (card number, expiration date and card verification value) to the website operators. The cards themselves were not sent out of the country. Instead, the offshore organisers would use the card accounts to make online or phone-based purchases. The online gambling operation earned about USD 100 000 a month.

Six defendants pleaded guilty to illegal gambling and were sentenced to three years probation. One defendant pleaded guilty to illegal gambling and money laundering and was sentenced to three years probation and six months home confinement. One defendant pleaded guilty to conspiracy and was sentenced to four years probation. One defendant pleaded guilty to bulk cash smuggling and was sentenced to four months imprisonment and three years probation.

Source: United States.

Case 3: Payment for drugs using prepaid cards

In 2009, a number of defendants were charged with running a drug trafficking ring in a federal prison and receiving payment outside the prison through prepaid cards. Gang members outside the prison allegedly established prepaid card accounts in the name of the defendants, who allegedly instructed their customers — their fellow prisoners — to pay for the drugs by having family members outside the prison deposit payments into the defendants' prepaid card accounts. The defendants have not yet gone to trial.

Source: United States.

Case 4: Possible use of prepaid cards for terrorist financing purposes

In a particular case, a father and his son, suspected to be operating as money remitters, held numerous prepaid cards which were charged daily from all over Italy. Shortly after, the sums were withdrawn so as the cards accounts' balances were almost always near to zero. A portion of the sums withdrawn from the prepaid cards was transferred to a bank account held by the father; funds were also credited to the same bank account from Pakistanis. The funds on the account were further used to order credit transfers. Both persons were found to be involved in the terrorist attacks which occurred in Mumbai in 2008.

Source: Italy.

Case 5: Prepaid cards used to launder drug proceeds

Following the dissemination of Suspicious Transaction Reports (SUSTRs) received by AUSTRAC to a law enforcement agency, an AUSTRAC alert was raised on a suspect and his associate. The information related to a student who on a number of occasions loaded structured amounts of AUD 9 900 to avoid reporting thresholds onto prepaid debit cards in his own name and that of his associate (i.e., conducting third-party loading transactions). The suspect had previously come to the notice of law enforcement agencies in relation to a cocaine seizure which he was alleged to have organised. Following further research and intelligence gathering a joint operation commenced involving multiple law enforcement agencies.

A further 15 SUSTRs were recorded on the AUSTRAC database, showing both the suspect and his associate conducting deposits of structured amounts onto prepaid debit cards. AUSTRAC information detected a further series of financial transactions linked to both targets. An assessment of AUSTRAC information was disseminated to the law enforcement agencies and assisted the investigation, resulting in the arrest of both targets. The associate departed Australia for South America and returned to Australia from another South American destination 12 days later with approximately 5.8 kilograms of cocaine in his baggage. He later admitted that he had previously brought drugs into Australia on two occasions for a payment of AUD 28 000 each time. He was arrested and charged with importing and possessing a prohibited import. The suspect was also charged with conspiracy to bring into Australia approximately 5.8 kilograms of cocaine, structuring and money laundering of almost AUD 400 000. He was found guilty and sentenced to seven years imprisonment.

Source: Australia.

b. Internet Payment Services:

Case 6: Use of IPS to move illicit proceeds gained through the sale of forbidden racist propaganda

In at least two proceedings regarding the illegal distribution of right wing propaganda music CDs, an IPS provider played a decisive role.

The service was used to effect the transfer of funds (purchase prices) to natural persons in Germany and abroad, involving buyers, retailers and most likely also wholesale dealers and producers (as can be concluded from the high amounts of some transactions) of racist propaganda material.

Distributing such material constitutes a criminal offence under German criminal law.

Source: Germany.

Case 7: Use of an IPS to move illicit proceeds gained through the sale of stolen goods on a commercial website

In 2004, an individual was charged with possession of stolen goods and benefiting from proceeds of crime. Over a three year period, the individual stole goods, bought stolen goods, and then sold them on a commercial website. The proceeds passed through an IPS account attached to his commercial website user accounts. The individual sold over 9 000 items including DVDs, computer hardware and software, and Nintendo Gameboys, for a total of over USD 459 000. Local law enforcement found CAD 188 000 in savings bonds that had been purchased with a portion of the proceeds. The individual was sentenced to two years in jail and fined CAD 83 000.

Source: Canada.

Case 8: Use of cash vouchers to collect extortion money

An unknown criminal sent an extortionate letter to a food discounter in Germany and demanded EUR 250 000 in cash vouchers issued by an IPS provider situated in the UK. The IPS provider ensured that the cash vouchers were supplied in the form requested. The provider was able to monitor the voucher numbers in the computer system and reported the point of sale where one of the vouchers was used to the police. The money was not paid out because the criminal was already arrested in an Internet cafe after observation by the police in Germany.

Source: Germany

Case 9: Suspected laundering of illicit proceeds gained through the possible online sale of counterfeit goods

An individual, working in France for a foreign company, had an account with an IPS provider and a bank account in France. The foreign company suspected to be involved in the scheme also held a bank account in France.

The account of the individual was credited for 138 operations and an amount of EUR 357 245. Among those, 44 operations were credited via the IPS provider – for more than EUR 300 000. Those latest operations seemed to come from sales made on a commercial website. Shortly after, nearly all of the money was transferred to the foreign company account in France.

The individual was suspected to be a strawman possibly used by the company to open an IPS account since companies cannot open accounts with IPS providers in France. Besides, the individual was known by the French customs for being involved in counterfeiting. This individual was found to have sold 18 650 articles over a period of five years.

Source: France.

Case 10: Laundering of illicit proceeds through cash vouchers

In 2010, several cases of the following pattern were reported to the German FIU. The average amount of the laundered proceeds of crime ranged from EUR 4 500-6 000. Transaction numbers were initially "phished" by Trojans from a bank account held in Germany. The "phishing transfer" was made to a bank account held by the financial agent.

The financial agent withdrew the money – deducting his commission – in cash. He subsequently purchased cash vouchers (max. EUR 500 per voucher) of an IPS provider at various issuing offices, like petrol stations, newspaper kiosks. The purchase was anonymous without identification of the buyer. The financial agent (*i.e.,* third party) sent the voucher number or a scanned copy of the voucher by e-mail to the person giving instructions. The PIN code was used on the Internet for payment of goods and services and for gambling websites on the Internet.

The law enforcement authorities were unable to trace the transaction channels.

It should be noted that, in such a case, several vouchers for smaller amounts –also if purchased at different locations- can be used jointly and combined. A conversion to other digital currencies by using various exchangers acting on the Internet is also possible.

Source: Germany.

Case 11: Use of digital currency account to facilitate Internet fraud and money laundering

A young person, acting as a nominee, opened a digital currency account to enable him to receive the proceeds of Internet banking thefts from an offshore associate. He then attempted to redeem the value of the digital currency account by requesting the digital currency exchanger to provide him with postal money orders. In an effort to conceal his identity he informed the cash dealer that he had lost his passport and requested that the exchanger call a money service business and inform them that a person matching his description would present himself to collect the money orders at a particular time. It is believed that he was not going to send money offshore but would keep the proceeds for himself. He has been arrested and prosecuted.

Source: Australia.

Case 12: IPS providers and nominees used to purchase illegal substances and launder proceeds from their sales

A law enforcement investigation targeting smugglers of steroids, growth hormones and other illegal performance enhancing drugs identified a number of targets involved in importation and distribution, operating throughout Australia. The traffickers within Australia were found to be sending funds overseas totalling several hundred thousand dollars to purchase the illicit substances. Additionally, they were found to be receiving several thousand dollars each week in revenue from the sale of the illicit substances.

The traffickers used legitimately issued identities, obtained in false names, to open multiple post office boxes to receive the drugs. Internet chat rooms and forums were used for networking and for online ordering. Individuals used IPS providers and money remittance services in Australia to make payments which were mainly under AUD 1 000.

Overseas suppliers were aware of prohibited imports into Australia and intentionally provided false descriptions of the goods to circumvent controls. The traffickers enlisted friends and spouses to make payments on their behalf and chose different branches from which to make payments. They would also regularly change names and purposely misspell names and addresses. The full addresses of the overseas beneficiaries were never reported, only the region.

Law enforcement executed over 140 warrants across Australia throughout this operation.

Source: Australia.

c. Mobile Payment Services:

Case 13: Suspected use of mobile payments to move funds related to fraud

A victim was fooled into believing that the spouse was involved in an accident and the victim was asked to send money using a mobile payment provider to pay doctor's or hospital's bill.

Source: Philippines.

Case 14: Suspected use of mobile payments to move funds associated to telemarketing fraud

SMS messages were sent to victims claiming that they had won an electronic raffle. To claim their prize, they were asked to send money using a mobile payment provider to pay for taxes related to prizes.

Source: Philippines.

Case 15: Selling stolen phone credits through mobile P2P payments

In April 2010, an individual was sentenced in Cayman Islands for using stolen credit card information to illegally obtain phone credits which he then sold through the mobile P2P payment services. Although the amount of money was small, the individual was charged for money laundering activity under the Proceeds of Crime Law of Cayman Islands.

Source: Cayman Islands Attorney General´s Office.

4.2 Typology 2: Exploitation of the non-face-to-face nature of NPM accounts

125. Many NPMs rely on a business model where face to face customer contact is minimal or nonexistent. This can facilitate abuse by criminals for money laundering purposes.

126. In a number of cases NPM products were used to launder illicit proceeds gained from fraud following identity theft or from stealing money from bank accounts or credit/debit cards using computer hacking or phishing methods. Since the bank accounts or credit and debit cards were held in the names of legitimate customers, the criminals were able to use them as reference accounts for the funding of prepaid cards or IPS accounts. In such instances, the NPM providers could not detect that the transactions were actually not initiated by their legitimate customer, or detect any other suspicious activity.

127. In other cases, stolen or fake identities were used to create NPM accounts which were also used as transit accounts in the laundering of illegal proceeds, or to commit both criminal activities (*e.g.*, fraud) and money laundering at the same time.

128. The prepaid card or IPS account appeared to be mainly used as transit accounts in most cases. Once the illicit funds had been transferred to those accounts, criminals or their associates withdrew them at ATMs or spent the funds for purchases of goods (often on the Internet).

129. Although in many of the case studies presented below, the IPS or prepaid card provider could not have detected suspicious activity, some shortcomings in some providers´ identification and verification processes and monitoring systems is likely to have contributed to the illegal activity going undetected for some time. For example, in Case 27, although individual bank transfers appeared legitimate, the use of four reference bank accounts in different cities for the same IPS account should have raised suspicion with the IPS provider.

a. Prepaid Cards:

Case 16: Laundering of proceeds stolen from individuals' bank accounts

In 2007, six defendants were prosecuted for using stolen information to transfer money illegally from bank accounts to accounts controlled by the defendants, including prepaid cards. The defendants used a freely available software program to scan the Internet for vulnerable personal and commercial computers holding financial account information. The defendants then initiated fraudulent transactions to transfer funds from the victims' accounts to accounts created in the names of front companies. A portion of the illicit proceeds in the front company accounts was used to load prepaid cards which the defendants used to make purchases. The defendants were accused of laundering about USD 166 000 in eight months. The six defendants each pleaded guilty to conspiracy charges and were sentenced to from 3 to 36 months in prison.

Source: United States.

Case 17: Laundering of proceeds stolen from a company's payroll accounts

Two defendants were charged in 2009 with illegally accessing business computer systems via the Internet and fraudulently transferring funds from the victims' bank accounts to prepaid cards. The defendants allegedly used stolen account logins and passwords to access victims' online personnel management accounts, which, among other things, allowed users to establish direct deposit of employee wages. The defendants allegedly directed employee wage payments to the hackers' prepaid card accounts. Over a period of 11 months, the defendants allegedly transferred USD 19 967.43 in illegally obtained funds. The defendants have not yet been tried.

Source: United States.

Case 18: Laundering of phishing activity proceeds through prepaid cards

In this case, prepaid cards are used as transit accounts where criminals sent funds from bank accounts after identity theft of the accounts' holders. The phisher pretended to be the bank account holder and sent funds to the prepaid card that was issued in the name of a strawman. After the funds were transferred to the card, a corresponding amount of cash was withdrawn at ATMs.

Additional typology: Use of strawman.

Source: Italy.

Case 19: Laundering of counterfeiting and fraud proceeds through open-loop prepaid cards

Within a few months, the accounts of Mr. POL and company BE were credited by international transfers for some 500 000 EUR from a Swiss company acting as an agent and trader in securities. These funds were used to load prepaid cards. In most cases, these cards were loaded with EUR 5 000 (maximum limit). Mr. POL claimed to have loaded these prepaid cards because he had given them to his staff for professional expenses. As soon as the money was loaded on the cards, the card holder quickly withdrew the money by repeatedly withdrawing cash from ATM machines.

Mr. POL was the subject of a judicial investigation regarding counterfeiting and fraud. Given the police information on Mr. POL, the funds from Switzerland may have been of illegal origin and linked to the fraud and counterfeiting for which Mr. POL was known. This hypothesis was confirmed by the ingenious scheme (international transfers, prepaid cards and cash withdrawals) used to repatriate funds to Belgium.

Source: Belgium.

Case 20: Use of "ghost employees" to launder illicit funds through prepaid cards

In 2009, a defendant was charged with embezzling from his employer and laundering the stolen funds through prepaid payroll cards. The defendant, a manager with a janitorial service, interviewed job applicants for the purpose of stealing their personal information which he used to create fake employment positions which came with prepaid payroll cards. The defendant kept the payroll cards, using them to withdraw money from ATMs and purchase goods. In three years, the defendant laundered about USD 200 000. The defendant has not yet been tried.

Source: United States.

Case 21: Credit card fraud and money laundering

In 2006, two defendants were prosecuted for using 61 stolen credit card account numbers to fund "virtual prepaid cards," which provide an account number, expiration date, and card verification value, but no physical card for consumer non-face-to-face transactions. The defendants then used these "virtual cards" to overpay their tuition at a university in the United States. The university issued a check for USD 31 045, the amount of the over-payment, thus helping the defendants to launder their illicit proceeds. One defendant pleaded guilty to wire fraud and was sentenced to 38 months imprisonment and five years supervised release. The other defendant was convicted of making a false statement in a loan application, money laundering, mail fraud, aggravated identity theft and possession of unauthorised access devices. He was sentenced to 61 months imprisonment and five years supervised release.

Source: United States.

Case 22: Laundering of proceeds gained through ID theft

In 2006, a defendant who managed a prepaid card program was prosecuted for using his prepaid card program to launder illicit proceeds for identity thieves. The identity thieves created 21 card accounts with stolen identity information, and loaded the cards with approximately USD 1 million stolen from victims' bank accounts. The bank account information had been stolen from user accounts of one IPS provider. The identity thieves withdrew funds from the prepaid card accounts at ATMs in Russia. The defendant pleaded guilty to money laundering charges and was sentenced to 120 months imprisonment.

Additional typology: Complicit NPM provider or program manager.

Source: United States.

Case 23: Fraud and money laundering

In 2007, three defendants were prosecuted for illegally accessing a payment processor and initiating fraudulent transactions resulting in approximately USD 700 000 being credited to 80 prepaid cards. The defendants allegedly operated from a hotel room using a laptop computer, a payment card encoder, and the phone line to access a commercial payment processor, misrepresenting themselves as businesses entering refund transactions, and using the card encoder to transfer the value of the fraudulent refunds to their prepaid cards. The defendants withdrew approximately USD 200 000 a day of the value loaded onto the prepaid cards at nearby ATMs and by purchasing Postal money orders. The principal defendant was convicted, but has appealed the conviction. Two other defendants plead guilty.

Source: United States.

Case 24: Fraud and money laundering

In 2009, three defendants were charged with stealing USD 5 million by hacking into a prepaid card company's database, stealing card information and manipulating account balances and transaction limits. The defendants allegedly used the card information to create duplicate prepaid cards and used them to withdraw money from ATMs throughout the world. In one month the defendants withdrew USD 750 000. Two defendants pleaded guilty to conspiracy, money laundering, bank fraud and counterfeit access device product but have not yet been sentenced. A third defendant pleaded guilty to conspiracy and access device fraud charges but has not yet been sentenced.

Source: United States.

b. Internet Payment Services

Case 25: Laundering of illicit proceeds through a digital currency provider

In 2009, the suspect illegally accessed individuals' Internet banking accounts and instructed the computer system to remit about JPY 740 000 (USD 8 300) to a digital currency exchanger to get e-currency units. Then, the suspect sold off a portion of the e-currency units to another digital currency exchanger to get real money. Finally the suspect made the digital currency exchanger deposit the money into some bank accounts that were acquired illegally and controlled by him.

Source: Japan.

Case 26: Fraud scheme and money laundering conducted through Internet payment services

An individual devised a scheme to defraud users seeking to purchase textbooks on a commercial website. The individual created approximately 384 phony bank accounts which were opened at a bank in Jurisdiction Z, for non-existent employees who he indicated to the bank, would sell college textbooks. The individual then used the bank account information to open approximately 568 seller accounts with the commercial website using P2P online payment services (i.e., an IPS provider).

The defrauder advertised the college textbooks for sale on all of the phony commercial website seller accounts he had created. Buyers, believing they were purchasing books from the commercial website sent over USD 5.3 million in payment to the seller accounts, using the IPS provider.

The defrauder subsequently transmitted the illicit proceeds from the IPS provider seller accounts to several Singapore-based bank accounts.

The law enforcement agency from Jurisdiction Z contacted Singapore's law enforcement agency, who then responded quickly to seize the tainted funds. With the close cooperation between the law enforcement agencies, the seized funds were successfully repatriated to the victims. The defrauder was also charged for wire fraud in Jurisdiction Z.

Source: Singapore.

Case 27: Funds stolen from bank accounts laundered through IPS accounts

A computer criminal stole the victim´s personal data for online banking (including customer and account data) then opened a fraudulent account with an IPS provider under the name of the victim. The personal data provided in the opening of the account (phone number, home address, date of birth etc.) were fake. The email addresses given were issued by so-called "free providers" that do not conduct any identification or verification of their customers themselves.

The criminal named a reference bank account for funding the fraudulent IPS account. This reference account was the victim's.

Then the criminal effected a fraudulent transaction from the victim´s reference bank account to the fraudulent IPS provider account. As the funds came from the referenced bank account, the transaction appeared legitimate to the IPS monitoring system. The received funds were transferred to other accounts held with the IPS. The law enforcement authorities were neither able to trace the money flows nor find out the criminals´ identity.

The criminal repeated this scheme with several victims, but always using the same IPS account. Thus, he changed the reference bank account for this IPS account four times in two months; the four named reference bank accounts were held with different banks in different cities.

Source: Germany.

4.3 Typology 3: Complicit NPM providers or their employees

130. A number of submitted cases feature prepaid card and IPS providers or their employees, which are controlled by criminals and wilfully or recklessly assisting money laundering and terrorist financing activities. In such cases, market entry restrictions such as fit and proper tests have failed or are not applicable to the respective entity under that jurisdiction.

131. In some instances (case studies #28, #30 and #31), both IPS and prepaid card providers were suspected to be complicit and colluding in facilitating the laundering of illicit proceeds.

a. Prepaid Cards

Case 28: Suspected use of open-loop cards & online payment systems to launder drug proceeds

This case was generated following the receipt of information from a foreign FIU which indicated that a number of individuals were charged for laundering millions of drug proceeds through a company providing open-loop prepaid cards in Country A. The funds were suspected to be loaded on prepaid cards and moved, for example, from Country A to South America, that is, back to the drug traffickers. Other criminal activities were also suspected to be the source of the illicit funds.

Two of the individuals, associated to the prepaid card company, were found to have addresses in both Country A and Canada, and had opened bank accounts and established at least one company in Canada.

The prepaid card company was located in Country A, but held many accounts in that country and in Canada. The bank accounts in Country A and in Canada were used to receive funds from various individuals and entities located in a number of different countries in Central America, Europe, Caribbean, Africa, Asia, South Asia as well as in Country A and Canada.

It was further revealed that two Canadian Internet Payment System providers (IPS) sent funds to the same prepaid card company in Country A. Based on available information, it appeared that both IPS offered a prepaid card service to their clients, which was provided by the prepaid card company in Country A.

One of the Canadian IPS was the subject of another case in which it was suspected of facilitating the laundering of Ponzi scheme proceeds.

Suspicious transactions included third-party cash deposits and international electronic funds transfers (EFTs). Most of the funds received in the Canadian accounts were transferred back to the accounts held in Country A by the prepaid card company and two other associated companies also located in Country A.

Additional typology: Third party funding

Source: Canada.

Case 29: Embezzlement activities and money laundering

In 2007, a defendant was prosecuted for embezzling more than USD 375 000 from his employer, a national chain convenience store, by fraudulently loading the proceeds onto prepaid cards. The defendant allegedly processed routine transactions that involved adding value to prepaid card accounts which appeared to be held by actual customers, but did not take in funds to cover the transactions. Although these transactions were processed by the prepaid card company, the defendant allegedly ensured that the transactions were not being recorded internally to avoid the detection of his embezzlement.

Source: United States.

b. Internet Payment Services

Case 30: Suspected use of IPS (including digital precious metals) and open-loop prepaid cards to launder proceeds of fraud schemes

This case was initiated following the receipt of information from law enforcement and a foreign financial intelligence unit (FIU) which indicated that a Canadian IPS provider, its subsidiary in the United States and other associated entities were suspected of laundering illicit proceeds derived from pyramid schemes (Ponzi schemes) and telemarketing fraud schemes.

It was revealed that the Canadian IPS also had subsidiaries in a European and an Asian country. In addition, it was found that at least five digital currency exchangers (located in Canada, the United States and a Northern European country), two digital precious metals providers (United States), three open-loop prepaid cards providers (in Canada and the United States) were knowingly or unknowingly used in this complex money laundering scheme. One of the prepaid card providers was found to have offered its product for the use of a virtual world´s gamers who could fund their virtual world accounts and withdraw their virtual currencies into real currencies directly at ATMs.

Generally, funds sent from foreign countries to Canadian bank accounts held by the Canadian IPS and prepaid cards providers were either used to load prepaid cards or to settle accounts* with other IPS or prepaid card providers located in other countries. In some instances, suspicious funds entered the financial system in Canada and appeared to be then layered through other countries, sometimes coming back to Canada.

Suspicious transactions included large deposits of cash and bank drafts often followed by international electronic funds transfers (EFTs) and the layering of illicit funds through EFTs sent between various bank accounts.

Source: Canada.

* In most instances, the reporting of these transactions were provided by financial institutions and involved the transfer of funds between the pooled bank accounts held by the IPS and prepaid card providers. Information about clients of the IPS and prepaid card providers were not available.

Case 31: Laundering of illicit funds through digital currency and prepaid cards

Within the scope of an investigation, an international group of offenders transferred illegally- obtained money through a financial service provider to Eastern European countries, where it was withdrawn by members of the group and converted to electronic currency through digital currency exchangers.

The digital currency was then transferred to accounts held by offenders with a financial service provider handling electronic currency in the countries involved. In co-operation with a bank located in an offshore region this financial service provider issued MasterCard "Cirrus-cards" (prepaid cards), which were acquired anonymously and loaded with electronic currency. The cards could be used worldwide in payment transactions at points-of-sale (POS) and cash dispensers which accept "Cirrus".

In this way, the flow of illegally obtained money was effectively concealed, and the offenders were able to access the secure illicit money promptly and anonymously.

Source: Germany.

Case 32: Laundering of illegal online gambling through an IPS

In 2007, an Internet payment business based in the Isle of Man and publicly traded on the Alternative Investment Market ("AIM") of the London Stock Exchange — admitted to criminal wrongdoing and agreed to forfeit USD 136 million in criminal proceeds as part of an agreement to defer prosecution.

The IPS business participated in a conspiracy to promote illegal (according to U.S. legislation) Internet gambling businesses and to operate an unlicensed money transmitting business.

Source: United States.

Case 33: Money laundering through a digital precious metals provider

In 2008, an Internet-based digital currency business, and its three principal directors and owners, pleaded guilty to criminal charges relating to money laundering and the operation of an illegal money transmitting business.

Several characteristics of the digital currency business operation made it attractive to users engaged in criminal activity, such as not requiring users to provide their true identity, or any specific identity. The digital currency business operation continued to allow accounts to be opened without verification of user identity, despite knowing that the business was being used for criminal activity, including child exploitation, investment scams, credit card fraud, money laundering and identity theft. In addition, the digital currency business assigned employees with no prior relevant experience to monitor hundreds of thousands of accounts for criminal activity. They also participated in designing a system that expressly encouraged users whose criminal activity had been discovered to transfer their criminal proceeds among other accounts of said digital currency business. Unlike other IPS providers, the digital currency business operation did not include any statement in its user agreement prohibiting the use of its services for criminal activity.

Source: United States.

4.4 Cross-border transport of prepaid cards

132. The 2006 FATF report featured another perceived risk / typology for the abuse of prepaid cards, namely the replacement of illicit cross-border movement of cash with the cross-border transport of prepaid cards. The best example to illustrate this does not involve open-loop prepaid cards, but traditional bank-issued debit cards. In 2007 in the United States, two defendants were charged with money laundering in connection with the transfer of drug profits to Colombia via the ATM network. The defendants allegedly instructed family members, friends and others to establish 380 bank accounts in six states. The defendant then made deposits between USD 500 and USD 1 500, allegedly depositing more than USD 100 000 in 112 bank accounts in a single day. For each account, the account holder obtained two ATM cards. The defendants kept one ATM card and mailed the other to Colombia where the funds were withdrawn via ATMs.

133. There are similar cases involving the cross-border movement of closed-loop payment cards as well as a few instances involving the cross-border movement of open-loop prepaid cards. For example:

- Prepaid cards were sent from the US to Canada with no balance, and a limit of USD 1 000. Although the cards were sent to Canada they were redeemable only in the United States. These cards were suspected to have been fraudulently purchased with cloned credit cards.

- In another instance, prepaid cards were sent from South America to Canada. These cards were sent to one individual, but were in the name of a number of other individuals. The issuer of the cards had surfaced in another investigation in the past. The individual to whom the cards were sent had also surfaced in the past and been of interest to European and American law enforcement authorities. As a result of the investigation, the cards were cancelled as the bank did not wish to tarnish its reputation.

- In Australia, the holder of a prepaid card was found to have regularly loaded value by paying cash just below the AUD 10 000 reportable threshold. A second card linked to the same account was sent overseas where the funds were withdrawn through ATMs. The process was repeated, with more than AUD 100 000 laundered through the scheme.

- An Australian investigation identified an individual as the holder of 12 legitimately issued driver's licences under fictional identities, as well as one licence issued under his real identity. In addition, the individual was identified as being in possession of numerous false identity documents and foreign passports. When the individual was detained by law enforcement officers he was found to be carrying approximately AUD 140 000 in cash generated by criminal activities and 46 prepaid cards. A search warrant at a storage unit rented in his name located further prepaid cards and gift cards. It was alleged the money was being taken to India for the purposes of money laundering. It appears that the individual purchased these cards, which are available over the counter at post offices and service stations in values of AUD 50 and AUD 100. Markings on some of the cards indicated they were valued at AUD 500, which suggested that they were purchased online.

134. While the first two aforementioned examples raise concerns about potential misuse of prepaid cards for money laundering purposes, they could not clearly be linked to money laundering or terrorist financing. However, the last two examples have been linked to money laundering and the fourth one also demonstrates how anonymous prepaid cards can be used in such criminal schemes.

135. Two of the case studies submitted (***cases 22 and 28***) also imply that cross-border movement of prepaid cards was involved, as the funds were withdrawn from the card in a jurisdiction different from

where they had been loaded. However, there are no additional details that would confirm that assumption (*e.g.*, detecting or confiscation of cards due to cross-border controls).

136. Based on the above, it appears that since 2006, a limited number of cases involving cross-border transport of prepaid cards have started to emerge. However, given the small number of examples available to date, the project team believed that it may be premature to combine these cases under one typology on its own. The lack of examples can be explained by the fact that prepaid cards are neither considered currency nor bearer negotiable instruments in the sense of FATF Special Recommendation IX in most jurisdictions. Accordingly there is no obligation to make a declaration when crossing borders. It is also very difficult for customs officers to easily differentiate prepaid cards from regular credit cards given that both share very similar physical attributes.

4.5 Red Flags

137. The analysis of the case studies identified red flags which are relevant to all NPM products and services. In addition, a small number of red flags appear to be associated predominantly with suspected complicit prepaid card providers. A few case studies are referred to as examples of the red flags and do not constitute the complete list of cases associated with each of the red flags.

138. Red flags will be indicators of suspicious activity where a product's actual use deviates from its intended use or does not make economic sense. For example, cash withdrawals in foreign jurisdictions will be expected where the product is a prepaid traveller card, but unusual where the product is marketed to minors. Red flags should therefore not be applied unthinkingly, but tailored to the product's characteristics.

All NPMs:

- Discrepancies between the information submitted by the customer and information detected by monitoring systems (***case 19***).
- Individuals who hold an unusual volume of NPM accounts with the same provider (***cases 21 and 23***).
- A large and diverse source of funds (*i.e.*, bank transfers, credit card and cash funding from different locations) used to fund the same NPM account(s) (***cases 6, 7, 16 and 17***).
- Multiple reference bank accounts from banks located in various cities used to fund the same NPM account (***case 27***).
- Loading or funding of account always done by third parties (***cases 1 and 3***).
- Numerous cash loading, just under the reporting threshold of USD 10 000 (*i.e.*, structured loading of prepaid cards), of the same prepaid card(s), conducted by the same individual(s) on a number of occasions (***case 5***)
- Multiple third party funding activities of a NPM account, followed by the immediate transfer of funds to unrelated bank account(s) (***cases 9 and 26***).
- Multiple loading or funding of the same accounts, followed by ATM withdrawals shortly afterwards, over a short period of time (***cases 18 and 19***).

- Multiple withdrawals conducted at different ATMs (sometimes located in various countries different from jurisdiction where NPM account was funded) (***cases 4 and 24***).

- NPM account only used for withdrawals, and not for POS or online purchases (***cases 18 and 19***).

- Atypical use of the payment product (including unexpected and frequent cross-border access or transactions) (***cases 2 and 24***).

Specific to suspected complicit prepaid card providers:

- Large number of bank accounts held by the same prepaid card company (sometimes in different countries) apparently used as flow-through accounts (may be indicative of layering activity) (***case 28***).

- Prepaid card company located in one country but holding accounts in other countries (unexplained business rationale which could be suspicious) (***case 28***).

- Back and forth movement of funds between bank accounts held by different prepaid cards companies located in different countries (may be indicative of layering activity as it does not fit the business model) (***case 30***).

- The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of a prepaid card company do not make economic sense (***case 30***).

CHAPTER 5: LEGAL ISSUES RELATED TO NPMS

139. This chapter addresses how the provision of NPMs is regulated in different jurisdictions.[59] **Section 5.1** introduces different regulatory approaches that are currently being applied to NPMs. **Section 5.2** deals with specific challenges for regulators, law enforcement and supervisors.

5.1 Regulatory models applied to NPMs

140. The FATF Recommendations require all entities or persons conducting certain activities to be subject to AML/CTF obligations and oversight. These include entities or persons transferring money or value, or issuing and managing means of payment.[60] Most NPM providers are therefore financial institutions and should be regulated and supervised in line with Recommendation 23 or Special Recommendation VI.

141. In NPM business models with a strong segmentation of services, *i.e.*, with several entities carrying out the financial activity jointly, it can be difficult to judge whether the respective contribution of one single entity in the chain is sufficient to designate it as a financial institution (and consequently subject it to regulation and supervision). Examples for this are the business models of digital currency providers,[61] but also the use of agents.[62] In both examples, different views are taken on whether these activities should be regulated and supervised or not.

142. Analysis of the questionnaire responses for this project showed that there are three different approaches to regulating New Payment Methods. In some jurisdictions NPM providers are not subject to AML/CFT regulation at all, or only certain types of NPMs are regulated. In others, the regulatory regime developed for more traditional financial institutions (such as banks or Money Service Businesses) also applies to NPM providers, or they are subject to new regulatory regimes specific to NPM providers.

5.1.1 Not subject to regulation

143. In some jurisdictions certain NPMs are not subject to regulation. In others, the degree of regulation differs depending on the type of NPM.

---

59 The World Bank is preparing work on regulation of "innovative retail payment products", which includes the NPM services featured in this report. To this end, a questionnaire has been launched in July 2010. The World Bank survey builds upon the *Survey on Electronic Money and Internet and Mobile Payments*, published in 2004 by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements, Basel.

60 FATF Glossary – "financial institution".

61 This is discussed in more detail below, see para. 170 ss.

62 This is discussed in more detail below, see para. 175 ss.

144. Issuers of **prepaid cards** are subject to both prudential and AML regulation in every jurisdiction that responded to the project questionnaire and that has domestic issuers of such cards.[63]

145. However, where there is a segmentation of services through the use of third parties that do not fit into the traditional definitions of financial institutions, these are usually not subject to regulation (*e.g.*, card program managers, retailers etc.). Third parties include agents and outsourcing arrangements. This issue is discussed in more detail below (See chapter 5.2 (*The use of agents / Outsourcing CDD measures*), para. 175 ss.).

146. As regards **Internet payment services**, 15 jurisdictions have reported Internet payment service providers seated in their jurisdiction. Of these, four jurisdictions did not require providers to obtain a licence or register for the provision such services.[64] As a result, there are no legal AML/CFT obligations for such providers in these jurisdictions. One of these unregulated providers (a digital currency provider) holds about 11 million customer accounts, serving customers from all over the world. While other unregulated providers may also operate globally, they do not reach the same size.

147. Third parties associated with Internet payment services are usually needed for funding the IPS account or withdrawing funds from it. They can be regulated or unregulated entities. Regulated entities are themselves subject to AML obligations and include traditional money remittance businesses (*e.g.*, Western Union), prepaid card issuers or banks.

148. Unregulated third parties are not normally within scope of AML legislation and include digital currency exchangers, which are a vital component of digital currency providers´ business models as they sell digital currencies for regular money or other e-currencies.

149. The provision of **mobile payment services** is regulated in most of the 15 jurisdictions that have identified domestic providers of such services.[65] However, in some jurisdictions the service is provided by unregulated entities (such as telecommunications companies) which have no legal AML/CFT obligations.

In its Working paper no. 146,[66] the World Bank has recommended that mobile payment services providers should be subject to regulation:

"1. The FATF may wish to consider treating telephone companies that facilitate transactions as financial institution (...).

2. After this, assessors should consider mobile financial services when applying the FATF methodology to country AML and CFT compliance (...)."

150. Mobile payment service providers often use agents for the distribution of their services, opening new customer accounts, as well as receiving and paying out cash from or to customers. Such agents typically are numerous and are themselves not subject to immediate regulation.

63 See Appendix A, *Prepaid Cards*, Table B.

64 See Appendix A, *Internet Payment services*, Table B.

65 See Appendix A, *Mobile payment services*, Table B.

66 World Bank (2008), p. 53.

5.1.2 Subject to existing regulation for traditional financial services

151. Some jurisdictions apply the same regulatory regime to NPM service providers as they apply to traditional financial institutions. As a consequence, in these jurisdictions, the provision of NPM services is restricted to banks or other traditional financial institutions.

152. For all jurisdictions that have submitted a response to the questionnaire, **open-loop prepaid cards** may only be issued by regulated financial institutions due to regulatory requirements. It is also the policy of card technology providers (*e.g.*, VISA, MasterCard) to only cooperate with such regulated entities.[67]

153. Although not enough details were provided by jurisdictions when responding to the questionnaire to provide exact numbers, it appears that in relation to **Internet payment services** some jurisdictions subject IPS providers to the same legal and regulatory requirements as traditional financial institutions, while others restrict IPS provision to banks or classify IPS providers as money services businesses or remittance providers.[68]

154. Finally, some jurisdictions restrict **mobile payment services** to banks or co-operation between banks and telecommunication companies. Such "bank-based models" usually result in each customer having an individual bank account which they can access through the mobile phone, rendering such services a type of mobile banking rather than mobile payment in the sense of this report.

155. Even though such mobile banking schemes fall outside the scope of this project, they do have to cope with some of the same issues and risks as mobile payment services (especially as regards such risks resulting from non-face-to-face business and the use of agents, or the application of simplified CDD measures), as can be seen from the following examples.

Box 7
Example: Mexico

As part of the efforts to promote financial inclusion, Mexico´s financial authorities have implemented a Mobile Banking model, making use of the existing telecommunications network to provide elemental banking services to the population, also in rural and remote areas.

The Mexican authorities distinguish between two types of Mobile banking:

In the classic mobile banking model, mobile phone users can link their mobile phone to an existing bank account (debit or credit card).

In the newly introduced mobile payment* model, phone users may open (bank) accounts at a telecommunications provider´s who acts as a banking agent. These so-called "low transactional accounts" are limited to basic banking services (deposits, withdrawals and incoming/outgoing payments), and transactions are limited to approx. 700 USD per month, resulting in lower CDD requirements.**

* The term "mobile payment" used by the Mexican authorities is not identical with the term "mobile payment" used in this report; see glossary.

** See 5.2, *The definition of low risk cases*, para. 161 for more details.

67 These are mostly credit institutions, but may also be other types of regulated institutions, *e.g.*, electronic money institutions in the EU (see 5.1.3, *Subject to specifically designed regulation*).

68 See Appendix A, Table B and C for Internet Payment services.

Box 8
Example: South Africa

In South Africa, a bank entered into a partnership with a mobile phone service provider to provide a banking service where accounts could be opened and activated via the phone without personal contact with the bank or a representative of the bank. The South African Reserve Bank has issued a Guidance note to determine the minimum set of criteria that must be met in the identification and verification process for such account openings.[69]

5.1.3 Subject to specifically designed regulation

156. Some jurisdictions have implemented a dedicated regulatory regime for providers of NPMs. For example, the EU´s "Electronic Money Directive" introduced "electronic money institutions", a new category of financial institutions. These are subject to the same AML obligations as traditional financial institutions, but the prudential requirements differ in recognition of restrictions imposed on e-money institutions´ activity.

Box 9
The EU concept of "electronic money"

According to Article 2 no. 2 of the revised EU Electronic Money Directive(EMD)* the term electronic money (or "E-money") is defined as follows:

"'*electronic money' means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer;..:"*

This definition has been carefully chosen to ensure technological neutrality and to encompass business models where the value is stored either individually on a customer´s device (such as a card or a mobile phone) or collectively on a central server. As a consequence, the term electronic money covers all types of NPMs discussed in this report.

The issuance of e-money is reserved to banks and "electronic money institutions", a new type of financial institution created by the EMD. Both types of financial institutions are subject to prudential and AML/CFT supervision. Compared to banks, the scope of activities in which electronic money institutions may engage is limited to a) issuing electronic money; b) the full range of payment services as defined in the EU Payment Services Directive**; c) provision of credit facilities linked to the payment services provided; and d) other business activities other than issuance of electronic money. However, e-money institutions cannot accept deposits. This constraint in activities is counterbalanced by an alleviation of prudential requirements for electronic money institutions. This is intended to facilitate market entry to newcomers.

The EMD, in conjunction with the 3rd Money Laundering Directive, leaves it to each member state´s discretion to allow simplified Customer Due Diligence for low risk products that do not exceed certain thresholds. The vast majority of member states has made use of this option to allow simplified Customer Due Diligence.***

* Official Journal of the European Union (2009)
** Official Journal of the European Union (2007)
*** For more details on the EMD and its interconnectivity with the Payment Services Directive, see Appendix D.

157. The United States is currently considering the introduction of a new subtype of money services business called "provider of prepaid access".[70] Unlike the EU legislation described above, this legislative initiative does not intend to facilitate market entry to new competitors in the market for payment services, but to close what has been identified as a gap in regulation.

69 South African Reserve Bank (2008)

70 See *Box 11 – United States* on FinCen´s *Notice of Proposed Rulemaking*.

5.2. Specific issues in regulation and supervision of NPM

158. Where NPM service providers are regulated, supervisors, law enforcement agencies and legislators are faced with a number of legal and practical challenges. Some guidance already exists in relation to some of these issues, but others have yet to be addressed.

The issues highlighted in the following are:

- Simplified Customer Due Diligence
  - The definition of low risk cases
  - Exemptions from AML obligations: Low risk financial activities and institutions -vs.- Low risk customers/products
  - Non-face-to-face business models: level of required CDD measures
- Digital currency providers: the use of exchangers
- The use of agents / outsourcing CDD measures
- "Hybrid" service providers
- Suspicious transaction reporting in cross-border scenarios
- Law enforcement and supervisory action against foreign providers
- Identification of secondary card holders

159. This list is not comprehensive or exhaustive; it focuses on issues related to the prevention and prosecution of Money Laundering and Terrorist Financing, regulation and other aspects of the FATF 40 + 9 Recommendations.[71]

Simplified Customer Due Diligence

160. Several jurisdictions allow financial institutions to apply simplified or reduced Customer Due Diligence measures in cases of low risk. There is however no uniformity of approach or a shared understanding with regards to (1) when a product can be considered low risk and (2) to what degree CDD measures can be reduced.

The definition of low risk cases

161. Several jurisdictions have identified in their legislation certain low risk scenarios in which simplified due diligence can be applied. With regard to NPMs, most jurisdictions rely mainly on value limits and transaction thresholds to define low risk scenarios, while others look at more risk factors including *e.g.*, the cross-border functionality of a product, the funding mechanisms and the usage limits of a product (see for example the South African approach in the text box below). According to the approach promoted by this report, a risk assessment should consider as many risk factors (as listed in the

[71] Other challenges may include the creation of fair competition and a level playing field, consumer protection aspects etc.

risk matrix above)[72] as possible in order to be more reliable and meaningful. The FATF standards currently do not provide guidance on or definitions of low-risk scenarios or related monetary thresholds specifically for NPM. Some private sector representatives have indicated that such guidance would be welcome.

162. Where jurisdictions use value limits to designate low risk situations, they differ significantly among jurisdictions, ranging from USD 5100 per year (Switzerland),[73] or USD 700 per month (Mexico)[74] to USD 1 000 per day (USA).[75]

Box 10
European Union:

The vast majority of member states has made use of the option to allow simplified Customer Due Diligence according to Article 11 par. 5d of the 3rd Money Laundering Directive* as amended by the second e-money Directive**, which states that member states may allow their institutions to apply simplified CDD measures with regard to electronic money

"where, if it is not possible to recharge, the maximum amount stored electronically in the device is no more than EUR 250, or where, if it is possible to recharge, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year upon the electronic money holder's request in accordance with Article 11 of Directive 2009/110/EC. As regards national payment transactions, Member States or their competent authorities may increase the amount of EUR 250 referred to in this point to a ceiling of EUR 500."

* Official Journal of the European Union (2005)
** Official Journal of the European Union (2009)

Box 11
United States

According to a US Notice of Proposed Rulemaking*, certain low value prepaid programs shall not be subject to the new regulation:

"Providing prepaid access to funds subject to limits that include a maximum value (...)where such maximum value is clearly visible on the prepaid access product:

(i) Not to exceed USD 1 000 maximum value that can be initially loaded at the time of purchase of the prepaid access;

(ii) Not to exceed USD 1 000 maximum aggregate value (such as through multiple transfers of value to a single prepaid access product) that can be associated with the prepaid access at any given time; and

(iii) Not to exceed USD 1 000 maximum value that can be withdrawn from the prepaid access device on a single day.

The reason for exempting such prepaid programs is that it is believed "that the potential for misuse is slight".**

* Federal Register (2010)
** Federal Register (2010), p. 40.

72 See above para. 63 ss.

73 Amount converted into USD for reasons of comparability; the actual threshold is CHF 5 000.

74 Amount converted into USD for reasons of comparability; the actual threshold is 2 000 UDIs ("inflation-indexed units").

75 Some of the following value limits refer to other products than NPMs, *e.g.*, bank accounts. However, they were included here to give a better overview over different approaches to handling low risk.

Box 12
South Africa:

In May 2010 South Africa has enacted an exemption for low risk prepaid products which exempts financial institutions issuing prepaid products from certain CDD obligations if the following criteria are met:

"(a) the value of every individual transaction initiated through the use of the prepaid payment instrument cannot exceed ZAR 200;

(b) the available balance cannot exceed ZAR 1 500 at any time;

(c) the monthly turn-over of value loaded onto the prepaid instrument cannot exceed ZAR 3 000;

(d) can only be used to purchase goods or services in the Republic;

(e) the reloading of value to the prepaid instrument to enable use or further use of the prepaid instrument can only be done by means of an online system requiring the client to enter a personal identification number;

(f) the use of the prepaid instrument cannot enable the remittance of funds, the withdrawal of cash or the receipt of cash as part of a transaction for the payment of goods or services or in any other form whatsoever." *

* South African Government Gazette (2010)

Box 13
Mexico:

In order to promote the financial inclusion of in particular the low income population, Mexico introduced a simplified regime of low risk products with simplified KYC and CDD requirements for specific transactions, products and financial services. These low risk products include the following two subtypes of bank accounts that are different from traditional bank accounts:

"Low Transactional accounts" are restricted to natural persons whose monthly deposits transactions are below 2 000 Units of Investment "UDI" (approx. USD 700). Simplified rules apply for KYC, account opening and Monitoring and Reporting.*

"Low Risk Accounts" are available for natural and legal persons whose accumulated transactions, including deposits and withdrawals, on a monthly basis do not exceed 40 000 UDIs (approx. USD 14 000). Simplified rules similar to those for "low transactional accounts" apply to these accounts, but more customer data needs to be collected when opening such an account.**

* The file requires to be integrated only with the client basic data (name, address and birth date) and it is not required to maintain a copy of the documentation. However, there is the obligation for the applicant to actually display a formal ID when initially opening this type of account.

** The file requires to be integrated with the client´s whole list data requirements, and it is not required to maintain a copy of the documentation. However, there is the obligation for the applicant to actually display a formal ID when initially opening this type of account.

5.2 Exemptions from AML obligations: Low risk financial activities and institutions -vs.- Low risk customers/products

163. The current FATF standards provide some flexibility that allow jurisdictions to allocate resources in the most efficient way to address the most pressing ML/TF risks. To deal with low ML/TF risks, the standards provide two options that must be clearly differentiated: (1) partial or full exemption from AML regulation and supervision for low risk activities and institutions; and (2) simplified or reduced CDD for low risk customers or products.

1. According to the glossary of the FATF Methodology (see definition of the term "financial institution"), there are two theoretical possibilities for partial or full exemption from regulation and supervision:

    a. Jurisdictions are permitted to exempt from or limit the application of the standards for **certain financial activities** on the basis of a proven low risk, and only in strictly limited and justified circumstances. Such an exemption would apply to the respective financial activity as such and automatically affect all institutions carrying out such an activity. As regards NPM, the project team is not aware of any jurisdictions that have

declared the provision of NPM as such exempt (fully or partially), based on a proven low risk.

Box 14
Example: Australia

Under the Australian AML/CTF Act, issuing a stored value card, or increasing its value, only constitutes a designated service if the value stored on the card is greater than:

- AUD 1 000, if whole or part of the monetary value stored on the card may be withdrawn in cash; or
- AUD 5 000, if no part of the monetary value stored on the card may be withdrawn in cash.

Where stored value cards are issued under amounts of AUD 1 000, the services associated with them are not designated services for the purposes of the AML/CTF Act and consequently not subject to any of the AML/CTF obligations imposed by that Act.

b. In addition, when a financial activity is carried out by a person or entity **on an occasional or very limited basis** (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing activity occurring, a jurisdiction may decide that the application of anti-money laundering measures is not necessary (either fully or partially) for that particular person or entity. This provision aims at non-financial institutions that occasionally carry out financial activities on the side (*e.g.*, hotels that occasionally exchange small amounts of currency for their guests).

2. Where a certain financial activity is not exempted from AML regulation and supervision, Recommendation 5 requires that financial institutions should undertake customer due diligence measures. The extent of such measures may be determined on a risk-sensitive basis, allowing for the application of **reduced or simplified CDD measures** in cases of low risk.

Box 15
Example: EU

According to EU legislation, the issuing of electronic money is a regulated financial activity, regardless of any value limits or thresholds that may apply to a certain product. Accordingly, issuers of electronic money are subject to the member states´ national AML/CFT laws.

The 3rd EU Money Laundering Directive grants member states the opportunity to allow their financial institutions to apply simplified CDD measures in designated cases of low risk. For the issuing of electronic money, concrete low risk scenarios are defined by Art. 11 para 5 lit. d of the Directive (see above para. 161 for more detail).

164. Although the term "simplified CDD measures" has not been defined (neither by the FATF standards nor by most of the national regulatory regimes or guidance), an exemption from CDD measures can only be granted in the cases described above under option 1), not in the cases of option 2). As a result, where firms carry out a designated financial activity and therefore are subject to AML/CFT obligations, exemptions from the CDD requirement are considered a breach of FATF Recommendation 5[76]. Accordingly, over the last five years more than ten jurisdictions have been criticised in their mutual evaluation reports for granting exemptions from CDD measures in low risk cases.[77]

165. In spite of this, several jurisdictions argue that in the absence of a definition of "simplified or reduced CDD" in the FATF standards an exemption can be considered as a case of simplified or reduced

[76] The FATF has also confirmed this understanding of Recommendation 5 in several publications on the Risk Based Approach (*cf. Guidance on the Risk-Based Approach to combating Money Laundering* and *Terrorist Financing: High Level Principles and Procedures*, June 2007, para. 1.24 and 1.26 (p. 6); also *cf. Risk Based Approach: Guidance for Money Service Businesses*, July 2009, para 48 (p. 14)).

[77] These exemptions did not necessarily relate to the provision of NPM services.

CDD measures, and that therefore the wording of Recommendation 5 does not necessarily exclude exemptions in low risk cases. For example, according to EC legislation, EU member states are allowed to exempt issuers of electronic money from applying any CDD measures in designated low risk cases,[78][79] and many member states have made use of this option. As a result, several NPM products issued in the EU are effectively anonymous.[80]

Non-face-to-face business models: level of required CDD measures

166. Non-face-to-face business is currently addressed by FATF Recommendation 8, which recommends that "*financial institutions should have policies and procedures in place to address any **specific risks** associated with non-face-to-face business relationships or transactions."* While the wording of Recommendation 8 does not explicitly speak of "high risk", the Interpretative Note to Recommendation 5 (para. 7) makes a reference to the Basel CDD paper (section 2.2.6) for specific guidance, which says:

> *"48. In accepting business from non face-to-face customers (…) there must be specific and adequate measures to mitigate the **higher risk**."*

Within the work being currently done by the FATF in the perspective of the 4th round of mutual evaluations, there is a clear recognition that non-face-to-face business relationships or transactions represent **a higher ML/TF risk**.

167. Recommendation 5 suggests that "*for **higher risk categories**, financial institutions should perform **enhanced due diligence***". Furthermore, the Interpretative Note to Recommendation 5 (para. 13) adds:

> "Simplified CDD measures are not acceptable **whenever** there is suspicion of money laundering or terrorist financing or **specific higher risk scenarios apply**."

The FATF standards do however not clarify whether "specific risk" in the sense of Recommendation 8 equates to "higher risk scenario" in the sense of Recommendation 5. If this interpretation were correct, NPM products relying on non-face to face transactions should not be eligible for simplified CDD.

168. To base a product or service´s risk rating on one risk factor alone (here: non face to face) would not take into account the principles of risk assessment developed in the 2006 NPM report (and retained by the project team in this report). According to these principles of risk assessment for NPMs, all risk factors featured in the risk matrix presented in para. 65 of this report should be taken into account when assessing the risk of an individual NPM service or product. Non-face-to-face business relationships and transactions do increase the risk rating of an NPM service or product, but other product features (*e.g.*, solid identification and verification procedures; or strict value limits) can considerably mitigate the risk, and even lead to the product or service being assessed as "lower risk" after all. Accordingly, such business models would not categorically have to apply enhanced CDD measures, but might even qualify for the application of simplified CDD measures in certain circumstances of low risk.

---

78 For more detail see Appendix D, section 3:*The Third Anti-Money-Laundering Directive (2005/60/EC).*

79 The European commission has defined technical criteria that will classify certain scenarios as "low risk" in Art. 11 and 40 of Directive 2005/60/EC in conjunction with Art. 3 of Directive 2006/70/EC.

80 Mainly cash vouchers and some prepaid cards (open-loop and closed loop), whereas IPS providers usually ask at least for the customer's name (which may remain unverified though).

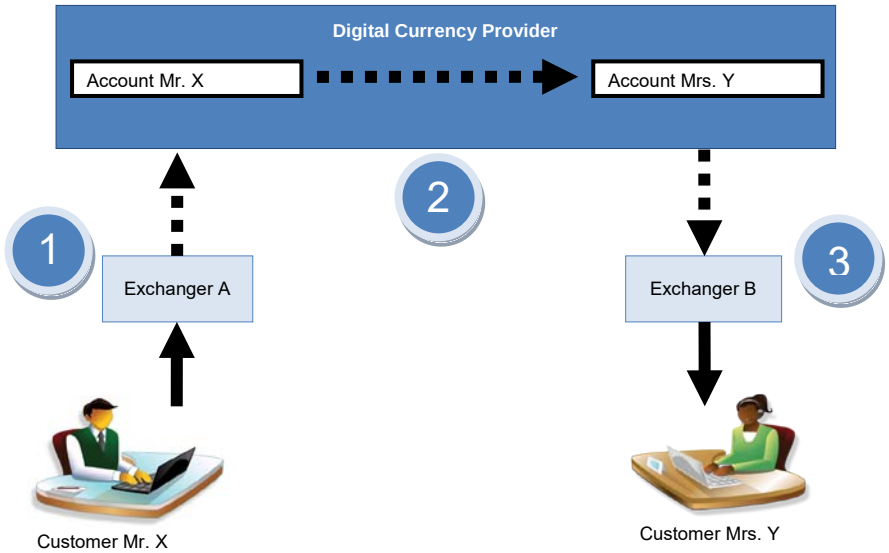
169. The project team has been informed that this issue is currently being discussed within FATF. It was indicated that the qualification of non-face-to-face business models as "higher risk" by the FATF standards might not automatically lead to a qualification as a higher risk scenario in the sense of Recommendation 5. It would be helpful if this conclusion was reflected in the standards (*e.g.*, in an Interpretative Note to Recommendation 5 or Recommendation 8).

Digital currency providers: the use of exchangers

170. The segmentation of services in digital currency business models makes it difficult to determine who the provider of the payment service is and thus subject to regulation.

171. The following diagram illustrates the segmentation of services in a digital currency provider business model, in which the actual payment is broken down into three separate steps, each carried out by a different entity:

Figure 4. Digital Currency Provider



Step 1: Funding of the customer account
Customer Mr. X pays an amount of real money to Exchanger A, who holds a certain amount of the digital currency. In exchange for the money received, the exchanger transfers an equivalent amount from his digital currency account to customer Mr. X´s digital currency account.

Step 2: Transfer of Digital currency
Customer Mr. X instructs the Digital Currency Provider to transfer a certain amount of digital currency to the Digital Currency account of Customer Mrs. Y.

Step 3: Withdrawal of funds
Customer Mrs. Y transfers a certain amount of digital currency from her own Digital currency account to the Digital Currency account of Exchanger B. In exchange for the digital currency received, the exchanger transfers an equivalent amount of real money to Customer Mrs. Y.

Source: NPM project team

172. In some jurisdictions, none of these steps would be considered a regulated activity in their own right:

- The exchangers exchange real money for digital currency, or even digital currency for another type of digital currency from different providers. They transfer value, but only between accounts of one and the same principal; they do not transfer money to third persons.
- The Digital currency provider transfers value from one person to another; however, he neither receives real money from the payer, nor does he pay out real money to the payees.

173. Other jurisdictions consider these activities to be regulated, and as a consequence consider all entities involved to be subject to supervision.

Box 16
US: MSB´s

The prosecution of an offshore Internet payment service marketing online to U.S. citizens prompted the application of existing law regarding money transmitters to any online payment service facilitating money transmission. The money transmitter definition in the U.S. states, in part:

"*Any person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means…*"

In addition to successfully applying this definition, and the associated registration, recordkeeping, and reporting obligations, to online payment services, including digital currency providers, U.S. prosecutors have applied it successfully to offshore service providers sending and receiving funds to U.S. customers.

Box 17
Germany: Involvement in unlawful business / Teilakttheorie ("theory of partial acts")

According to the German Banking Act, supervisory authorities may issue a cease-and-desist-order not only against entities conducting unlawful business themselves, but also against undertakings which are involved in the preparation, the conclusion or the settlement of such business.

Similarly, a provider is considered a "de facto branch" of a financial institution if it carries out relevant steps ("partial acts") of a financial service for that institution. As a consequence, the "de facto branch" needs to be licensed unless the financial institution it works for is licensed either in Germany or another member state of the European Economic Area.

Based on the aforementioned principles, the German authorities have initiated an administrative proceeding against an unlicensed, Germany-based digital currency exchanger that traded in digital currency issued by a provider seated in South-East Asia. The administrative proceeding is still ongoing.

174. The problem of regulating and supervising Digital currency providers and their related entities such as exchangers is exacerbated by the fact that their services often require no physical presence in a jurisdiction, but can be carried out from anywhere via the Internet. The entities involved are therefore able to choose a jurisdiction where they are not subject to regulation as their seat and provide their services from there.

The use of agents / Outsourcing CDD measures[81]

175. CDD and other AML measures are usually carried out by officers or employees of the regulated financial institution itself. However, in many NPM business models these tasks are in practice performed by third parties, including agents, intermediaries, or are outsourced. While these can be

81 For the purposes of this report, the terms "agent" and "outsource" shall be used synonymously.

different legal concepts entailing different legal obligations and requirements, for the purpose of this report these concepts shall be used interchangeably.

The FATF 40+9 Recommendations address the issue of agents and outsourcing in two different contexts, namely in Recommendation 9 and Special Recommendation VI.

176. Recommendation 9 only marginally touches on this subject. It refers exclusively to third party reliance and introduction; it does not cover agents and outsourcing agreements, nor does it provide a definition of outsourcing or agency. However, a footnote in the Methodology text accompanying Recommendation 9 is actually the only place within the standards that explicitly explains the current FATF approach towards agents and outsourcing: "*the outsource or agent is to be regarded as synonymous with the financial institution i.e., the processes and documentation are those of the financial institution itself.*"[82]

177. The only Recommendation explicitly mentioning agents is Special Recommendation VI, which recommends that "*each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions.*" The interpretative note to Special Recommendation VI defines an agent as "*any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).*"

178. The general interpretation of Special Recommendation VI is that it does not require agents to be subjected to AML obligations and supervision in their own right either. While the wording of Special Recommendation VI may leave room for other interpretations, this can be concluded from the definition of "agent" in the glossary of the methodology (which implies that the agent is subdued to the regulated principal) and the Interpretative Note to Special Recommendation VI, which in paragraph 8 finds it sufficient that the principal business maintains "*a current list of agents which must be made available to the designated competent authority"*

179. According to these principles in the current FATF standards, in most jurisdictions agents and outsources of financial institutions are not normally subject to AML legislation or regulation themselves, thus having no legal AML/CFT obligations of their own.[83] Instead, the principal (or outsourcer), being a regulated institution, will remain solely responsible for meeting the AML/CFT obligations for its activity, including actions (and omissions) of its agents or outsources. Shortcomings of the agent are attributed to the principal (*i.e.*, financial institution), which may be sanctioned for any breach of its own AML/CFT obligations, conducted by its agent.

180. As regards Money Services Businesses, FATF has issued some guidance on the handling of agents, providing some useful input on the notions of "know your agent", agent monitoring and agent training. While this guidance does not explicitly refer to NPM service providers, these concepts appear to be applicable those as well.

---

82 Footnote 16 of the FATF Methodology for assessing compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations.

83 Agents are often subject to contractual AML/CFT responsibilities that are imposed on them by the agency contract with their principal. However, there is no direct legal liability of the agents and no possibility for authorities to sanction agents if they breach their contractual AML/CFT obligations. There are usually no legal requirements for the principal to impose contractual AML/CFT responsibilities on their agents.

181. Some jurisdictions, including the U.S. and Germany, have recently reassessed their approach and have come to the conclusion that there is a gap in regulation. As a consequence, they propose to impose legal AML/CFT obligations on agents. The term "agent" in this sense may cover many different activities, including for example card program managers or sellers of prepaid funds.

a) Card program managers

182. In some business models, the prepaid card program is effectively run by card program managers. The card program manager may have ownership and control of the business model and take any important business decisions, while the issuing bank only provides access to the technical card platforms. As a result, a card program manager´s role in an NPM business model may be greater than that of a traditional outsource or agent.[84] Still, like a regular agent, the card program manager usually is not supervised and outside the scope of AML legislation, while the issuing financial institution remains legally responsible for meeting its legal and regulatory obligations.

183. This separation of business responsibility and regulatory liability situation is exacerbated if the card program manager and the issuing bank are located in different jurisdictions. If, for example, the card program manager is based in a jurisdiction with a robust regulatory regime (to which the card program manager is not subject though), this strict regime could be circumvented by cooperating with an issuing bank that is based in a jurisdiction with lower AML/CFT standards or less effective supervision.

184. A related issue is market entry. As most card program managers are not currently subject to regulation and supervision, they are also not subject to market entry requirements like fit-and-proper tests carried out by the supervisory authorities. It is therefore often down to the issuing institution themselves to identify whether its agent/program manager´s intentions are legitimate. Case studies evidence that some institutions have failed to discover the illegitimate intentions of their program managers, or have even knowingly and collusively entered into a co-operation with illegitimate program managers (see above section 4 "Typologies", *cases 22 and 28*).

185. As a result, some jurisdictions are currently considering subjecting card program managers and other third parties subject to legal AML/CFT obligations. No such regime has been finalised yet. The most advanced initiative is a US notice of proposed rulemaking (NPRM) by FinCEN, which was published for public consultation on June 28, 2010.[85]

Box 18

According to the NPRM, FinCEN proposes to implement a new subtype of Money Service Business (MSB) called "provider of prepaid access". The provider of prepaid access is described by FinCEN as follows:

"*In general, this term will apply to any person that serves in the capacity of oversight and control for a prepaid program. The determination of the applicability of this term to any given player in the program's transaction chain will be a matter of facts and circumstances; we do not "assign" this term to any particular role. We recognize that there may be situations in which no single party alone exercises exclusive control. However, we do believe that there will always be a party in the transaction chain with the predominant degree of decision-making ability; that person plays the lead role among all the others, and is in the best position to serve as a conduit for information for regulatory and law enforcement purposes. We wish to state clearly and emphatically that identifying the provider of prepaid access is not simply an arbitrary decision by the program participants. As with other MSBs, the role of the provider of prepaid access is determined through the facts and circumstances surrounding the activity; no single act*

84 The definition of "agents" for the purpose of Special Recommendation VI in the glossary of the FATF methodology states that agents work "*under the direction of or by contract with a legally registered or licensed remitter*" This implies that the agent usually is considered to be subordinated to the principal, *i.e.*, the financial institution.

85 Federal Register (2010)

or duty alone will be determinative. While not exhaustive, we consider the following activities to be strong indicators of what entity acts in a principal role:

• The party in whose name the prepaid program is marketed to the purchasing public. For example, whose press release trumpets the launch of a new product? Whose name is used in print, on-line advertisements, and on the face of the card/device itself? In legal parlance, the individual or entity who "holds himself out" as the lead player will be a very important determining characteristic.

• The party who a "reasonable person" would identify as the principal entity in a transaction chain—the principal decision-maker.

• The party to whom the issuing bank looks as its principal representative in protecting its network relationship and its brand integrity.

• The party who determines distribution methods and sales strategies.

• The party whose expertise in the prepaid environment is recognised by the others, particularly by the issuing bank, as instrumental in bringing together the most appropriate parties for the delivery of a successful program.

We intend for these enumerated characteristics to illustrate that there is no one single determinant; the provider of prepaid access need not do, or refrain from doing, any single activity. The totality of the facts and circumstances will identify the provider of prepaid access."

As a type of MSB, providers of prepaid access would have to be registered with FinCEN. According to the NPRM, they should be obligated to establish and maintain AML programs (incl. staff training), to collect identification data and transaction records and retain them for five years, and to file CTRs and SARs. FinCEN also proposes to impose the same obligations on the "sellers" of prepaid access; these however should not be considered MSBs and accordingly would not have to register with FinCEN.

The new obligations of providers and sellers of prepaid access shall not affect the legal liability of any involved banks or financial institutions: their AML obligations remain unchanged.

b) Sellers of prepaid funds

186. Several NPM providers use a network of partners (*e.g.*, retailers, pharmacies etc.) to sell their product to the customers. In some jurisdictions, there are moves to treat these as agents acting on behalf of the NPM provider, while in others they are treated as plain merchants rather than agents.

Box 19

United States

In the Notice of proposed rulemaking (NPRM) described above,* FinCEN proposes to impose direct AML/CFT obligations not only on the issuing bank and the "providers of prepaid access", but also on the seller of prepaid products:

"We are also mindful that, among all the typical parties, a very important role is that of the seller. The seller alone has face-to-face dealings with the purchaser and is privy to information unavailable elsewhere in the transaction chain. For that reason, we believe the seller to be secondarily important among all the entities involved in the program. (…) The seller is uniquely situated to see the first step in the establishment of a prepaid relationship, and to interact directly with the purchaser who may, or may not, be the ultimate end-user of the card. The requirements of this party to maintain records over a five-year time period and to report suspicious activity, also serve the law enforcement´s needs.

(…)

The seller of prepaid access is the party with the most face-to-face purchaser contact and thus becomes a valuable resource for capturing information at the point of sale, unlike any other party in the transaction chain. Typically, the seller is a general purpose retailer, engaged in a full spectrum product line through a business entity such as a pharmacy, convenience store, supermarket, discount store or any of a number of others. Precisely because this party deals face-to-face with the purchaser, and has the ability to capture unique information in the course of completing the transaction, we believe the seller should fall within the regulation´s direct reach.

Because the seller´s role is complimentary with, but not equal to, the authority and primacy of the provider of prepaid access, we choose not to require registration with FinCEN. The seller, we believe, is generally acting as an agent on behalf of the provider and this treatment is consistent with other agents under the MSB rules.

However, the seller´s agency does not excuse compliance with the other responsibilities assigned under this

proposed rule: (1) the maintenance of an effective AML program, (2) SAR reporting, and (3) recordkeeping of customer identifying information and transactional data."

* Federal Register (2010)

187. Similarly, in Australia besides issuing prepaid cards the activity of "increasing the monetary value" (*i.e.*, loading or reloading funds onto cards) of certain stored value cards[86] is considered a designated service which makes providers of such services a reporting entity under the Australian AML/CTF Act and incurs a range of important obligations. These include the requirement to have an AML/CTF program, customer identification and ongoing customer due diligence, record keeping and reporting obligations.

188. Other jurisdictions do not share the point of view described above, *i.e.*, that the current approach to agents would constitute a gap in regulation, and do not support the idea of subjecting agents to AML obligations in their own right. As an alternative, it has been suggested to reinforce or clarify the requirements on the outsourcing / agency agreements of financial institutions, especially as regards AML/CFT obligations. Many jurisdictions have legislation in place on requirements for outsourcing contracts; however, this is currently not mirrored in the FATF 40+9 Recommendations.

"Hybrid" service providers

189. Some non-financial business companies have started to take up providing NPM services (*e.g.*, telecommunications companies providing mobile payment services). These "hybrid" payment service providers may challenge existing regulatory regimes because due to their financial activities, in many jurisdictions they would either be excluded from the market (as such activities are limited to credit institutions only);[87] or they would be subject to regulation regarding all their lines of business, not only their financial activities. Furthermore, if the hybrid provider is a big company, due to its size it would be impossible to make use of regulatory waivers in many jurisdictions.

190. These hindrances may force interested hybrid providers to either provide their financial services through a separate legal entity focussed on financial services, or may deter some potential candidates from entering into the market of NPM altogether.

Box 20
Example European Union

The new EU regime for the issuance of e-money as revised by the second E-Money Directive (EMD) aims at facilitating market access to newcomers, namely telecommunication companies or large-scale retailers who want to engage in the market of e-money. Following the Payment Services Directive, the exclusivity principle will no longer apply to electronic money institutions, who are now entitled to engage in any business activity besides issuing electronic money (Art. 6 para 1 lit. e) EMD).

For the calculation of an electronic money institution´s own funds or safeguarding requirements, only the funds relating to the e-money business are taken into account, excluding the funds relating to other lines of business activity ("ringfencing").

Suspicious transaction reporting in cross-border scenarios

191. The provision of cross-border services, which is typical for many NPM business models (especially most IPS providers) raises issues as regards filing suspicious transaction reports and the effectiveness of law enforcement. In most jurisdictions, NPM providers are only obligated to report

86 Australian Attorney-General's Department (2006)

87 See 5.1.2, *Subject to existing regulation for traditional financial services.*

suspicious transactions to their home FIU, even if the persons involved in the suspicious transaction (customer / sender / receiver) are based in a different country. That country´s FIU will depend on an effective international cooperation and information sharing with the NPM provider´s home FIU. Where such cooperation is lacking, the effectiveness of the STR reporting regime and law enforcement of suspicious cases may be seriously impeded.

192. Where agents are used to provide cross-border services, the situation is similar. Agents are usually not subject to the STR regime in most jurisdictions. If they report suspicious transactions, it will most likely be towards their principals (*i.e.*, the NPM service provider) on a contractual basis. As described above, the NPM provider would then file an STR to its home FIU, but not necessarily to the FIU of the country where the agent is based.

Box 21
European Union

Within the EU Committee on Money Laundering and Terrorist Financing (CPMLFT), it is currently being discussed to which Financial Intelligence Unit reporting should be done in cross-border situations, as well as issues of attribution of competence among AML supervisors where a payment institution under the Payment Services Directive has a recourse to an agent to sell services in another Member State than the one where it is established.

While this discussion arose with regard to agents of money remittance services, the outcome of the discussion will have an immediate impact on NPM providers for whom the same provisions regarding agents apply.

Law enforcement and supervisory action against foreign providers

193. Where NPM providers provide their services across borders online only (*i.e.*, without any physical presence in the jurisdiction of the customer), foreign authorities will have limited possibilities to take action, but will normally have to rely on their counterparts in the jurisdiction where the provider is based.

194. However, some national authorities have successfully taken action against foreign providers by making use of the tools of their national criminal law and their national administrative law.

195. For example, United States authorities have used the provisions of US criminal law to impose sanctions on foreign providers located in the Isle of Man (see above **case 31**) and in the Caribbean (see above **case 33**). These national sanctions could be applied as the defendants (*i.e.*, the directors and owners of the foreign providers) either resided in the US or travelled into the US.

196. German authorities have issued administrative cease-and-desist orders against IPS service providers located in South-East Asia and Central America. According to German supervisory law, such measures can be taken only if business is conducted in Germany. However, authorities have considered activities that were provided from abroad, to take place “in Germany” when certain conditions were met. As regards the provision of financial activities through the internet, the activity will be considered to be conducted in Germany if the content of the website is designed to target the German market. Indicators for this include (list not exhaustive): domain of the website (“.de”), website in German language, customer information that is specific to Germany or the German financial sector, references to the German legal framework, and appointment of German contact persons.

Identification of secondary card holders

197. Several prepaid card providers issue cards that are specifically designed to facilitate cross-border remittances. In such business models, a main card is issued to the customer / cardholder; in addition, the customer will dispose of one or several additional cards (also “partner cards”; “remittance cards”) which they can pass on to third persons; these are the intended recipients of the remittance

transactions. The remittance is then carried out in two steps: first the cardholder loads the remittance amount on the prepaid card; secondly, the recipients may withdraw the amount at any ATM worldwide with the help of their secondary cards.

198. In a number of these business models, only the main cardholder is identified. The holders of the additional cards often remain unknown to the card issuer.

199. In the 2009 Mutual Evaluation Report for New Zealand, one such business model and the related supervisory practice have been described in much detail:

Box 22
New Zealand Mutual Evaluation 2009

According to the Mutual Evaluation Report at the time the assessment was conducted, where there were three or more "facility holders" (=account or card holders) financial institutions in New Zealand were generally "only required to perform CDD on the principal facility holders (*i.e.,* those whom the financial institution reasonably regards, for the time being, as principally responsible for the administration of the facility", while all other facility holders who remained **unidentified** were also able to conduct transactions via the facility held at the financial institution. This was criticised by the assessment team and affected the rating for Recommendation 5. *

However, as regards the **verification** of such secondary cardholders, the assessment team apparently had no objections to the application of simplified CDD:

"419. Simplified CDD is allowed when the facility provided is a remittance card facility. In such cases, there is no requirement to verify the identity of the second card holder (2008 Interpretation Regulations). These types of remittance card facilities are only offered by one bank in New Zealand. The authorities advise that the remittance card regulation exemption was designed to mitigate the AML/CFT risks that could attach to remittance products, and places a number of conditions and constraints on the eligibility for exemption. These conditions and constraints include: *i)* a maximum total annual remittance, and maximum balance on the card of NZD 9 999.99; *ii)* eligible cards can only be used on international bank Automated Teller Machine (ATM) and *Electronic Funds Transfer at Point of Sale* (EFTPOS) networks; *iii)* full FTRA verification and record keeping requirements apply to the primary card holder (account opener); *iv)* identification and record keeping requirements apply to the one other permitted card holder (who cannot be resident in New Zealand); and **v)** the issuing institution is required to carry out ongoing due diligence and transaction monitoring on the facilities. The authorities concluded that the above limitations mitigate the AML risk to an acceptable degree for the product to be offered in New Zealand on the basis that full CDD is applied to the primary card holder and simplified CDD is applied to the second card holder. This conclusion was based on a review co-ordinated by the Reserve Bank and involving officials including the Ministry of Justice, the Ministry of Pacific Island Affairs and the FIU. The review considered material from the NZ Police, APG and FATF, including typologies and evidence of misuse of stored value card and travel card-type products. Discussions were also held with several banks about product options and AML/CFT risk management options, and sample data was collected about remittance volumes and average size. A Public Discussion document and subsequent Cabinet paper were produced justifying the limitations in the regulation to mitigate the AML/CFT risk to reasonable levels consistent with the expected form and approach of the new AML/CFT Bill and New Zealand's longer term compliance with the FATF Recommendations."

* FATF (2009b), p. 84, 93.

200. While generally all holders (*i.e.*, primary and secondary holders) of an account or a card should be identified, there is room for discussion whether this is still necessary if the specific card model can be qualified as "low risk" and therefore simplified CDD measures might be applied. While a full exemption from CDD measures regarding the (primary) customer has been criticised as not in line with Recommendation 5,[88] it is unclear whether this should also apply to an exemption of secondary card holders (assuming that the primary card holder has been appropriately identified and verified). This will be dependent on the degree of control the secondary card holder has over the product, and whether he needs to be qualified as a customer of the NPM provider, or might be considered the customer´s beneficial owner, or some kind of beneficiary.

88 See 5.2, *Exemptions from AML obligations.*

CHAPTER 6: CONCLUSIONS AND ISSUES FOR FURTHER CONSIDERATION

201. Market adoption of NPMs has increased since the 2006 report, and is likely to increase even more in the future. More and more NPMs offer the opportunity to transfer funds globally. As a result, evidence of the misuse of NPMs for purposes of ML and –to some extent- TF have also increased.

202. New types of NPMs are likely to emerge in the future. Because of the convergence and combination of NPMs it will be more complex for supervisors and legislators to assess if such payment systems are vulnerable to ML/TF abuse. The continued development of NPMs therefore requires an appropriate, flexible and 'future proof' FATF framework.

203. In addition to the risk assessment (section 3) and the development of typologies (section 4), this report examines whether the FATF 40+9 Recommendations continue to provide an adequate framework to address recent technological and regulatory developments in the field of NPMs.

204. The project team has come to the conclusion that the FATF Forty Recommendations and Nine Special Recommendations provide a broadly adequate framework to address the vulnerabilities associated with new payment methods, although there is a need for the FATF to explore some issues in the international standards that require further development or clarification. The project team is aware of the fact that FATF has already launched a thorough review of its standards and that some issues raised in this paper are being addressed in this context.

205. The project team has concluded that it would be desirable for FATF to provide more clarity on some issues that arise in relation to NPMs. It is understood that some of those issues are already being addressed in the context of the preparation of the fourth evaluation round.

206. When discussing the questions listed below, the responsible working groups should take into account not only aspects related to the prevention of ML and TF, but also the positive and beneficial effects of NPMs (*e.g.*, financial inclusion, shifting transactions from the informal to the formal sector, promotion of competition and economic growth in national markets) as well as legitimate market demand and private sector concerns in order to find an appropriate balance.

207. In all cases the cost/benefit ratio should be taken into account when making policy decisions on NPMs. Decision makers should carefully consider *e.g.*:

- Whether the AML/CFT benefit justifies the potential extra costs and efforts that may arise for institutions as well as for supervisors, FIUs or other agencies.

- Whether there is a risk that specific measures might lead to significant disadvantages for NPM customers (*e.g.*, regarding cost or "convenience" of the NPM service) and whether these potential disadvantages might tempt some customers to make their payment transactions through unregulated payment service providers instead.

208. Policy decisions should strive to find the right balance between an efficient and comprehensive AML/CFT regime and legitimate market demand and private sector concerns.

Questions relating to simplified CDD:

1. Should Recommendation 5 provide for an exemption from CDD measures in cases of "low risk"? (Recommendation 5)

209. Recommendation 5 recommends that "*financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.*"

210. Furthermore, Recommendation 5 recommends that "*financial institutions* ***should apply each of the CDD measures*** *(as listed in Recommendation 5) but may* ***determine the extent of such measures on a risk sensitive basis*** *depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances,* ***where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures***."

211. The standards do not provide a definition of "reduced or simplified CDD measures", and they do not explicitly exclude exemptions from this term either. A number of jurisdictions currently grant institutions a full exemption from CDD measures in designated low risk cases. While this has been criticised to be not in line with Recommendation 5 in some mutual evaluations, there are also others (including a number of jurisdictions, organisations such as the World Bank and private sector representatives) that take the view that Recommendation 5 does (or should) provide the possibility to grant exemptions from CDD measures in low risk cases.

212. In the context of the review of the standards, the FATF will be proposing some changes to the standards that aim at addressing these concerns. The following aspects should be taken into account:

213. Exemption from verification:

- The overall risks of a product or service can also be mitigated by other means such as applying account and transaction limits. Imposing very restrictive limits on the transactions or other functionalities may have an even more deterring effect to would-be launderers than the prospect of being verified. Furthermore, intensive monitoring can help mitigate the ML risk of products as well.

- In some jurisdictions, verification of the customer´s identity may be difficult to accomplish, especially where ID documentation or other reliable documentation is not available for a great part of the population.

- Verification can also prove to be a financial burden for institutions or customers (*e.g.*, where customers must travel a long distance to the bank or vice versa to be verified), deterring customers and institutions alike, and potentially endangering the economic success of individual NPM providers.

- Case studies indicate that criminals were able to launder money even where verification had taken place, *e.g.*, by using stolen or fake identities, or strawmen.

214. Exemption from identification:

- Unlike verification, identification does not seem to cause a lot of cost or effort; the NPM provider simply needs to ask the customer's name.

- In the case of additional cardholders, can it be acceptable to exempt institutions from the identification of the additional cardholders (*e.g.*, if the primary cardholder is thoroughly identified and verified, and other measures and systems such as monitoring are in place)?

2. Is the application of simplified CDD acceptable for non-face-to-face business models? (Recommendations 5 and 8)

215. FATF should provide clarity whether non-face-to-face business models automatically qualify as "high risk scenarios" in the sense of Recommendation 5. While FATF experts have recently discussed this, there is no official statement yet that "specific risk" should not automatically equate with "higher risk" in the sense of Recommendation 5. It would be helpful if FATF could provide greater clarity on this by amending the standards, taking into account the following aspects:

- The approach to risk assessment chosen in this report (and the 2006 report) suggests that all risk factors and all mitigants should be taken into account in order to find an overall risk rating of an individual product or service. It would be against this approach to assess a product as high risk just because it features one particular risk factor (*i.e.*, non face to face), without looking at the all the other risk factors and mitigants.

- Several NPM providers currently apply simplified CDD to non face to face business models and would be seriously affected if this practice was declared inacceptable. Private sector representatives have indicated that this might jeopardize the commercial viability of some NPM services.

Questions relating to the treatment of agents:

3. Should agents of NPM providers be subject to regulation and own AML/CFT obligations? (Recommendation 23, Special Recommendation VI)

216. Depending on the type of activities carried out by agents, they can play a very important role in the execution and completion of a payment transaction. Compared to more traditional financial services, the use of agents to carry out functions related to AML/CFT appears to be more common among NPM providers. Such agents may be required as an intermediary or an interface between traditional financial services and more "virtual" payment services. Using agents may also be an effective and inexpensive alternative to opening branches for NPM service providers, especially when providing NPM services abroad.

217. The FATF 40 + 9 Recommendations do not require agents to be subjected to AML/CFT obligations in their own right. While some jurisdictions have recently suggested that this might constitute a gap in regulation, others consider the current approach appropriate and sufficient.

218. FATF should consider whether the standards should more explicitly address issues relating to the effective oversight of agents carrying out key operational functions, either through direct supervision or through indirect supervision carried out by the principal

219. When making this consideration, the following aspects should be taken into account:

- FATF should consider providing guidance to NPM providers on how to design the contractual relationship with their agents and to enable supervisors to control whether the institution fulfils its AML/CFT obligations through its agents. While some guidance has already been introduced for Money Service Businesses (*e.g.*, the concepts of "know your agent", agent

monitoring and agent training),[89] it remains unclear whether FATF considers this guidance applicable for other financial institutions (such as NPM providers) as well.

- Where agents are subjected to AML obligations, this should not result in a reduction of the principals´ own AML obligations.

- Suspicious transaction reporting: agents are often the only persons having actual face-to-face contact to the customer. Valuable information for suspicious transaction reporting (*e.g.*, suspicious customer behaviour) may therefore only be available to the agent. Such information may be lost or delayed if the agent has no reporting obligations or needs to report to the principal only.

- A reporting obligation for agents should not result in a reduction or waiver of the institution´s own obligation to file suspicious transaction reports. The financial institution may have additional information on the customer and his transactions that is not available to the agent, and may therefore be able to detect suspicious transactions that would not be noticed by an agent.

- Furthermore, FATF could consider which authority the principal and/or agent should be reporting to if agents located in a different jurisdiction than their principal are subjected to reporting obligations: the FIU in the principal´s ("home") jurisdiction; or the FIU in the agent´s ("host") jurisdiction; or double reporting to both jurisdictions?[90]

- Staff training: where agents are subjected to AML/CFT obligations, they should also be required to appropriately train their staff. This training may also be provided by the principal.

- Cost of compliance: where new AML obligations are imposed on agents, this may lead to additional costs and efforts, rendering the service less attractive for agents and/or customers. However, in business models where agents currently already are subject to contractual AML obligations towards their principal, it is unclear whether subjecting them to legal (rather than contractual) AML obligations should effectively result in a relevant increase of costs and efforts.

- Subjecting agents to direct legal AML/CFT obligations may potentially serve as a strong disincentive to act as an agent, potentially making it difficult for NPM providers to find agents and thereby reducing the number of access points to regulated and supervised NPM service providers.

- Efficiency of oversight: if agents are regulated and subjected to AML/CFT obligations, there will be a significant increase in the number of entities to be supervised by the financial supervisors. There are doubts whether this can be accomplished effectively in all cases.

89 FATF (2009)

90 For example, Jersey has issued guidance that agents should report to both FIUs.

4. How should the term "agent" be defined (Recommendation 9, Special Recommendation VI)?

220. Regarding the term "agent", the first difficulty is to find a valid delineation to the terms "outsourcing" and "reliance" or "third party introduction" (as addressed by Recommendation 9). The project team understands that this issue is currently being addressed within FATF.

221. Secondly, FATF does not define the types of activities that can be considered as creating an agency relationship. For example, exchangers used in digital currency business models may argue that they are independent businesses trading in electronic currency. Sellers of prepaid funds (*e.g.*, retailers selling prepaid cards or cash vouchers) might argue that they are just merchants, acting outside the financial sector.

Other issues:

5. Should the scope of Special Recommendation IX be expanded to include "electronic money" or "stored value", especially prepaid cards? (Special Recommendation IX)

222. Special Recommendation IX recommends that "countries should have measures in place to detect the physical cross-border transportation of **currency and bearer negotiable instruments**, including a declaration system or other disclosure obligation."

223. The 2006 report identified the cross-border movement of prepaid cards as a potential ML risk. The project team still considers this a significant potential risk, even though only few case studies have been submitted to prove that criminals have made use of that potential typology in the past.

224. In order to control and counter the cross-border movement of stored value, it would be helpful for customs authorities if they could make use of the tools that have been implemented for the cross-border movement of cash and bearer negotiable instruments according to Special Recommendation IX, such as a declaration or disclosure system and the possibility to confiscate funds. However, in most jurisdictions, these tools (that have their origin in Special Recommendation IX) are only applicable to currency and bearer negotiable instruments, which means that prepaid cards do not have to be declared when crossing borders.[91]

225. Most jurisdictions do not classify prepaid cards, or other means of "stored value" or "electronic money", as cash or bearer negotiable instruments in the sense of Special Recommendation IX. In order to be able to subject these cards to cross-border controls, it would therefore be necessary to widen the scope of Special Recommendation IX (and resulting from that national custom laws) to include such cards as well (alternatively, the text of Special Recommendation IX might remain unchanged, but the definition of either "cash" or "electronic money" might be widened to include stored value or electronic money). When considering expanding the scope of Special Recommendation IX, the following aspects should be taken into account:

- There are currently different opinions whether Prepaid cards should fall under the scope of Special Recommendation IX. While some jurisdictions stress the point that such cards

---

[91] Only few jurisdictions apply these rules to prepaid cards. For example, section 12a of the German Customs Administrative Act (*Zollverwaltungsgesetz*) applies cross-border controls to "cash and equivalent means of payment" including a.o. "cheques, bills of exchange, precious metals and stones and electronic money" (section 1, para 3a *Zollverwaltungsgesetz*).

resemble cash in many ways, others find them to be a type of debit or credit card, which were intentionally kept outside the scope of Special Recommendation IX.

  - Prepaid cards resemble cash in that they are anonymous, represent a certain currency value and can be widely used for the purchase of goods or services. The cards are paid in advance (no credit system) and can be transported across borders.

  - On the other hand, prepaid cards are also similar to the use of debit or credit cards, which undoubtedly do not fall under the scope of Special Recommendation IX. The value of prepaid cards is usually not stored on the card itself, but on a server, with the card being only an access device to the funds.

- It should be examined further whether the reasons that excluded credit and debit cards from the scope of Special Recommendation IX are valid for prepaid cards as well.

- Effectiveness: Currently, there are still technical difficulties with the verification of prepaid cards. It is unclear how custom officials would determine the actual value that is stored on a card. Would card readers have to be installed, and would these work for all technical standards from different card providers? However, technical challenges may be overcome once a legal foundation has been laid for cross-border controls for prepaid cards.

- Where prepaid cards can be transported across borders with no or only minimal funds on it, and then be funded (or "activated") after they have arrived at their destination, this can also effect the efficiency of a cross-border declaration regime for such cards.

6. Should Recommendation 10 include IP addresses for transactions initiated through a personal computer?

226. There is currently no explicit requirement under Recommendation 10 to retain the IP addresses of personal computers through which a payment transaction is initiated. While most NPM providers would most likely do so in their own interest, there are reports from law enforcement about providers who do not retain the IP addresses of their customers, or delete them too soon (*i.e.*, before the 5-year period suggested by Recommendation 10). The FATF should take note of this issue and consider adding the IP address to the list of examples of "necessary records on transactions" in crit. 10.1 of the Methodology.

7. Updating this study

227. Taking into account the continuous development in the sector of NPMs, regarding the technical development as well as the corresponding reaction of legislators and responsible authorities, the project team suggests that this study be updated after an appropriate period of time. Depending on future developments in certain sectors, and on future case studies detected, it may be reasonable to alternatively publish separate typologies reports on single categories of NPMs (*e.g.*, typology report on prepaid cards).

APPENDIX A: SUPPLEMENTAL NPM QUESTIONNAIRE RESULTS AND ANALYSIS

This section gives an overview of the responses by a total of 37 jurisdictions plus the European Union Commission to the questionnaire issued by the project team. The majority of the respondents identified NPMs in their jurisdiction with prepaid cards being most popular (34 of the countries have such providers), then followed by IPS providers with 17 countries and mobile payment services with 16 countries.

The summary of the information provided by each jurisdiction is provided in the following tables and is presented by NPM category, that is, prepaid cards, Internet payment services and mobile payment services.

- Table A: Short description of the NPM and market (when provided)
- Table B: Information on regulatory provisions and any additional information
- Table C: AML/CFT provisions can derive from regulations in place or from business practice
- Table D: Reports of AML/CFT cases or if any illegal operators have been found

Prepaid Cards

Prepaid cards is the largest NPM category with thirty-four countries (more than double the number (14) of countries identified in 2006) reporting its presence in their jurisdiction. All prepaid cards are issued by financial and credit institutions. However, the prepaid card programs are often managed by third parties that are not, in some instances, directly covered by the AML/CFT regime. Information regarding the market size is rarely available and when provided varies extensively, that is 300 to over 100 million card holders.

Thirty-three out of 37 jurisdictions reported some form of licensing and registration requirements, as well as supervision and AML/CFT provisions for prepaid card issuers and program managers. One country reported no licensing or registration requirements but indicated that such providers were supervised. Some countries such as United States and Mexico are currently in the process of making changes to their legislation and regulations to ensure a better AML/CFT coverage of such organisations.

Twelve countries indicated that it was possible to acquire prepaid cards anonymously in cases where the maximum account balance was limited. For other countries, it is not possible to do so.

A total of 18 case studies included in this report were provided by seven different countries. Seven additional countries referred cases for which not enough details were provided or it was impossible to provide them because of legislative limitations. All countries reported that no illegal operator was known to operate in their jurisdiction.

A. Description of Prepaid Cards

Countries	Short description of NPM	Examples of limits
Argentina	Prepaid cards are offered by about 7 providers; some cards issued are associated to a bank account, and for the other prepaid product the customer must be a client of the bank to obtain the card. Normal CDD measures must be applied (overall estimate of 929 000 cards and 7 providers)	
Australia	Prepaid cards are offered but no statistics regarding the number of providers and users were provided	Only the prepaid cards issued with a value limit of AUD 1 000 or more are covered by the Australian AML/CTF Act.
Belarus	Prepaid cards are offered by at least two providers and are issued by banks, and therefore fall under the same regulations as banks	
Belgium	About 106 providers mainly issued by banks	
Brazil	Prepaid cards issued by banks jointly with VISA and Mastercard but no further information provided	
Bulgaria	Two providers with about 5 000 cards – regulations are in accordance with EU Directives	
Canada	Six providers with nine products – all issued by banks jointly with credit card providers; cards loaded by online bill payment function from a bank account, cash at MSB agent location or authorised retailer location or financial institution, direct deposit in some instances, card to card transfers through SMS on cell phones; multiple cards can be linked to one account in at least one instance	Varies depending on card type but with maximum balance up to CAD 10 000; daily withdrawal limit up to CAD 2 000; daily purchases up to CAD 2 000; maximum per load up to CAD 10 000
Cayman Islands	One provider (money services business) with about 140 cards – no additional information was provided	
Colombia	2 providers with over 410,000 accounts; cards are issued by financial institutions and are Visa or Mastercard branded; they are used for low value payments; one the available cards is rechargeable	
Denmark	Prepaid cards issued by banks in conjunction with VISA and Mastercard but little information provided as to the features of the products.	
Estonia	No providers in jurisdiction and prepaid cards not used as payment instrument in Estonia – however, one prepaid card company registered in a foreign country and issuing cards in another country were found to be active in Estonia and other countries – that prepaid card company no longer active in Estonia	

Countries	Short description of NPM	Examples of limits
European Union	13 prepaid card issuers operating with e-money license. Of the 3 biggest prepaid products offered, 2 non-reloadable have a maximum limit of 150 EUR and one is a Mastercard reloadable prepaid; estimated 164 million cards at end of 2008	When maximum limit of 150 EUR for non-reloadable and 2 500 EUR for reloadable cards – no CDD necessary
France	All credit institutions can issue open-loop prepaid cards (about 1.3 million issued in 2008); most common type of prepaid card funded by bank transfers or credit cards held by parents; Among many other products, one virtual card is loaded with credit card or through SMS on cell phone; one other card is used for international money transfers and managed from the Internet or a mobile phone by SMS and is funded by credit card or mobile phone... latter can only be purchased in France but will be soon available to other European customers	First type is reloadable up to 600 EUR but initial load amounts no more than 100 EUR; for virtual card, transactions must be under 150 EUR; international money transfer card can be used for maximum 6 000 EUR per year for both receiving and sending (total)
Germany	About 100 providers and 300 000 to 500 000 cards – most of the cards issued by banks, often in association with retail companies, and can be used at ATMs and POS; also have some prepaid cards that are solely virtual, *i.e.,* only used online and no physical card provided to client	
Gibraltar	Two providers with 70 000 cards (one is only marketed in the UK and the other one is marketed in EU and EEA); due diligence limited to registered cards only	
Italy	180 providers with over 8 million cards for use at ATMs and credit card payment systems - various types including ones issued by post offices in Italy which can receive payments by one major IPS provider and can be funded by cash, transfer of funds from other card holder; another one issued by a bank can be funded by cash at bank branches, at ATMs belonging to same bank as issuer of the card, through Internet and mobile banking	Post office prepaid card is reloadable for a maximum of 3 000 EUR; another card can have a maximum load of 10 000 EUR; another one reloadable up to 5 000 EUR
Japan	8 major e-purses companies with over 105 million accounts; also referred to as prepaid certificates; funded and redeemed through bank transfers and credit cards; available at convenience stores, vending machines and department stores etc.	
Lebanon	Issued by banks and financial institutions and Visa or Mastercard branded with over 39 000 accounts; mostly purchased and used by individuals for Internet purchases	On average, total balance of USD 300
Luxembourg	2 providers – one provider estimated at 200 000 reloadable cards; another card is provided through EPT (postal services) which must be linked to a personal account at EPT	
Macao	Only one prepaid product and no further information provided with estimated 304 accounts – only credit card institutions can issue prepaid cards	
Mexico	6 credit institutions (4 in process) with overall number of over 2.6 million which provide anonymous and personalised cards	

Countries	Short description of NPM	Examples of limits
Netherlands	3 providers (2 offering only non-reloadable cards and one reloadable card used for payroll); issuers of prepaid cards are licensed as a credit institution or as an electronic money institution	Non-reloadable cards are from 5 to 50 EUR; Payroll prepaid card has a total maximum balance of 10 000 EUR and a daily maximum of 5 000 EUR
Norway	Prepaid card issued by all commercial and savings bank. And VISA mentioned as a prepaid but no further information provided (140 banks issued about 6 million)	
Peru	No providers seated in jurisdiction and no regulations currently exist but are under consideration	
Philippines	24 banks (including branches of foreign banks) have issued prepaid/cash cards; providers are considered electronic money issuers (EMIs) which are required to determine individual and consolidated balances of their e-money instruments; a total of over P350 million outstanding balance as of December 2009 and February 2010 in one instance and over 500 000 card holders for one provider (info not provided by other two providers) – see questionnaire response for more info on legislative framework	Aggregate monthly load limit of P100 per e-money (or card) holder – deemed very low
Portugal	5 providers and about 75 500 accounts; one is used by corporations which provide them to employees;	one reloadable card only used in Portugal has a maximum balance of 15 000 EUR, a maximum payment of 5 000 EUR or 20 transactions per day
Republic of Armenia	Six banks have issued over 1650 cards; only banks can issue prepaid cards	
Republic of Poland	4 types of prepaid cards all issued by banks licensed under Polish law and have either the VISA or Maestro logo. No further information provided in terms of limits, funding and withdrawal.	
Russia	18 providers with over 2 million cards; one of provider distributes the card on website, post office and couriers and it can be funded through mobile payments; some of the cards are virtual	
Singapore	The banks are fully liable for the stored value collected (more than 20 providers and over 15 million open-loop prepaid cards in circulation); one provider uses contactless technology primarily in transport sector and small retail (close to 10 million cards); another provider uses smart card technology retail purchases (close to 6.5 million cards)	
Slovak Republic	12 providers (banks) have issued almost 4 million cards; agents can serve as intermediaries and are covered under the Payment Services Directive (2007/64/EC)	
South Africa	Four different card types all issued by one bank and branded by Visa; over 100 000 cards	

Countries	Short description of NPM	Examples of limits
St. Vincent & the Grenadines	Two providers have issued over 16 000 cards; prepaid debit cards are only issued by local banks and there no intermediaries	
Sultanate of Oman	All prepaid are bank issued of which 2 are Visa International linked. No further information provided on products. (4 providers with close to 120 000 accounts)	
Sweden	Swedish credit institutions and Swedish financial institutions are allowed to issue prepaid debit cards.	
Ukraine	Not much info provided – just stats regarding STRs and possible cases involving prepaid cards	
United Kingdom	FSA regulates e-money issuers. Not all issuers are also providers of prepaid cards	
United States	Federal Reserve estimated that there were USD 13,3 billion worth of open-loop prepaid card purchase transactions in the US in 2006 (compared to $2,4 trillion for credit cards) – many different prepaid cards are available and can be funded using wire transfers or with cash at agents locations; some programs are managed by third parties who are responsible to identify customers and provide all transaction data to the issuing bank and notify the bank of suspicious transactions; some issuing banks manage their own programs; a new regulation currently under consideration, would require among other things that certain non-bank businesses managing prepaid card programs register with the US federal government	

B. Access to Activity

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Argentina	Y	Y	
Australia	N	Y	
Belarus	Y	Y	
Belgium	Y	Y	
Brazil	Y	Y	
Bulgaria	Y	Y	

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Canada	Y	Y	Prepaid cards are not explicitly covered under Canada's AML/CTF regime but most issuers and distributors are covered
Cayman Islands	Y	Y	
Colombia	Y	Y	
Denmark	Y	Y	
Estonia	n/a	n/a	
European Union	Y	Y	
France	Y	Y	
Germany	Y	Y	Institutions issuing e-money must verify identity of customer and record it (although not needed to do it by means of reliable documents) for all types of cards – even when non-reloadable and under 150 EUR or reloadable and under 2 500 EUR within one year
Gibraltar	Y	Y	
Italy	Y	Y	
Japan	Y	Y	
Lebanon	Y	Y	
Luxembourg	Y	Y	
Macao	Y	Y	
Mexico	Y	Y	
Netherlands	Y	Y	
Norway	Y	Y	
Peru	n/a	n/a	
Philippines	Y	Y	
Portugal	Y	Y	
Republic of Armenia	Y	Y	
Republic of Poland	Y	Y	

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Russia	Y	Y	
Singapore	Y	Y	
Slovak Republic	Y	Y	
South Africa	Y	Y	
St. Vincent & the Grenadines	Y	Y	
Sultanate of Oman	Y	Y	
Sweden	Y	Y	
Ukraine	no info	no info	
United Kingdom	Y	Y	
United States	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers	Y	

C. AML/CFT Provisions

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Argentina	Y	Y	14	Y
Australia	Y	Y	Yes but no exact number available	Y
Belarus	Y	Y	1 348 (June 1, 2009 to May 31, 2010)	n/a
Belgium	Y	Y	16	Y
Brazil	Y	Y	951	n/a
Bulgaria	Y	Y	none	Y
Canada	Y for issuing banks; currently N for 3rd party program managers if not an	Y for issuing banks; currently N 3rd party program managers if not an	10 re open-loop & 80 re closed-loop	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
	MSB	MSB		
Cayman Islands	Y	Y	320 in 2008/09	n/a
Colombia	Y	Y	96 re open-loop 22 re closed-loop	Y
Denmark	Y	Y	none	Y
Estonia	n/a	n/a	n/a	n/a
European Union	Y	Y	none	Y
France	Y	Y	none	Y
Germany	Y	Y	25	Y
Gibraltar	Y	Y	42	Y
Italy	Y	Y	122	Y
Japan	N	Y	none	N
Lebanon	Y	Y	none	Y
Luxembourg	Y	Y	none	Y
Macao	Y	Y	40	Y
Mexico	Y	Y	5	Y
Netherlands	Y	Y	none	Y
Norway	Y	Y	Not able to distinguish	Y
Peru	n/a	n/a	n/a	n/a
Philippines	Y	Y	301 in 2009	Y
Portugal	Y	Y	none	Y
Republic of Armenia	Y	Y	8	Y
Republic of Poland	Y	Y	none	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Russia	Y	Y	none	N
Singapore	Y	Y	85	Y
Slovak Republic	Y	Y	none	Y
South Africa	Y	Y	48 since July 2009	Y
St. Vincent & the Grenadines	Y	Y	none	Y
Sultanate of Oman	Y	Y	details with Royal Oman Police	Y
Sweden	Y	Y	none	Y
Ukraine	no info	no info	2107	no info
United Kingdom	Y	Y	105	Y
United States	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers; 836 reported in 2008 by banks, MSBs and securities firms	Y

D. AML/CFT Cases – Illegal operators

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Argentina	n/a	N	n/a
Australia	Y	Y	N
Belarus	N	N	unknown
Belgium	N	Y	N
Brazil	n/a	N	N
Bulgaria	Y	N	N
Canada	N	Y	N

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Cayman Islands	N	N	unknown
Colombia	Y	Y	none
Denmark	Y	N	Cannot be disclosed
Estonia	N	One international case already provided by other country	n/a
European Union	Y	N	n/a
France	N	N	none
Germany	N	Y	none
Gibraltar	Y	N	N
Italy	Y	4 recurring schemes	N
Japan	Y	N	N
Lebanon	N	N	N
Luxembourg	N	N	N
Macao	N	2 cases which appear to involve bank debit cards (not sure if they are prepaid) or credit cards	N
Mexico	Y	No examples provided but indicated 3 formal complaints and 10 intelligence reports	N
Netherlands	Y	N	One provider offered or wanted to offer service without a license
Norway	N	N	N
Peru	n/a	n/a	n/a
Philippines	N	Y	N
Portugal	N	N	N
Republic of Armenia	Y for cards with maximum load of 1 300 USD	N	N
Republic of Poland	N	N	N

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Russia	Y for cards less than 500 USD	N	N
Singapore	Y for cards with load limit of 1 000 USD or less	N	N
Slovak Republic	N	N	No info provided
South Africa	N	No details provided but mentioned that cases usually involve 419 scams (telemarketing fraud) and ACB credit fraud	N
St. Vincent & the Grenadines	N	N	N
Sultanate of Oman	N	No details provided but referred to phishing and skimming cases – details with Royal Oman Police	N
Sweden	N	N	N
Ukraine	no info	2 schemes and 2 cases provided but not very clear	no info
United Kingdom	N	2 generic examples – not real cases	N
United States	Y (Mastercard and Visa limit anonymous cards to 500 USD and 750 USD respectively)	Y	N

Internet Payment Services

The number (17) of countries reporting the presence of IPS providers remains almost the same as the one reported (15) in 2006. These refer to services which include online payments to merchants, to individuals (p2p) which are account-based. They can be funded by bank transfers, credit card, prepaid card, other IPS accounts and digital currency providers. Three additional countries only reported the presence of online banking services which are directly linked to bank accounts and not covered in this report.

Nineteen out of 37 jurisdictions reported some form of licensing and registration requirements, as well as supervision and AML/CFT provisions for IPS providers. One country reported no licensing or registration requirements but indicated that such providers were supervised. Only four countries indicated that it was possible to open IPS accounts anonymously under certain conditions such as when transactions are conducted under a low threshold.

A total of 14 case studies included in this report were provided by seven different countries. Five additional countries referred cases for which not enough details were provided or it was impossible to provide them because of legislative limitations. All countries for the exception of two countries reported that no illegal operator was known to operate in their jurisdiction.

A. Description of Internet Payment Services

Countries	Short description of NPM
Argentina	Cannot determine the numbers – same regulations than for financial institutions
Australia	A few providers are operating in this jurisdiction but no statistics were available
Belarus	A few providers appear to be operating in this jurisdiction and to fall under same regulations as banks but response to questionnaire was not clear
Belgium	No stats re providers and number of accounts
Brazil	2 providers
Bulgaria	Three providers with a total of about 45 000 accounts
Canada	One Internet payment services provider • Funding through local bank deposits, bank transfers (domestic & international), credit and debit cards • Redemption through prepaid cards, bank transfers (domestic and international) and cheques Four digital currency exchangers
Cayman Islands	No providers – however, such providers would be considered money remitters and therefore would be covered by Cayman Islands' Money Services Law
Colombia	Online payment service providers are not authorised in Colombia, therefore not subject to regulation and supervision; however, some online payment service providers seating in other jurisdictions are active in Colombia
Denmark	No info regarding online payment services
Estonia	11 credit institutions provide online banking services (not covered in this report) – not clear if it also includes online payment services; however, a new legislation which should be effective by the end of May 2010 will cover new payment institutions and electronic money institutions
European Union	18 online payment service providers in the EU (over 90 million accounts but not all active) – two main ones have 65 million and 10 million accounts respectively
France	Few online payment services in France (23 million customers by end of 2009)
Germany	No Internet payment system provider seated in jurisdiction but a number of IPS seated in

Countries	Short description of NPM
	European Economic Area (EEA) conducting business in Germany – licensed through the "European passport"
Gibraltar	No legislation currently in force requiring providers to register
Italy	One main provider – no other info provided
Japan	No info about providers
Lebanon	No providers seating in jurisdiction
Luxembourg	Only one provider – about 60 million in Europe and about 18 million that are active
Macao	Information provided appears to involve online banking services and not online payment services such as IPS providers covered in this report
Mexico	No information provided
Netherlands	One IPS linking customer's bank account to online purchases; also allowing payments to other Dutch bank accounts – 45 million transactions made in 2009 by 10 million bank accounts with a total turnover of 3.4 billion EUR
Norway	Information appears to be referring to online banking services (140 banks and 12 million accounts?)
Peru	No providers seated in jurisdiction and no regulations currently exist but are under consideration
Philippines	No statistics provided as both online banking services (not covered in this report) and online payment services cannot be distinguished; only banks were mentioned for their online banking services
Portugal	Not aware of any online payment service seated in jurisdiction
Republic of Armenia	No providers yet but draft legislation has been prepared to cover such providers
Republic of Poland	No info provided
Russia	About 23 providers – two main ones sharing about 90% of the market; total of about 13 million accounts; accounts can be funded through cash-in terminals (cash is deposited at the terminals and funded into e-money account by providing account number), post office, prepaid cards and e-currency exchangers
Singapore	MAS does not regulate non-FI online payment services and therefore does not have relevant info on them.
Slovak Republic	Provided info on both online banking services (not covered in this report and online payment services) for a total of 21 providers – number of online payment services not clearly identified
South Africa	No providers but Banks Act would cover such accounts since such providers would need to obtain a bank licence or partner with a bank
St. Vincent & the Grenadines	No providers
Sultanate of Oman	23 providers with almost 80 000 accounts – however appears to refer to online banking services and MSB services (*i.e.,* related to remittances?)
Sweden	Swedish credit institutions and Swedish financial institutions are allowed to offer online payment services – no other info provided
Ukraine	No information available as the online payment service is just about to be established
United Kingdom	Three main providers
United States	One main provider reported to have 81 million active accounts, and others are operating in the US

B. Access to Activity

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Argentina	Y	Y	
Australia	N	Y	
Belarus	Y	Y	
Belgium	Y	Y	
Brazil	N	N	
Bulgaria	N	N	
Canada	Y	Y	IPS and digital currency exchangers considered money services businesses – and therefore need to register with FINTRAC and required to report suspicious transactions
Cayman Islands	Y	Y	
Colombia	N	N	
Denmark	n/a	n/a	
Estonia	Y	Y	
European Union	Y	Y	
France	Y	Y	
Germany	Y	Y	
Gibraltar	n/a	n/a	
Italy	Y	Y	
Japan	n/a	n/a	
Lebanon	n/a	n/a	
Luxembourg	Y	Y	
Macao	Y	Y	
Mexico			
Netherlands	Y	Y	
Norway	Y	Y	
Peru	n/a	n/a	
Philippines	Y	Y	
Portugal	n/a	n/a	
Republic of Armenia	n/a	n/a	
Republic of Poland	n/a	n/a	
Russia	N	N	

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Singapore	n/a	n/a	
Slovak Republic	Y	Y	
South Africa	Y	Y	
St. Vincent & the Grenadines	n/a	n/a	
Sultanate of Oman	Y	Y	
Sweden	Y	Y	
Ukraine	n/a	n/a	
United Kingdom	Y	Y	
United States	Y	Y	Considered money transmitters and therefore covered by AML/CTF regime

C. AML/CFT Provisions

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Argentina	Y	Y	none	Y
Australia	Y	Y	Yes but no exact number provided	Y
Belarus	Y	Y	n/a	n/a
Belgium	Y	Y	3	Y
Brazil	N	N	none	N
Bulgaria	N	Y	3	Y
Canada	Y	Y	150	Y
Cayman Islands	Y	Y	none	Y
Colombia	N	N	5	N
Denmark	n/a	n/a	n/a	n/a
Estonia	Y	Y	29 received from providers of alternative payment services	Y
European Union	Y	Y	none	Y
France	Y	Y	70	Y
Germany	Y	Y	61	Y
Gibraltar	n/a	n/a	n/a	n/a
Italy	Y	Y	2	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Japan	n/a	n/a	none	n/a
Lebanon	n/a	n/a	n/a	n/a
Luxembourg	Y	Y	About 500	Y
Macao	Y	Y	7 but possibly related to online banking and not IPS	Y
Mexico	n/a	n/a	317 re Internet fraud	n/a
Netherlands	Y	Y	Only one in 2006	Y
Norway	Y	Y	n/a	Y
Peru	n/a	n/a	n/a	n/a
Philippines	Y	Y	n/a	Y
Portugal	n/a	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a	n/a
Russia	N	Y	n/a	N
Singapore	n/a	n/a	1021 mostly related to goods traded using online payment services	n/a
Slovak Republic	Y	Y	7 between 2005 and 2008, none in 2009	n/a
South Africa	Y	Y	none	Y
St. Vincent & the Grenadines	n/a	n/a	n/a	n/a
Sultanate of Oman	Y	Y	none	Y
Sweden	Y	Y	none	Y
Ukraine	n/a	n/a	n/a	n/a
United Kingdom	Y	Y	73	Y
United States	Y	Y	Over 18,000	Y

D. AML/CFT Cases – Illegal operators

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Argentina	n/a	N	n/a
Australia	Y if under low threshold of AUD 1 000	Y	N
Belarus	n/a	n/a	n/a

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Belgium	n/a	Y	n/a
Brazil	N	N	N
Bulgaria	N	No details provided but mentioned that three cases developed by the FIU involved foreign online payment service providers	n/a
Canada	N	Y	none
Cayman Islands	N	N	N
Colombia	n/a	3 cases but not clear if related to ML through online payment services	n/a
Denmark	n/a	N	n/a
Estonia	N	No details provided but mentioned that typical crimes are phishing and other Internet fraud schemes	N
European Union	Y	N	n/a
France	N	Y	none
Germany	N	Y	Issued two cease-and-desist orders against foreign online payment service providers conducting business in Germany
Gibraltar	n/a	n/a	n/a
Italy	Y	N	n/a
Japan		Y	
Lebanon	n/a	n/a	n/a
Luxembourg	N	Ongoing cases but not able to share info at this point	N
Macao	n/a	n/a	n/a
Mexico	n/a	N	n/a
Netherlands	N/A?	N	5 or 6
Norway	N	n/a	N
Peru	n/a	n/a	n/a
Philippines	N	n/a	N
Portugal	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a
Russia	Y (when registering with two main providers, one can choose between anonymous	N	no info

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
	and registered account – the latter allows more services)		
Singapore		Y	
Slovak Republic	N	N	n/a
South Africa	N	N	N
St. Vincent & the Grenadines	n/a	n/a	n/a
Sultanate of Oman	N	details with Royal Oman Police	N
Sweden	n/a	N	n/a
Ukraine	n/a	N	n/a
United Kingdom	N	N	N
United States	Y	Y	Y (US has prosecuted online payment services that failed to register and failed to obtain licenses)

Mobile Payment Services

The number (16) of countries reporting the presence of mobile payment services providers has tripled in relation to the number (5) reported in 2006. These refer to services that are account-based which can be funded by bank transfers, credit card, prepaid card, and other NPMs. They are the services that use SMS or NFC technology. Two additional countries reported the testing of mobile payment services in their jurisdiction while two other countries only reported online banking services (directly linked to bank accounts) which are really the extension of banking services that are not covered in this report.

Twenty-one out of 37 jurisdictions reported some form of licensing and registration requirements, as well as supervision and AML/CFT provisions for mobile payment services providers. Only three countries indicated that it was possible to open mobile payment service accounts anonymously.

Only three case studies included in this report were provided by two countries. All countries reported that no illegal operator was known to operate in their jurisdiction.

A. Description of Mobile Payment Services

Countries	Short description of NPM	Examples of limits
Argentina	No information provided	
Australia	A number of mobile banking providers are operating in this jurisdiction but no specific statistics were provided regarding the number of accounts	
Belarus	No information provided	
Belgium	One provider recently established offering payments for small purchases and P2P payments; account loaded by bank transfers, credit card or debit card; payments done by SMS or by Internet mobile; considering offering international wire	

Countries	Short description of NPM	Examples of limits
	transfers in the future between Belgium and Northern Africa	
Brazil	One mobile service model is being tested	
Bulgaria	Three providers with a total of about 26 000 accounts	
Canada	Seven providers including five which are an extension of online banking and two that offer mobile banking through SMS – one of the latter, offered by telecommunications company, also offer a prepaid card on which funds can be transferred from mobile banking account; accounts can be funded by credit card, debit or prepaid card, or through wire transfers	Individual transactions limited to 250 CAD and 1 000 CAD is the maximum balance for the account
Cayman Islands	No providers – however, such providers would be considered money remitters and therefore would be covered by Cayman Islands' Money Services Law	
Colombia	No providers in jurisdiction but legislation covers such services which can only be offered by credit institutions	
Denmark	A number of mobile payment providers are available but no details were provided.	
Estonia	3 credit institutions offer mobile banking with over 250 000 accounts (however, nearly 82 000 seem to be inactive); SMS and NFC technology are both used	
European Union	Estimate of 8 providers in EU; accounts can be funded by credit card or bank transfers, and between account holders with the same mobile payment provider; payments done using SMS	
France	No providers yet but mobile payment services using NFC technology are being tested	
Germany	No mobile payments provider available	
Gibraltar	No providers	
Italy	Discussions about offering such services, some initiatives underway but no provider yet established	
Japan	No information provided	
Lebanon	No providers seating in jurisdiction	
Luxembourg	3 providers but no details	
Macao	No information provided	
Mexico	No providers but legislation applied to banking institutions could apply in terms of operational limits	
Netherlands	Two services available that are linked to a bank account and payments are made through SMS; one model using near-field communication (NFC) technology was tested but was not successful	One of them has a limit of 2 500 EUR in payments per year
Norway	2 providers with about 5 million customers	
Peru	Four banks offer online banking services through mobile phones and therefore are covered under AML regime; mobile payment services offered by non-bank entities are not currently regulated but such measures are under consideration	
Philippines	21 providers including banks and one non-bank provider; most of these relate to online banking services done through mobile phones; however, one e-money provider (non-bank institution and a wholly-owned subsidiary of a telecommunications company) offers a digital currency	

Countries	Short description of NPM	Examples of limits
	service (with over 1 million accounts) on mobile phones at the same time as providing digital currency exchange services (cash to e-money and vice-versa); another provider offers SMS technology to banks providing mobile services	
Portugal	Not aware of any mobile payment service seated in jurisdiction	
Republic of Armenia	No providers yet but draft legislation has been prepared and is under discussion.	
Republic of Poland	No information provided	
Russia	A number of different providers with the number of accounts reaching about 15 million in 2009 and the volume of mobile payments reaching about USD 230 million; SMS technology used to purchase services and goods, as well as transferring funds to another mobile payment account holder	
Singapore	There are several mobile payment service operators testing various types of services including ones using NFC technology. MAS does not supervise or regulate such service operators and therefore does not have additional info.	
Slovak Republic	3 providers	
South Africa	One current provider (with 40 000 active accounts) and another one under development	
St. Vincent & the Grenadines	No providers	
Sultanate of Oman	4 providers with over 120 000 accounts offered by telecommunications companies and banks, using SMS at least for one program	
Sweden	Swedish credit institutions and Swedish financial institutions are allowed to offer mobile payment services – no other info provided	
Ukraine	No information available as the mobile payment service is just about to be established	
United Kingdom	The industry has yet to take off in the UK. Mobile phones only used as a communications methods with a payment service provider, rather than the phone being the payment instrument itself.	
United States	Mobile payment services market is still in the start-up stages but some providers are present – some services are linked to bank accounts (extension of online banking) but some are linked to IPS and sometimes offered in combination with prepaid cards or credit card providers	

B. Access to Activity

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)
Argentina	n/a	n/a
Australia	Y	Y
Belarus	n/a	n/a
Belgium	Y	Y
Brazil	N	N
Bulgaria	Y	Y

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)
Canada	Y when offered by banks	Y when offered by banks
Cayman Islands	Y	Y
Colombia	Y	Y
Denmark	Y	Y
Estonia	Y	Y
European Union	Y	Y
France	Y	Y
Germany	Y	Y
Gibraltar	n/a	n/a
Italy	Y	Y
Japan	n/a	n/a
Lebanon	n/a	n/a
Luxembourg	Y	Y
Macao	n/a	n/a
Mexico	Y	Y
Netherlands	Y	Y
Norway	Y	Y
Peru	Y (when linked to bank account)	Y (when linked to bank account)
Philippines	Y	Y
Portugal	n/a	n/a
Republic of Armenia	n/a	n/a
Republic of Poland	n/a	n/a
Russia	Y (banks and telecom companies)	Y (banks) N (telecom companies)
Singapore	n/a	n/a
Slovak Republic	Y	Y
South Africa	Y	Y
St. Vincent & the Grenadines	n/a	n/a
Sultanate of Oman	Y	Y
Sweden	Y	Y
Ukraine	n/a	n/a
United Kingdom	Y	Y
United States	Y	Y

C. AML/CFT Provisions

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Argentina	n/a	n/a	none	n/a
Australia	Y	Y	none	Y
Belarus	n/a	n/a	n/a	n/a

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Belgium	Y	Y	none	Y
Brazil	N	N	n/a	N
Bulgaria	Y	Y	none	Y
Canada	Y when offered by banks	Y when offered by banks	5	Y when offered by banks
Cayman Islands	Y	Y	none	Y
Colombia	Y	Y	none	Y
Denmark	Y	Y	none	Y
Estonia	Y	Y	none	Y
European Union	Y	Y	n/a	Y
France	Y	Y	none	Y
Germany	Y	Y	none	Y
Gibraltar	n/a	n/a	n/a	n/a
Italy	Y	Y	n/a	Y
Japan	n/a	n/a	n/a	n/a
Lebanon	n/a	n/a	n/a	n/a
Luxembourg	Y	Y	none	Y
Macao	n/a	n/a	n/a	n/a
Mexico	Y	Y	n/a	Y
Netherlands	Y	Y	none	Y
Norway	Y	Y	Cannot distinguish	Y
Peru	Y (when linked to bank account)	Y (when linked to bank account)	none	Y (when linked to bank account)
Philippines	Y	Y	194	Y
Portugal	n/a	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a	n/a
Russia	Y (banks) N (telecom companies)	Y (banks & telecom companies)	Y (banks) – none N (telecom companies)	n/a
Singapore	n/a	n/a	n/a	n/a
Slovak Republic	N	Y	One STR in 2009	Y
South Africa	Y	Y	none	Y
St. Vincent & the Grenadines	n/a	n/a	n/a	n/a
Sultanate of Oman	Y	Y	none	Y
Sweden	Y	Y	n/a	Y
Ukraine	n/a	n/a	n/a	n/a
United Kingdom	Y	Y	none	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
United States	Y	Y	31 (2008)	Y

D. AML/CFT Cases – Illegal operators

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Argentina	n/a	n/a	n/a
Australia	Y	N (one case was provided but it was unclear if it was related to the type of mobile payment services covered in this report)	N
Belarus	n/a	n/a	n/a
Belgium	N	N	N
Brazil	n/a	n/a	n/a
Bulgaria	N	n/a	N
Canada	Y	N	N
Cayman Islands	N	Y	N
Colombia	N	N	N
Denmark	Y	N	N
Estonia	N	N	N
European Union	Y	n/a	N
France	N	N	N
Germany	N	n/a	N
Gibraltar	n/a	n/a	n/a
Italy	n/a	n/a	n/a
Japan	n/a	n/a	n/a
Lebanon	n/a	n/a	n/a
Luxembourg	N	N	N
Macao	n/a	n/a	n/a
Mexico	N	n/a	n/a
Netherlands	N	N	none
Norway	N	N	N
Peru	N	N	N
Philippines	N	Y	N
Portugal	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a
Russia	Y	N	N
Singapore	n/a	n/a	n/a
Slovak Republic	N	N	N

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
South Africa	unknown	N	unknown
St. Vincent & the Grenadines	n/a	n/a	n/a
Sultanate of Oman	N	Details available with Royal Oman Police	N
Sweden	n/a	n/a	n/a
Ukraine	n/a	n/a	n/a
United Kingdom	N	N	none
United States	Y	N	none

APPENDIX B: EXCERPTS FROM THE 2006 REPORT ON NEW PAYMENT METHODS

This section provides an overview of the general characteristics and functions of specific New Payment methods, as described in the 2006 typologies report on New Payment Methods. These excerpts are presented in order to provide readers that are not familiar with the general working mechanisms of NPMs, with a general overview of the technical background of these instruments. For more detailed information, interested readers are referred to the 2006 report itself, which contains more information and features additional instructive appendices (www.fatf-gafi.org/dataoecd/30/47/37627240.pdf).

Prepaid cards

Prepaid payment cards provide access to monetary funds that are paid in advance by the cardholder. While there are many different types of prepaid cards that are used in a variety of ways, they typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the funds prepaid for all cards issued. The cards may be issued by, and accounts may be held at, a depository institution or a non-bank organization; pooled accounts would be normally held by the issuer at a bank.

Prepaid cards can be issued for limited or multiple purposes. Limited-purpose or *closed system* prepaid cards can be used for only a limited number of well-defined purposes and their use is often restricted to specific points of sale or for specific services. Examples include merchant-issued gift cards, prepaid long distance service, and mass transmit system cards. These cards may either be limited to the initial value posted to the card (non-reloadable) or may allow the card holder to add value (up to a certain limit) and reuse the card (reloadable). The issuer of the card or its service provider typically operates the network on which the cards can be used. The value on the cards generally is linked to a prepaid account established by the issuer or service provider. Transactions are processed in a similar fashion to transactions involving debit or credit cards.

Multipurpose or *open-system* prepaid cards can be used across a broader range of locations for a wider range of purposes. Such cards may be used on a national or international scale but may sometimes be restricted to a certain geographical area. Multipurpose cards may be used by the person who purchased the card or by someone else. Examples include payroll cards and general purpose "cash cards" for individuals without bank accounts or a credit card. These cards are usually associated with a card payment network, such as Visa or MasterCard, which permits them to be used in the same manner as a debit card to make purchases or to get cash from an automated teller machine (ATM). Some issuers do not require the cardholder to have a depository account. These cards are distributed by merchants, depository financial institutions, and money/value transfer (MVT) systems for a variety of purposes. Most are reloadable.

---

[15] The expression "bank account" used in this box refers to accounts held at financial institutions that are subject to AML requirements.

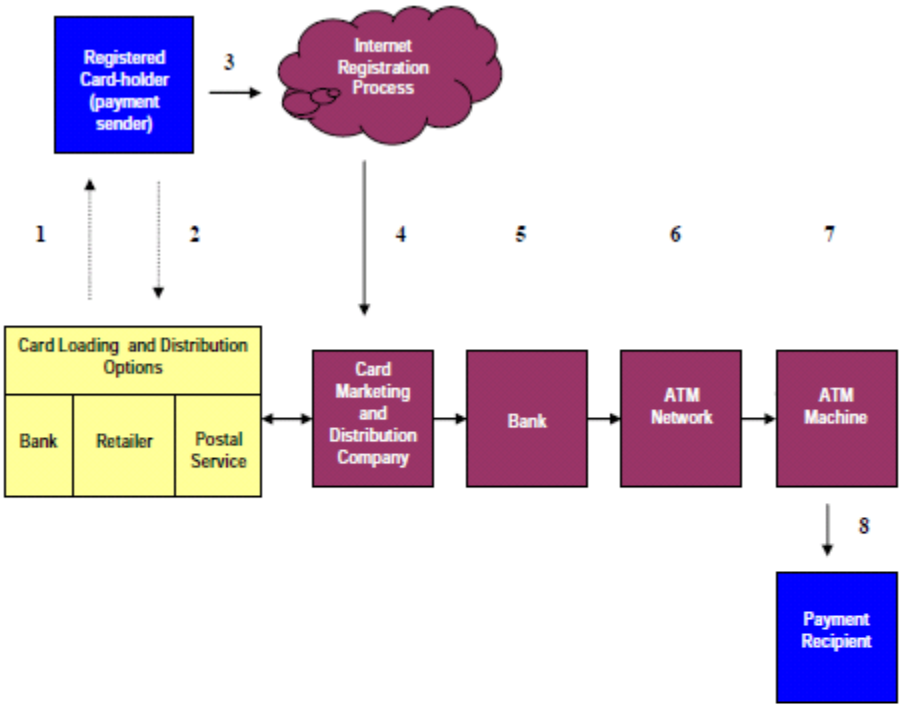


Figure 1 The process of issuing an open-system, magnetic strip, prepaid card varies by issuer. Steps (1), (2), and (3) above may occur in any order. In those three steps an individual completes the registration process for a prepaid card, prepays funds into the card account, and receives the card. Step (4) is the transfer of registration information to the service provider. When a card carries a bank association service mark (as in the case of MasterCard- or Visa-branded cards), the service provider must contract with a bank (5) in order to have access to the global ATM networks (6). Individual ATM machines (7) connect to local networks and often global networks allowing individuals in one country (8) to access funds held in another country.

Electronic purse

An electronic purse, or e-purse (also referred to as a "stored value card" as the value is stored on the card), is value stored electronically in a device such as a card with an integrated circuit chip (called a smart card or chip card).[16] Unlike a card with a magnetic stripe, which stores account information, an e-purse actually stores funds on the card's memory chip. The user is literally carrying his funds with him on the card (hence the name electronic purse).

In some e-purse programs value can be transferred from the card directly to participating merchants or another individual without the transaction going through an account at an intermediary. This may limit the amount of

[16] This definition augments slightly the normal CPSS usage of the term "electronic purse" to also encompass the term "electronic money". For the purposes of this report, the term electronic purse is "a reloadable, multi-purpose prepaid card which may be used for small retail or other payments instead of coins" where the "value is stored electronically in a device such as chip card."

identifying information available with such transactions. To obtain funds from an e-purse payment, however, the merchant or individual must redeem the value from an account held by the e-purse provider at the e-purse issuing institution. As the funds are on the card, no online connection and no cardholder identification are needed to make a payment. The electronic purse function was designed to substitute for cash in everyday situations. Today, electronic purses are mainly used for micropayments such as for public transportation, parking tickets or vending machines.

The development and use of card-based e-purses has declined considerably over the past decade so that very few e-purse systems remain in existence. In addition, these few remaining e-purse solutions are generally not interoperable regardless of the market in which they operate. Only one system, the German GeldKarte that operates in the border area of Germany and Luxemburg (See Figure 2), is known to be used in multiple national jurisdictions. Furthermore, e-purses usually have a limited storing capacity for funds (e.g. the German GeldKarte has a load limit of EUR 200).

Figure 2

Mobile Payments

Mobile payments refer generally to the use of mobile phones and other wireless communications devices to pay for goods and services. Payments are initiated from a mobile communications device using voice access, text messaging protocols (such as short/single messaging service or SMS), or wireless application protocols (WAPs) that allow the device to access the Internet. Authorization often occurs by keying in a unique personal identification number (PIN) associated with the customer or mobile device. Adoption of mobile payments varies from country to country. Use of mobile phones as a means to initiate payments is relatively widespread in Southeast Asia and in some European countries.[17]

Most mobile payment services simply use the phone as an access device to initiate and authenticate transactions from existing bank accounts or payment cards.[18] This is the equivalent of using the Internet to initiate a direct debit or credit transfer from a bank account, or a credit or debit card transaction. This is an extension of traditional payment methods.

New mobile payments: Where mobile payment services are not based on an underlying bank or payment card account, the telecom operator typically acts as a payment intermediary to authorize, clear, and settle the payment.[19] Telecom companies engaged in these activities may not be overseen by a country's central bank or other banking regulator but may be subject to AML/CFT measures.

The telecom operator may either allow the phone owner to charge certain transactions to the phone bill (post-paid) or may permit the phone owner to fund an account held by the telecom operator or other service provider for the purposes of making payments (prepaid). Prepaid mobile payments accounts operate in the same manner

---

[17] See CPSS, "Policy issues for central banks in retail payments," BIS, CPSS #52, March 2003, at http://www.bis.org/publ/cpss52.htm.

[18] See CPSS, "Survey of developments in electronic money and internet and mobile payments," BIS, CPSS #62, March 2004, at http://www.bis.org/publ/cpss62.htm.

[19] Telecom companies offering mobile payment services provide for the settlement of the payment transactions completed via their systems through normal banking channels.

as a prepaid card or an electronic purse. When the phone is used in the same manner as a prepaid card, the phone owner uses the phone as a payment system access device to authorize the deduction of value from the prepaid account. When the phone functions as an e-purse, the prepaid value is stored on the subscriber identify module or SIM card within the mobile phone.

Post-paid and prepaid card-like mobile payments are much more common than e-purse mobile payments. In the case of prepaid mobile payments, telecom providers often offer this service in conjunction with a bank. For example, in the Philippines two telecom companies offer mobile payment services, Globe Telecom and Smart Communications. Smart Communications' Smart Money is co-branded with Banco de Oro. The transactions and funds transfers Smart Money users initiate via their mobile phone are authorized against a prepaid account held at Banco de Oro. Smart Money users can also send cross-border remittances by providing relatives with a MasterCard-branded prepaid card linked to the Smart Money account that can be used to withdraw cash from an ATM.

Globe Telecom serves as the intermediary for funds transfers using G-cash and operates without a bank partner. As a result, Globe customers cannot withdraw funds from their prepaid accounts at ATMs but only over the counter at participating businesses. Figure 3 illustrates a G-Cash funds transfer from one Globe Telecom subscriber to another using SMS. Both G-Cash and Smart Money are subject to AML/CFT regulations (including suspicious transaction reporting) and supervision.

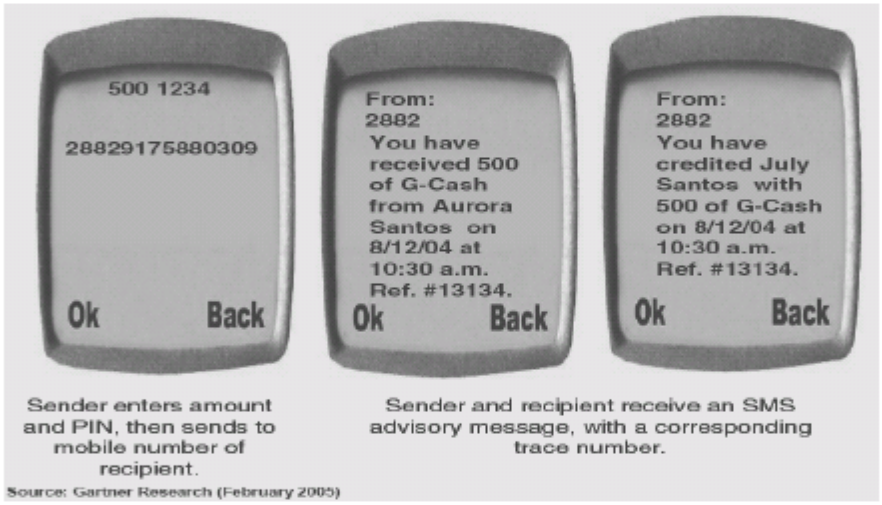


Figure 3 G-Cash Phone-to-Phone Remittance

Internet payment services

The expression "Internet payment services" is generally used to address: (i) payment services that rely on a bank account and use the Internet as a means of moving funds to or from a bank account; and (ii) payment services provided by non-bank institutions operating exclusively on the Internet and that are only indirectly associated with a bank account.

In the former case, Internet payment services refer to traditional payment methods where the Internet is only an innovative channel to exchange the information that is needed to move the funds from one account to another, which allows customers to access their bank accounts from home, 24 hours a day.

Where Internet payment services do not rely directly on a bank account, such as PayPal, individuals can transfer funds, shop online, or participate in online auctions, using a pre-funded account; however, the payment service provider may not be subject to the same AML/CFT measures that apply to banks. The service provider usually

will not have a face-to-face relationship with its customers. Depending upon the accessibility of the Internet payment service, these activities can involve payments or funds transfers across national borders.

Some non-bank Internet payment services allow customers to hold accounts with the payment service provider, while others offer only to send or receive individual payments using the customer's existing bank or credit card account. When non-bank Internet payment services offer customer accounts they may pool those customer funds in a single account at a bank. The account may be held in the name of the service provider. In that case, the bank holding the service provider's account may have no direct relationship with the service provider's individual customers.

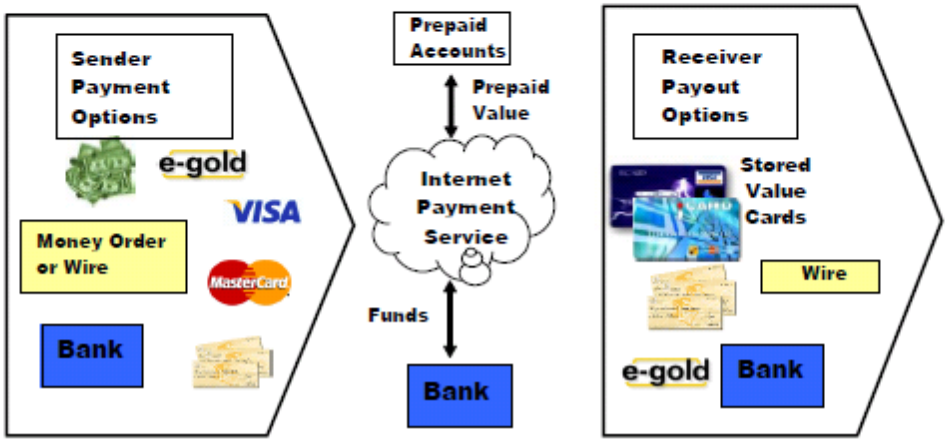


Figure 4

While a limited number of similar products exist in certain countries, PayPal appears to be the most widely used non-bank, Internet-based NPM. PayPal primarily functions as a payments intermediary for individuals and organizations that wish to trade with each other or transfer funds via the Internet. PayPal operates by allowing an individual to set up a pre-paid account in his name with PayPal that can be funded from a credit or debit card or a bank account via a credit transfer. Using those pre-paid funds, individuals can buy items or transfer funds to other PayPal account holders. The payment or transfer of funds occurs as a book-entry transaction between the PayPal accounts. When an individual wishes to access the funds in his PayPal account, he directs PayPal to credit his credit or debit card or bank account via a credit transfer or even a paper check.

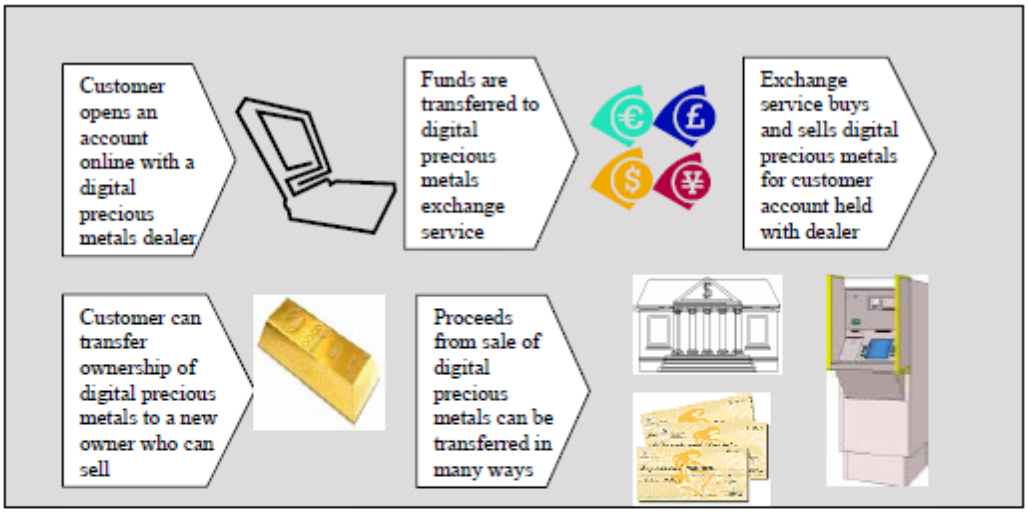
Service providers will differ as to the methods of payment they will accept to initiate a funds transfer, and the methods of payment they will use to distribute funds to the recipient. Figure 4 above illustrates how an individual can use a bank-issued credit card or other traditional payment methods to fund an Internet-based transaction account and subsequently make purchases or transfer all or a portion of the prepaid value to another account holder via book-entry by the service provider. The recipient can then use those funds to conduct additional transactions or withdraw the money via a traditional retail payment method. Online money transfer services set their own terms as what form of payment they will accept from senders and what forms of payment they make available to receivers.

Digital precious metals[20]

Digital precious metals are a relatively new online MVT system that involves the exchange of options or the right to purchase an amount of precious metals at a specific price. These derivatives can be exchanged, like traditional commodity or securities derivatives, between account holders in a digital precious metal service. Consumers purchase a quantity of virtual precious metal holdings based on the current price of the metal on the world commodity exchanges. Once a purchaser has acquired a quantity of the virtual precious metal, those holdings or a portion of them can be transferred either to another individual or a merchant in exchange for goods and services.

The oldest and best known of the digital precious metals dealers is e-gold Ltd., which claims to have almost 2 million accounts.[21] According to e-gold and other digital precious metals dealers, the rationale for using this store of value is to facilitate online transactions without regard for underlying currencies or access to foreign exchange. Transactions involving digital precious metals have immediate finality, which may appeal to online merchants that must pay high credit card interchange fees due to high fraud rates. Some digital precious metals dealers also allow users to maintain anonymous accounts. These traits are concerning to U.S. federal law enforcement agencies.

The transaction process associated with transferring the virtual holdings of precious metals between account holders can involve two separate service providers: the digital precious metals dealer, which maintains the accounts that contain the virtual holdings of precious metals; and the digital precious metals exchange service, which can act as a broker for the digital precious metals that the dealers buy or sell. Some dealers transact directly with account holders. Upon completion of a transaction, the selling account holder transfers ownership of his virtual precious metal holdings to the purchaser and can receive the proceeds of the sale through a variety of traditional and non-traditional payment methods (See Figure 5).



[20] The issuers of digital precious metals use the term "digital currency" to describe the barter arrangement they facilitate. Because of the potential confusion this common industry term would create with the term "e-purse" and "e-money", we have adopted the term "digital precious metals" for this report.

[21] E-dinar is a spin-off of e-gold and is affiliated with the Islamic Mint, a private organization working to revive the gold and silver currencies described in the Koran, the gold dinar and silver dirham. See: www.e-dinar.com.

Figure 5 Buying and selling digital precious metals typically involves working with two separate service provider categories: the digital precious metals exchange service and the digital precious metals dealer.

APPENDIX C: BIBLIOGRAPHY AND RELATED PUBLICATIONS ON NPMS AND ML/TF RISK

- Arthur D. Little (2009), *Global M-Payment Report Update – 2009*, April 2009, www.adl.com/uploads/tx_extthoughtleadership/ADL_Global_M_Payment_Report_Update_2009_Executive_Summary.pdf

- Australian Attorney-General's Department (2006), *Australian AML/CTF Act*, Act No. 169 of 2006 as amended, Table 1, Page 55, Item 23

- Bank for International Settlements (2009), *Statistics on payment and settlement systems in selected countries – Figures for 2008*, December 2009, www.bis.org/publ/cpss88.pdf.

- Basel Committee on Banking Supervision (2001), *Customer due diligence for banks*, section 2.2.6;

- Bester, H., D. Chanberlain, L. de Koker, C. Hougaard, R. Short, A. Smith and R. Walker (2008), *Implementing FATF Standards in developing countries and financial inclusion: Findings and guidelines*, FIRST initiative, South Africa

- Commission of the European Countries (1998), *Proposal for a European Parliament and Council Directive on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions* and *amending Directive 77/780/EEC on the co-ordination of laws, regulations and administrative provisions relating to the taking up and pursuit of the business of credit institutions*, COM(1998)461 final, p. 10; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1998:0461:FIN:EN:PDF

- Commission of the European Countries (2008), *Impact Assessment accompanying the Draft Proposal for a Directive of the European Parliament and of the Council amending Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions*, SEC(2008)2572, p. 5; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2008:2572:FIN:EN:PDF

- De Koker, Louis: "The money laundering risk posed by low risk financial products in South Africa: Findings and guidelines", 2009, Journal of Money Laundering Control, Vol. 12, No. 4

- Direct Express Media (2008), *U.S. Treasury Introducing Direct Express® Debit Card to Social Security Recipients in Western states*, www.directexpress.org/Media/News_9_3_08_West_Announcement.cfm

- FATF (2006), *Report on New Payment Methods*, FATF, Paris, www.fatf-gafi.org/dataoecd/30/47/37627240.pdf

- FATF (2008), *Money Laundering and Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems*, FATF, Paris, www.fatf-gafi.org/dataoecd/57/21/40997818.pdf
- FATF (2009a), *Risk Based Approach: Guidance for Money Service Businesses*, FATF, Paris, www.fatf-gafi.org/dataoecd/45/1/43249256.pdf.
- FATF (2009b), *Mutual Evaluation Report of New Zealand*, FATF, Paris, www.fatf-gafi.org/document/28/0,3343,en_32250379_32236963_43998044_1_1_1_1,00.html
- FATF (2010), *Mutual Evaluation of the Federative Republic of Brazil*, FATF, Paris, p. 98, www.fatf-gafi.org/document/53/0,3343,en_32250379_32236963_45538741_1_1_1_1,00.html
- Federal Register (2010), *Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access, Proposed Rules*, Vol. 75, No. 123, Monday, June 28, 2010, http://edocket.access.gpo.gov/2010/pdf/2010-15194.pdf.
- Finextra (2010), *Safaricom brings M-Pesa to ATMs with Equity Bank partnership*, 18 January 2010, www.finextra.com/news/fullstory.aspx?newsitemid=20963.
- First Data (2009), *First Data Reveals Success Factors for Prepaid Cards in Europe*, 26 November 2009, www.firstdata.com/en_ae/about-first-data/media/press-releases/11_26_09
- Foster K., Meijer E., Schuh S., and Zabek A., (2010), *The 2008 Survey of Consumer Payment Choice*, No 09-10, Federal Reserve Bank of Boston, Boston, www.bos.frb.org/economic/ppdp/2009/ppdp0910.pdf
- Joint Money Laundering Steering Group(2010), *Joint Money Laundering Steering Group Guidance*, Part I Chapter V
- Official Journal of the European Union (2005), *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance)*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF
- Official Journal of the European Union (2007), *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending, Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF
- Official Journal of the European Union (2009), *Directive 2009 2009/110/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives, 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC*, Directive 2009/110/EC; OJ L 267 (10.10.2009), p. 7; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF
- Master Card (2010), *Independent Research Forecasts that the European Open-loop Prepaid Market Will Reach $156bn (€127bn) by 2017*, 3 June 2010, www.mastercard.com/us/company/en/newsroom/independent_research.html

- Payments Council (2010), *Payments Council, The Way We Pay 2010, The UK's Payment Revolution*, www.paymentscouncil.org.uk//files/payments_council/the_way_we_pay_2010_final.pdf,
- Payment News (2010), *MasterCard Releases Prepaid Market Sizing Report*, 12 July 2010, www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html
- Securities and Exchange Commission (2009a), *Form 10-K, Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act for 1934 for the fiscal year ended September 30, 2009, VISA INC*, commission file No. 001-33977 filed 20 November 2009, Washington, USA, www.sec.gov/Archives/edgar/data/1403161/000119312509239249/d10k.htm, *accessed October 2010*.
- Securities and Exchange Commission (2009b), *Form 10-K, Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act for 1934 for the fiscal year ended September 30, 2009, MasterCard Incorporated*, commission file No. 001-32877, filed 18 February 2010, Washington, USA, www.sec.gov/Archives/edgar/data/1403161/000119312509239249/d10k.htm, *accessed October 2010*.
- South African Government Gazette (2010), *National Gazette No 33241 of 04-Jun-2010*, Volume 540, 002.
- South African Reserve Bank (2008), *Guidance Note 6/2008, Issued in Terms of Section 6(5) of the Banks Act, 1990: Cell-phone banking*, Pretoria, South Africa, 2008-05-07, www.reservebank.co.za/internet/Publication.nsf/LADV/18B4D18670F4E8EC422574520032B728/$File/G6+of+2008.pdf, *accessed October 2010.*
- UN Counter-Terrorism Implementation Task Force (2009), *Tackling the Financing of Terrorism*, CFITF Working Group Report, New York, 2009, www.un.org/terrorism/pdfs/CTITF_financing_ENG_final.pdf
- United Nations Development Programme Afghanistan (2009), *Law and Order Trust Fund for Afghanistan (Phase V), [01-10-2008- 31-12-2008] Quarterly project report [3rd Quarter, 1387]* www.undp.org.af/whoweare/undpinafghanistan/Projects/3rdQ08Reports/2009-01-29%20-%20Third%20Quarter%201387%20Progress%20Report%20-%20LOTFA.pdf
- Visa Corporate Site (2010), *Financial Inclusion - Pakistan eases burden of displaced citizens by delivering financial support through Visa*, www.currencyofprogress.com/_media/pdfs/case_studies/VISA_Inclusion-Pakistan.pdf, accessed October 2010
- World Bank (2008), Working paper Nr. 146, *Integrity in mobile phone financial services*, Washington, 2008, p. 18 ss., http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf
- World Bank (2009a), *Preventing Money Laundering and Terrorist Financing A Practical Guide for Bank Supervisors*, Washington, 2009, http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/PMLTL.pdf

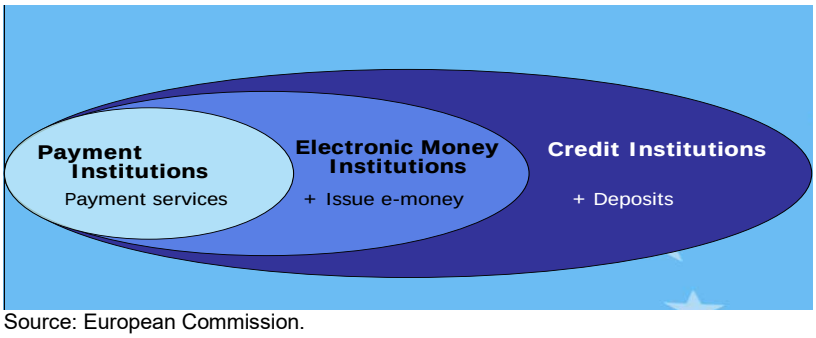
- World Bank (2009b), Working paper Nr. 174, *New technologies, New risks? Innovation and Countering the Financing of Terrorism*, Washington, 2009, http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/New_Technogies.pdf

APPENDIX D: THE EU LEGAL FRAMEWORK FOR NEW PAYMENT METHODS

The EU legal landscape for payments has dramatically changed since 2006: Regulation (EC) No. 1781/2006 transposed FATF SRVII[92]; the Payment Services Directive (2007/64/EC - PSD') provided a supervisory regime for the provision of payment services by non-banks and harmonised the rules governing the provision of payment services across the EU, thus enacting FATF SRVI; the new E-Money Directive 2009/110/EC (the new EMD) will replace the current EMD (2000/46/EC). Besides such reforms, the third Anti-Money Laundering Directive (AMLD) 2005/60/EC[93], adopting a risk-based approach, envisaged thresholds for applying Simplified Customer Due Diligence to electronic money; such thresholds have been revised by the new EMD.

The Payment Service Directive: new entrants in the payments market

The PSD provides the legal foundation for the creation of an EU-wide single market for payments; from a supervisory point of view, it bans carrying out payment services without an appropriate licence or registration. A new category of payment service provider (the "payment institutions") has been created besides those which are connected to taking deposits (banks) or issuing electronic money (electronic money institutions): with a license as payment institution non-banks (such as telecommunication companies) will have access to the payments market.



Source: European Commission.

The licensing regime allows payment institutions to provide payment services across the entire EU territory. Examination of the AML/CFT scheme by competent authorities is part of the decision-making process following the application to become payment institution. In addition, following a risk-based approach, the PSD provides for a waiver regime[94] whereby natural or legal persons unable to meet all the

---

92 The provisions related to FATF SRVII were not considered relevant by the project team for the purpose of this report.

93 OJ L 309, 25.11.2005, p. 15–36.

94 This waiver regime aims to *"bring all persons providing remittance service within the ambit of certain minimum legal and regulatory requirements*

prudential requirements may nevertheless carry out payment services at national level; AML/CTF measures apply also to waived payment institutions.

A fundamental change introduced by the PSD was the abolition of the exclusivity principle pursuant to which entities engaged in financial activities could not carry out business activities: this reform allows new operators, including telecom or IT providers, to enter the payment market and develop innovative payment services.

To date, the PSD has been implemented in the vast majority of the Member States of the EU/EEA.[95]

The legal framework for e-money issuance

The issuance of e-money has been regulated in the EU since the year 2000. Electronic money can be issued by electronic money institutions or by banks: both categories of financial institutions are subject to prudential supervision.

The definition of e-money provided by the current EMD has posed many problems of interpretation mainly due to its absence of technical neutrality and the lack of clarity with regard to services falling within grey areas. This is why the new EMD refines the definition to substantially cover all situations where the payment service provider issues a pre-paid stored value in exchange for funds, which can be used for payment purposes because it is accepted by third persons as a means of payment[96].

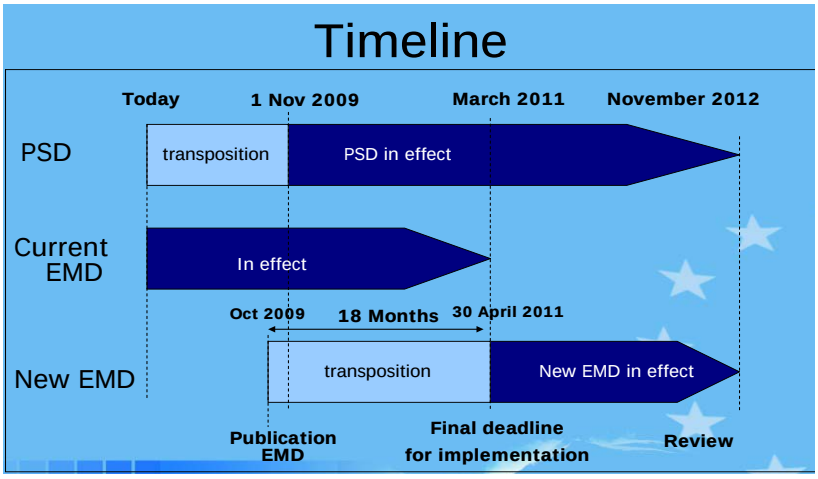
Another significant change introduced by the new directive is the further alleviation of prudential requirements for electronic money institutions and the extension of the activities they may engage in, to cover the full range of payment services and include the provision of credit facilities linked to the payment services provided. As a matter of fact, the too restrictive regime provided for by the first EMD was deemed to be the main cause of the lack of expansion of the e-money market in the EU outside the banking system[97]. The new regime for the issuance of e-money aims at facilitating market access to newcomers, namely telecommunication companies or large-scale retailers who want to engage in the market of e-money. Following the PSD, the exclusivity principle will no longer apply to EMIs. Such increased flexibility will facilitate cross-over of new payment methods (e.g., on-line payment accounts with m-payments) and with traditional payment methods used for the purpose of money remittance (e.g., money remitters with m-payments or prepaid cards).

---

95 The European Economic Area includes all EU Member States, Norway, Liechtenstein and Iceland.

96 In practice, electronic money can be either cards based or server based. In the former case the funds are stored on a chip of a physical smart card, in the latter mostly on a computer hard disk. The cards used for the storage of money can be prepaid-cards or so-called electronic purses. A special type of cards related e-money is the payment by way of using the SIM-cards of a mobile telephone. Server based e-money is also known as software or network money.

97 This legal framework restricted the e-money institutions' activities to the issuance of electronic money and the provision of closely related financial and non-financial services, such as the administering of e-money and the issuing and administering of other means of payment. This implied that activities such as mobile telecommunications services or retailing could not be performed by EMIs. Companies engaged in these businesses and willing to issue electronic money therefore had to split up their activities in two separate entities. Granting any form of credit was also an excluded activity. The framework included a strict prudential regime for electronic institutions, which was designed with the regime for banks as main point of reference.



Source: European Commission.

3. The Third Anti-Money-Laundering Directive (2005/60/EC)

The Third AML Directive (2005/60/EC) is the principal European Act setting Anti-Money Laundering measures; e-money institutions fall under its scope of application. This directive requires financial institutions and other players in key services and sectors to implement, inter alia, Customer Due Diligence (CDD) measures, *i.e.*, identify and verify the identity of their customers. Following a risk-based approach, simplified Customer Due Diligence is allowed in appropriate cases upon discretion of single Member States. Regarding the issuance of e-money products, the AMLD enables Member States to allow e-money issuers to apply simplified Customer Due Diligence where:

- if the device cannot be recharged, the maximum amount stored in the device is not more than EUR 150,
- if the device can be recharged, a limit of EUR 2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1,000 or more is redeemed in that same calendar year by the bearer.

Most EU Member states define simplified CDD in this sense as applying no CDD measures at all (which is considered in line with the AMLD by the EU Commission). A few member states do not allow their EMI to refrain from CDD completely even in such "low-risk" cases as they believe this would not be in line with Recommendation 5 (cf. crit. 5.9 of the FATF methodology; this is discussed in detail in section 5.2 of the report).

The payments industry expressed some concerns according to which the requirements aimed at countering money laundering and terrorist financing - namely, full application of identification and record keeping requirements - pose a particular challenge in the case of electronic money due to the low average amounts involved in electronic money transactions; this is why the new EMD increases the former threshold for applying Simplified Customer Due Diligence. For non-rechargeable devices the threshold is increased up to EUR 250 (from the current EUR 150). Member States will also have the option to increase such threshold up to EUR 500 for national transactions only. For rechargeable devices the current threshold (EUR 2500) is maintained.

According to the information available to date, the vast majority of Member States has made use of the option for not applying CDD to e-money below the thresholds; with the transposition of the new EMD this choice could be confirmed. In those Member States where the option is not used, as well as in those cases where e-money instruments exceeding the correspondent thresholds are issued, normal CDD measures apply[98].

In all cases where the issuance of e-money instruments is linked to a bank account (*i.e.*, where it is typically the e-money institution itself issuing the product), CDD measures have to be applied when the account is opened and funded. The compliance with these obligations is subject to supervision by national competent authorities.

Notwithstanding the provisions described above, CDD measures must be applied in any case of a suspicion of ML/TF irrespective of the product or transaction.

98 These obligations apply when: (i) establishing a business relationship; (ii) carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; (iii) there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold; (iv) there are doubts about the veracity or adequacy of previously obtained customer identification data.

APPENDIX E: GLOSSARY OF TERMS

Agent

A person or business which acts on behalf of a principal entity in providing payment services. If the principal is a regulated financial institution, it is responsible for the actions of its agent and also remains liable for its own AML obligations. For the purposes of this report, the terms "agent" and "outsource" shall be considered synonymous.

For the purposes of FATF Special Recommendation VI, the glossary to the FATF methodology and the Interpretative Note to Special Recommendation VI define the term "agent" as follows:

"For the purposes of Special Recommendation VI, an *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). "

Sub-Agent

A person or business acting on behalf of an agent to provide payment services.

"Bank based" business models

For the purposes of this report, bank based models are such models that require each customer to have an individual bank account in order to make use of the NPM service. The term does not stretch out to any business model that has any cooperation with a bank (*e.g.*, many NPM providers need to have a bank account in order to receive funds from customers, or to pay out funds to customers).

Brick-and-mortar exchanger

An exchanger that conducts all business on a face-to-face basis.

Card program manager

The entity responsible for establishing and running prepaid card business models in cooperation with a bank or electronic money institution. The program manager will usually market the prepaid cards and establish relationships with banks and distributors or customers. They typically do not themselves issue electronic money and are therefore not a regulated entity.

Some issuing institutions also manage their card programs themselves, *i.e.*, without cooperation with card program managers.

Cash vouchers

A prepaid product which can be purchased at several retailers and used for person - to -business (P2B) or person-to-person (P2P) transactions on the Internet.

Cash-back

Merchant points of sale (POS) used to withdraw cash by overpaying for purchased merchandise and receiving the overpaid amount in cash.

Customer Due Diligence (CDD)

According to FATF Recommendation 5, the customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information[4].

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Digital currency exchanger

(See "Digital currency provider")

Digital precious metals

(See "Digital currency provider")

Digital currency provider (DCP)

A type of internet payment service. Digital currency providers (DCP) keep and administer accounts for their customers, but typically do not directly issue "digital currency" to their customers/account holders. Instead, customers purchase their digital currency from exchangers, who will then transfer the purchased amount of digital currency into the customers DCP account. Funds kept in DCP accounts may be denominated in fictitious currencies or in real currencies. A sub-type of DCP denominates the funds in units of precious metal and supposedly invests funds received in that respective precious metal as a means of deposit protection. These DCP are also called "Digital precious metals providers".

Distributor

A company that sells products produced by other companies to consumers. Distributors may also offer a range of services to their customers, such as technical support.

Intermediary

A very general term for a person or company that acts as a mediator between parties, acting in cooperation with the NPM provider to provide services to customers. The term covers all types of third parties that are in the chain between the NPM provider and the customer, potentially including agents, distributors, retailers, exchangers and others.

(Electronic) Point of Sale – (E)POS

Merchant or shop that accepts a certain payment method as a means of payment. A POS usually requires certain technical devices or terminals in order to be able to make use of the payment method (*e.g.*, a card terminal to swipe the prepaid card, or special software to integrate the possibility for paying via Internet payment services in online shops).

Electronic Money ("E-Money")

While the term "electronic money" is used in the FATF methodology´s definition of *financial institutions*, the glossary does not provide a definition of the term *electronic money* itself.

Some jurisdictions use "electronic money" as a technical term in their legislation. For example, Art. 2 para. 2 of the revised EU Electronic Money Directive defines electronic money as follows:

"'electronic money' means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions (…)and which is accepted by a natural or legal person other than the electronic money issuer "[99].

Other jurisdictions´ definitions of electronic money may differ.

Electronic purse

An electronic purse, or e-purse (also referred to as a "stored value card" as the value is stored on the card), is value stored electronically in a device such as a card with an integrated circuit chip (called a smart card or chipcard).[100] For the purpose of this report, the term "electronic purses" is folded into the term "prepaid cards", as the method of storing the value (either centrally on a server or on the card itself) is no longer considered of relevance for the risk assessment of the card product.

Internet payment services

---

99 EU Directive 2009/110/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0110:EN:NOT)

100 FATF Report on New Payment Methods (www.fatf-gafi.org/dataoecd/30/47/37627240.pdf)

For the purposes of this report, the expression "Internet payment services" is used to address payment services operating exclusively on the Internet that are not or only indirectly associated with a bank account and may also be provided by non-bank institutions[101]. The expression does not include payment services that rely on a bank account and use of the Internet as a means of moving funds to or from a bank account ("online banking").

Merchant

A business that sells goods or services to consumers and maintains an arrangement with an acquirer to process transactions.

Mobile banking

Users can access traditional banking services through their mobile telephone. This is different from mobile payments in the sense that the regulated entity is a bank providing traditional banking services.

- **Mobile financial information services**

  Users may view personal account data and general financial information, but transactions cannot be executed using the service.

- **Mobile bank and securities account services**

  Users may transact in a similar fashion to internet banking.

Mobile payment services

Allows non-bank and non-securities account holders to make payments with mobile phones. However, payment service providers may be non-traditional financial institutions with widely varying controls and supervision measures.

Mobile money services

A subtype of mobile payment service, where subscribers are able to store actual value on their mobile phone (similar to e-purses). They may use phone credits or airtime as tender for payment. Such systems offer versatility but may fall out of regulation and prudential supervision altogether.

Money or value transfer service

Money or value transfer service refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.[102]

Money remittance

---

101 FATF Report on New Payment Methods (www.fatf-gafi.org/dataoecd/30/47/37627240.pdf)

102 See glossary to the FATF methodology.

A term commonly used to describe international money or value transfers by economic migrants to their home nation.

Negotiability

The level of acceptance across retailers for different payment methods. Some payment methods may have high negotiability because they are widely accepted but others may be very limited.

New payment methods (NPM)

For the purposes of this report, the term "New Payment Methods" encompasses prepaid cards, mobile payment services and internet payment services (IPS).

Open-loop prepaid card

A prepaid card which can be used at a wide range of terminals (vs. closed-loop prepaid cards with limited negotiability)

Outsourcing

An arrangement between a company and a service provider to provide services which would otherwise be carried out by the company itself. It is important to note that responsibility for ensuring compliance ultimately remains with the company. For the purposes of this report, the terms "agent" and "outsource" are used synonymously.

P2B

Person-to-business transaction.

P2P

Person to person transaction.

Phishing

Phishing is a criminal technique used to illegally obtain valuable information. For example, consumers will be sent fake e-mails from addresses that mimic those of banks. These emails will then dupe consumers into entering their account details.

Ponzi schemes

An investment scam that appears to pay high returns to investors. However these returns are paid from the investor's money or by incoming funds from new investors. The fraudster will either disappear with the money invested or the scheme will collapse.

Prepaid card

A payment card pre-loaded with funds. The card can then be used at businesses where the card type is accepted, including on the internet and abroad.

Prepaid card issuer

A bank or other financial institution that issues prepaid cards.

The term issuer is also used in connection with other types of NPM "value", *e.g.*, issuer of electronic money, or of digital currencies. The issuer is the entity that the customer has a contract with, and from whom the customer can demand redemption or withdrawal of funds.

Prepaid internet payment products

Products offered by firms which allow customers to send or receive funds through a virtual prepaid account. In some jurisdictions these firms may not fall within the definition of a "credit institution".

Processor

A company that processes transactions on behalf of an acquirer or merchant.

Red Flags

Indicators of suspicious activity where a product's actual use deviates from its expected usage. Red flags should therefore be tailored to the product's characteristics.

Smart cards

Cards featuring an electronic chip. This is usually used to process additional customer information.

Straw man

A real or fictitious individual used by others as a front for illegal activities such as money laundering and fraud.

Utility

A measure of the variety of payment options offered by a particular type of payment method. For example, some payment methods may offer person to business (p2b) transactions only while others may also allow for person to person (p2p) payments.

Virtual worlds

A simulated world which exists within a virtual environment. This commonly refers to computer games which are based on the internet such as Second Life. Often the economy is based upon a digital currency which can be bought and/or converted into real money.

FATF/OECD
December 2010

www.fatf-gafi.org

Appendix EE:

FATF, *FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers* (Paris: FATF, 2010)

FATF • GAFI
Financial Action Task Force Groupe d'action financière

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

FATF Report

Money Laundering through **Money Remittance** and **Currency Exchange Providers**

June 2010

COUNCIL OF EUROPE – COUNTERING MONEY LAUNDERING AND FINANCING OF TERRORISM (MONEYVAL)

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL (formerly PC-R-EV) was established in 1997. At their meeting of 13 October 2010, the Committee of Ministers adopted the Resolution CM/Res(2010)12 on the Statute of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). This new statute elevates MONEYVAL as from 1 January 2011 to an independent monitoring mechanism within the Council of Europe answerable directly to the Committee of Ministers. The aim of MONEYVAL is to ensure that its member states have in place effective systems to counter money laundering and terrorist financing and comply with the relevant international standards in these fields.

For more information about MONEYVAL, please visit the website:

WWW.COE.INT/T/DGHL/MONITORING/MONEYVAL

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

TABLE OF CONTENTS

ABBREVIATIONS

AML	Anti-money laundering
CFT	Counter financing of terrorism
CE	Currency exchange
CDD	Customer due diligence
CTR	Cash transaction report
EU	European Union
FIU	Financial intelligence unit
ID	Identification
KYC	Know your customer
ML	Money laundering
MR	Money remittance
NA	Not available
STR	Suspicious transaction report
TF	Terrorist financing

EXECUTIVE SUMMARY

1. This joint FATF/MONEYVAL report contains information on money laundering and terrorist financing methodologies associated with the money remittance and currency exchange sector. The findings contained in the report derive from information provided by 61 FATF, MONEYVAL and Egmont Group member States and other open source material. Though the focus of the report is to a certain degree on the MONEYVAL region and the wider European area, the experience of countries from other regions of the world was actively sought and integrated into the report.

2. Apart from providing a useful general overview of the sector of money transfer remittances and currency exchange providers, the regulatory framework, the supervision and sanctioning regimes, the report sets out identified money laundering and terrorist financing methods and techniques involving money remittance and currency exchange providers.

3. Several case studies described in this report illustrate that money remittance and currency exchange businesses have been both witting and unwitting participants in laundering activities, in all three stages of the process (placement, layering and integration), and in certain instances, for terrorist financing purposes. The identified risks of ML/TF through the sector detailed in the report are related to clients, owners or agents. The cases highlight also the links between money laundering in the money remittance sector and other criminal activities (*e.g.*, fraud, trafficking in human beings, smuggling, drug trafficking, economic crime).

4. A number of vulnerabilities to money laundering across the sector that make up the money remittance and currency exchange sector were identified. The analysis of the case studies and other materials enabled the project team to compile numerous examples of indicators of potential money laundering activities related to transactions, customer profile and behaviour as well as specific indicators for bureaux de change and money remittance providers that may help the industry to identify and describe suspicious behaviours and protect themselves against money launderers and other criminals.

5. Clearly, laundering through money remittance and currency exchange providers poses a number of regulatory and enforcement challenges. At the same time, it was observed that there is low detection of money laundering in comparison to the size of the industry as a whole. The money laundering and terrorist financing threat in the sector not only results from direct penetration of criminals into operations of money remittance or currency exchange providers. The absence or lax implementation of AML/CFT standards and adequate related policies provide opportunities which are being exploited by money launderers and other criminals.

6. Finally, the report maps also a number of issues and areas which were identified in this context as appearing to require additional efforts, both from regulatory and supervisory authorities as well as from the industry, in order to reduce the misuse of the sector and ensure that ML/TF risks are adequately addressed. These issues will likely require further investigation together and updating research, not only to continue the development of a better understanding of specific money laundering and terrorist financing risks in the money remittance and currency exchange sector but also to ensure that regulatory responses are proportionate and effective.

INTRODUCTION

7. Specialised financial businesses have for many years played an increasing role in providing certain types of services, including money remittance (MR), foreign currency exchange (CE) and the issue/management of means of payment to a variety of actors. The globalisation of financial markets and the development of information technology have made the movement of funds across the world easier and have thus further spurred the growth of these specialised financial services. The service providers in this field (the "MR/CE sector") are quite diverse and range from simple businesses to complex chain operators.

8. In order for criminals to move, hide and eventually use the funds generated by their illegal activities, they must seek ways to launder those funds without drawing the attention of law enforcement or other authorities. Given the range of products and services offered, the variety of distribution channels, the high transfer speed and the fact that they are often cash-intensive businesses, the MR/CE sector may provide significant opportunities for criminals desirous of laundering funds unless appropriate safeguards are in place. Particular risks involved with the sector are related not only to the misuse of MR/CE businesses for laundering money but also to the owning of such businesses by criminal groups and corrupt employees co-operating with criminals.

9. Typologies reports published by the Financial Action Task Force (FATF) over the years have highlighted money laundering risks posed by *bureaux de change* (FATF typologies report, 1996-1999 and 2001) and examined money laundering and terrorist financing vulnerabilities of alternative remittance systems (FATF typologies report 2004-2005). At the time that these studies were conducted, little information was available on the MR/CE sector in MONEYVAL member States or on the ML/TF risks facing the sector. Thus, MONEYVAL and the FATF decided in 2008 to undertake a joint project on methods of money laundering through MR/CE businesses.

Scope of research

10. In most jurisdictions, MR/CE businesses are not defined as banks. While in some countries, such as the United States[1] and the United Kingdom, national legislation has defined this group of financial service providers, the MR/CE sector in most countries is not explicitly defined. In the FATF 40 Recommendations as well as in the third EU Money Laundering directive[2], those financial businesses providing MR/CE services are considered to be a subset of financial institutions[3]. Using the term *non-bank financial institutions* to refer to MR/CE services can also be misleading in that the term as defined by the FATF also included broker dealers in securities and casinos. The term is even less helpful now, as the FATF currently makes the distinction between financial institutions on the one

1 In the United States, the term *money services business* has been defined since 1999 when the Secretary of the Treasury issued a ruling revising the regulatory definitions of certain non-bank financial institutions for purposes of the Bank Secrecy Act. These revised definitions were grouped into a separate category of financial institution called *money services businesses* or *MSBs*.

2 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

3 For further details, please see the glossary of the FATF 40 Recommendations and article 3 (2) (a) of the Directive 2005/60/EC.

hand and *designated non-financial businesses and professions (DNFBPs)* on the other. The former category includes all of the activities that are provided by MR/CE services.

11. Typically, MR/CE services include three types of activity:

- Currency dealers/exchangers;
- Money remitters; and
- Issuers, sellers and redeemers of stored value and monetary instruments, such as money orders and traveller's checks.

12. The category "money remitters" is diverse, ranging from large organisations, like Western Union, to what are often termed "informal value transfer systems". This latter category includes systems that often operate outside the "regulated" financial system and are deeply rooted in historical, cultural and economic backgrounds. Well known examples include "hawala", "flying money" systems indigenous to China, India's *hundi* system, and the *padala* system used in the Philippines[4].

13. Given the research already conducted on the subject by the FATF other international organisations, this study does not attempt to duplicate already existing information. For this reason, it was decided to exclude from its scope the analysis the misuse of new payment methods[5], of traveller's checks and money orders. The methods and trends of money laundering and terrorist financing through alternative remittance systems are also not analysed in-depth[6] because the potential misuse of such systems for terrorist financing was already covered in the 2008 terrorist financing typologies report produced by the FATF.[7]

14. This research report therefore focuses on non-bank financial institutions that provide at least one of the following services: (1) money remittance, (2) currency exchange/dealing and (3) issuing, cashing or redeeming of cheques/money orders/stored value cards.

15. The research conducted on this subject also provided an opportunity to take stock of potential money laundering threats arising from the changeover to the Euro in certain countries. This is an important issue for many MONEYVAL members in that a number of EU members from MONEYVAL have yet to adopt the Euro as official currency and are looking to develop best practices based on measures already adopted by euro zone countries to address those threats. This research thus attempts to lay out relevant findings, in the light of developments in this specific sector as well as in the EU regulatory area, resulting from the adoption and implementation of the EU legislation that directly impacts upon the MR/CE sector.

16. After examining how MR/CE businesses may be misused for money laundering purposes and identifying vulnerabilities that may be exploited by criminals, the report will look at appropriate measures which could be taken to address the identified vulnerabilities. It should be stressed that

---

4 HM Treasury (2006). For more details about the alternative remittance system, the profile of the users of the system and its role in ML, please refer to Chene (2008).

5 See FATF (2006). The FATF has since updated this research , and a report on the subject was published in October 2010 that considers the vulnerabilities of new payment methods to ML/TF (the report focuses on prepaid debit cards, mobile payment services, on-line payment systems). Additional literature on ML/TF schemes through new payment technologies is also available (see US Department of Justice (2006), Sienkiewicz (2007), Choo (2008)).

6 See FATF (2005), MENAFATF (2005), Carroll (2007). See also for further information the IMF (2005a, 2005b)

7 See FATF (2008a)

available information has allowed the money laundering threat facing MR/CE businesses to be documented. Regarding the threat of terrorist financing facing such businesses however, there was far less sector-specific information to work with. This report then focuses primarily on the range of ML techniques to which MR/CE businesses may be vulnerable and provides a series of illustrative typologies. A non exhaustive list of indicators of potentially suspicious activity has been included in the report, which is intended to assist the private sector, law enforcement and regulators detecting ML within the sector. Finally, the report also briefly lays out a series of issues and areas for further consideration.

Methodology and sources

17. The research and analysis of the material used to develop this report was conducted by a small joint project team of experts from MONEYVAL and FATF jurisdictions. The experts contributed to the analysis and drafting of the report through a series of working meetings and exchanges of written material that took place over a period of about two years. The project was led by Estonia, with Mr Raul Vahtra and Ms. Kerly Krillo of the Estonian financial intelligence unit heading up the work, including the main task of drafting this report. The following countries and organisations contributed to the project with either substantive material or expertise: Australia, Bulgaria, Cyprus, Germany, Italy, Mexico, the Netherlands, Poland, Romania, Sweden, Spain, the United States, the Egmont Group and the European Bank for Reconstruction and Development.

18. One of the main sources of information for the project was a detailed questionnaire which solicited a range of range of material, including case studies, national-level typologies research and other relevant expertise. Well over 50 questionnaire responses were received and analysed by the project team from FATF, MONEYVAL and Egmont Group members.[8] The project team also used the discussions and findings of the Joint FATF/MONEYVAL meeting of experts on typologies (held in Monaco, 24-26 November 2008, which gathered participants from 40 countries, 2 international organisations and 3 FATF-style regional bodies), as well as other FATF typologies reports, case studies and open source information.

19. While the focus of this report is to a certain degree on the MONEYVAL region and the wider European area, the experience of countries from other regions of the world was actively sought and integrated into the report.

Acknowledgements

20. This project was conducted by a team of experts from both FATF and MONEYVAL members, who have contributed to the project throughout the working meetings and by providing written contributions and comments which have been reflected in this report. The project team would like to thank all FATF, MONEYVAL and Egmont Group members which responded to the survey and provided other valuable input to this research.

8 See Annex 1 for a list of contributing jurisdictions.

CHAPTER I –OVERVIEW OF MONEY REMITTANCE & CURRENCY EXCHANGE SECTORS

1.1 General

21. The globalisation of the financial sector and the vast development of information technologies has contributed to a considerable increase in the volume of the activity carried out by the MR/CE sectors during the past two decades. In the US for example, the estimated value of financial services provided by the money service business industry, which includes MR/CE activity,[9] was approximately USD 200 billion annually in 1997; however, by 2005 the industry had grown to approximately USD 284 to USD 305 billion (FinCEN 2005). Unfortunately there are no similar figures available for the equivalent sector in other parts of the world; therefore it is impossible to estimate the size of the MR/CE industry globally.

1.2 The money remittance sector in MONEYVAL/FATF member States

22. The World Bank estimate of money remittance (MR) worldwide is 443.5 billion USD for 2008 and 420.1 (estimated) for 2009. Not all countries are able to determine the total volume of incoming and outgoing MR activity. It is therefore difficult to provide an indication of the proportion of global MR that MONEYVAL/FATF countries represent. Nevertheless certain jurisdictions are able to provide reliable estimates of the volume of MR activity, and these are included in Table 1 below. From this information, countries can be divided into two groups:

- *Senders, i.e,.* countries where the amount of outgoing money transfers are remarkably higher than incoming.
- *Receivers, i.e.,* countries where the amount of incoming money transfers are remarkably higher than outgoing.

23. At European level, the first group mostly includes primarily the "old" EU member states (Germany, Greece, Italy, and Spain), along with Croatia, Cyprus, Malta, and Monaco; while in the second group southeastern European countries and former Soviet republics (Armenia, Bulgaria, Georgia, "the former Yugoslav Republic of Macedonia" and Ukraine) predominate.

Table 1. Volume of money remittances sent and received in selected MONEYVAL/FATF member States (2006-2008, million EUR)

Country	Sent			Received		
	2006	2007	2008	2006	2007	2008
Armenia	615.6	787.7	722.0	971.0	1 353.7	1 433.5
Bulgaria	NA	11.1	8.6	NA	94.7	73.5
Cyprus	190.5	212.1	227.3	17.0	37.1	29.8

9 See paragraph 10 above for an explanation of the difference between MSBs and MR/CE service providers as the terms are used in this report.

Country	Sent			Received		
	2006	2007	2008	2006	2007	2008
Germany	1 830.1	1 927.3	1715.5	548.0	1 026.7	1 200.1
Spain	4 891.0	6 267.0	NA	202.0	222.0	NA
Georgia	92.9	77.5	77.5	387.1	606.0	701.1
Greece	570.4	775.4	NA	178.4	203.9	NA
Croatia	44.5	42.0	43.9	21.9	22.3	22.0
Italy	4 528.9	6 044.1	5 980.0	248.2	252.2	191.6
Monaco	10 732.0	11 471.0	11 833.0	1 469.0	1 382.0	1 389.0
"the former Yugoslav Republic of Macedonia"	5.6	7.1	10.3	68.6	78.8	95.3
Malta	68.3	80.7	78.7	31.0	64.9	35.2
Ukraine	97.2	133.6	267.2	1 070.4	1 444.7	1 773.5

NA: not available.

24. Among those MONEYVAL/FATF countries that provided information for this study, MR systems are very heterogeneous. Even within the same geographical regions, countries often have very different MR systems. Therefore, it is difficult to highlight any 'typical cases'.

25. The number of independent MR service providers[10] varies greatly from one MONEYVAL/FATF country to another (see table 2 below, data reflecting 2008 figures). At one end of the scale are the United States with more than 25 000 MRs (this number does not include agents)[11], the UK (approximately 2 800 MRs) and Mexico (approximately 1 100 MRs). At the other end of the scale are Austria, Japan, Monaco, Moldova, San Marino, Serbia and Turkey. In these countries, there are no companies that provide MR services alone. In these jurisdictions, MR services are provided by either banks and/or post offices, which also offer other services in addition to MR. Most countries, however, are in between the two extremes.

Table 2. Number of money remittance service providers in FATF and MONEYVAL member States

Country	N° of MR providers	Country	N° of MR providers	Country	N° of MR providers
USA	25 096	Chile	15	Poland	2
UK	2 818	Greece	14	Croatia	1
Hong-Kong, China[1]	2 008	Armenia	11	Liechtenstein	0
Mexico	1 085	Slovakia	11	Austria	0
Denmark	334	Bulgaria	7	Japan	0
Argentine	122	Cyprus	7	Monaco	0
Sweden	96	Malta	7	Moldova	0
Finland	70	Latvia	6	San Marino	0
Spain	46	France	4	Serbia	0

10 Note: throughout this study 'independent MR service providers' refers to the companies to whom the money transferring is a core business, it does not include banks, post offices, and other agents of the MRs to whom MR is side-business.

11 As at 13 February 2009.

Country	N° of MR providers
Germany	38
Estonia	34
Italy	30
Netherlands	28

Country	N° of MR providers
Lithuania	4
Romania	4
Macau, China	2
"the former Yugoslav Republic of Macedonia"	2

Country	N° of MR providers
Turkey	0
Albania	NA
Georgia	NA
Ukraine	NA

Table Notes:

Remarks: only independent MR services providers (excluding banks, post offices, agents).

1. Please note that in Hong-Kong, China no distinction is made between money remittance and currency exchange providers. Remittance agents and money changers (RAMCs) are entitled to provide both services. Although not all RAMCs provide both services, most of them do so.

26. In some countries, MR providers have well-developed agent systems, with post offices, currency exchange offices, banks, travel agencies, hotels and other companies providing remittance services as agents of the MR companies. Examples in which MR services are offered by other than specific MR businesses include:

Albania:	currency exchanges (as agents of Western Union and MoneyGram);
Bulgaria:	banks, currency exchanges and financial houses;
Chile, Liechtenstein, Monaco:	post offices (in the first two as agents of Western Union and in the latter as agents of Western Union and MoneyGram);
Croatia:	post offices and one bank[12] (as agents of Western Union);
Estonia:	post offices, banks, currency exchanges and travel agencies;
Finland:	currency exchanges, travel agencies and miscellaneous shops;
France:	post offices (through an agreement with a branch of Western Union licensed as a financial company);
Germany:	post offices, currency exchanges and banks;
Greece:	post offices and currency exchanges (as agents of Western Union);
Italy:	currency exchanges, travel agents, hotels, phone centres, internet centres, news agents and stationers;
Malta:	post offices, travel agencies and hotels;
Moldova:	banks (as agents of Western Union, MoneyGram);
Mexico:	post offices, currency exchanges, banks and travel agencies;
Netherlands:	travel agencies;
Poland:	banks, one credit unions' financial services provider, travel agencies and a few other providers of selected banking

12 Société Générale Splitska Banka.

	services;
Romania:	both post offices and banks (as agents of Western Union, MoneyGram);
Slovakia:	post offices, currency exchanges and banks;
Spain:	post offices;
Sweden:	post offices, currency exchanges, banks, money transaction offices, travel agencies and hotels;
"The former Yugoslav Republic of Macedonia":	currency exchanges, banks, travel agencies and hotels;
UK:	post offices, travel agents and other outlets like restaurants and general stores; and
US:	currency exchanges, banks, travel agencies and hotels.

27. Post offices usually provide money transfers as an independent side-business of their main activity or act as agents for other MR companies. Typically they are registered / licensed as money remitters in several countries. For example, in San Marino 5 out of 10 post offices operating domestically are authorised to perform money transfer services.

28. Banks offer MR services in Argentina, Chile, Cyprus, France[13], Greece, Malta, the Netherlands, Poland and Serbia, and Spain.

29. Both post offices and banks are authorised to perform MR services as side-businesses in Albania; Armenia; Denmark; Georgia; Hong-Kong, China; Italy; Latvia; Macau, China; Poland; Turkey and Ukraine.

30. Furthermore, currency exchanges (in Argentina, Chile, Malta, the Netherlands, Romania), travel agencies (in Cyprus, Romania) and hotels (Romania) also offer MR services, although money transfer is not their core business activity. This distinguishes them from companies that are defined as 'independent MR providers' in this report.

31. The distinction between national/international MR providers also differs greatly. In some countries, like Croatia, Liechtenstein and Lithuania, Western Union is the only MR service provider. In others, like "the former Yugoslav Republic of Macedonia" and Poland, where Western Union and MoneyGram operate as MR providers, there are no similar domestic MR operators. In other countries on the other hand, such as Japan and San Marino, no international companies operate. Latvia combines both systems. Latvian Post is the only national provider of money remittance services. The foreign providers are not registered and are supervised by banks that provide money transfer service.

32. When an MR service establishes a permanent business relationship, the identification of the client is mandatory for money remitters in most jurisdictions. For occasional transactions, the thresholds triggering certain measures vary from the obligatory identification of all customers in Argentina, Austria, Cyprus, Germany, Italy, Netherlands, and Spain, to EUR 15 000 in Finland, San Marino, and Serbia. In respect to the identification requirements for clients initiating money

[13] The particular feature of the France is the presence of foreign banks (mostly African and Asian) that are specialised on offering money remittance services to their customers. Quite naturally, the customers of these banks are foreigners living in France.

remittance, countries can be placed into the following three broad categories (for more details, please refer to table 6 in annex 3):

1. Identification of the client is mandatory for each MR transaction;
2. Identification applies starting from a EUR 1 000 threshold (as required in the EC Regulation No 1781/2006) and
3. Identification applies starting from some other threshold.

33. If there is a suspicion of ML or TF, as a general rule, the threshold does not apply and identifying the client and informing the FIU is mandatory.

Table 3. The client identification threshold in MONEYVAL/FATF member States

No threshold, mandatory identification	Argentina; European Union State members[1]; Liechtenstein; Macau, China[2]; Monaco
EUR 1-999	Armenia, Georgia, Japan, Turkey, Ukraine
EUR 1 000	Croatia, Mexico[3], Moldova[4], San Marino
EUR 2 000-2 999	"The former Yugoslav Republic of Macedonia" and US
EUR 3 000-11 999	Chile
EUR 12 000	Albania
EUR 15 000	Serbia

Table Notes:

1. In EU Member States, financial institutions must identify and verify the complete information on the payer/originator before executing any wire transfer regardless of any threshold. Only where the wire transfer is (1) executed from an account of a customer who has been identified and whose identity has been verified in the course of the account opening and whose identification records have been stored according to requirements of the 3rd EU AML Directive or (2) of an existing customer whose identity has to be verified at appropriate times according to the 3rd EU AML Directive financial institutions stating that there is no requirement to repeatedly verify the originator's identity (Art. 5(3) of Regulation (EC) No. 1781/2006). In case a wire transfer is not made from an account, the financial institution must verify the identity of the originator only when the amount is above EUR 1 000 unless the transaction is carried out in several operations that appear to be linked and together exceed EUR 1 000.

2 In Macau, China, under the regulations for cash remittance activities, cash remittance companies are required to record the identification and address of remitters and beneficiaries regardless of the amount of the remittances in Macau. For wire remittances done through banks and post office, the threshold is MOP 8 000 (appr. USD 1 000).

3 In Mexico, there are three different thresholds in order to require information for individual cash operations or with travellers cheques, as follows:

- between USD 1000 – 3000, information is requested

- between USD 3000 – 5000, information is requested along with a copy of the official identification

- for USD 5000 or more, information is requested and a whole file is integrated to the system.

4 In Moldova, the threshold for occasional transactions is 50,000 lei (appr. EUR 3 500) and for electronic and wire transfers 15 000 lei (appr. EUR 1 000). At the same time, according to the foreign exchange legislation, payment/ transfers shall be made by licensed banks upon the submission by the individual of the identity document regardless of the amount of the payment/ transfer.

1.3 The currency exchange sector in MONEYVAL/FATF member States

34. Similar to money remittance, the currency exchange[14] (hereinafter CE) services vary somewhat in MONEYVAL/FATF member. However, due to the standardised nature of the business, the differences are not as noteworthy as for MR.

[14] The terms '*bureaux de change*' and 'currency exchange providers' refer to the same type of activity. For the sake of consistency within this report, the term 'currency exchange provider' is used.

35. According to the data received, the number of currency exchange service providers shows considerable variation from one MONEYVAL/FATF member to another (see table 4 below). In a number of countries (*e.g.*, Croatia; Georgia; Hong Kong, China; Mexico; Poland; Serbia; Spain; United Kingdom, Ukraine and United States) the number exceeds 1 000. At the other end of the scale, there are Finland and Monaco with less than 5 currency exchange providers.

Table 4. Number of bureaux de changes[1] in selected MONEYVAL/FATF member States

Country	No. of bureaux de change	Country	No. of bureaux de change	Country	No. of bureaux de change
Albania	NA	Bulgaria	625	Sweden	56
Argentina	NA	France	515	Denmark	44
Poland	4 193	Italy	489	Germany	24
US [2]	3 294	Romania	470	Macau, China	17
Mexico [3]	2 757	Slovak	455	Greece	12
Spain	2 256	"the former Yugoslav Republic of Macedonia"	271	Netherlands	12
Hong Kong, China[4]	2 008			Malta [5]	7
Serbia	1 781	Moldova	319	Finland	4
UK	1 404	Armenia	246	Monaco	2
Croatia	1 242	Japan	196	Austria [7]	0
Ukraine [6]	1 104	Estonia	163	Cyprus[7]	0
Georgia	1 050	Chile	128	Liechtenstein[7]	0
Turkey	755	Latvia	75	San Marino[7]	0
		Lithuania	62		

Table Notes:

1. Only independent service providers, i.e. excluding banks and other businesses for which CE is not a core business.
2. As of 13 February 2009, the date of the US response to the questionnaire for this project.
3. currency exchange services providers.
4. Please note that in Hong-Kong, China no distinction is made between money remittance and currency exchange providers. Remittance agents and money changers (RAMCs) are entitled to provide both services. Although not all RAMCs provide both services, most of them do so.
5. In Malta CE (as well as MR) providers form part of a wider category of entities defined as "financial institutions". Therefore, the number of MR and CE providers in the tables refers to the same institutions
6. In Ukraine, the following institutions are authorised to open currency exchanges for conducting currency exchange transactions: banks operating under a banking license and having prior written permission, and financial institutions/national operators of postal services that obtain general license from the National Bank of Ukraine for conducting non-trade transactions with currency values.
7. Only banks provide currency exchange services.

36. Naturally in most (if not in all) countries, banks are authorised to perform CE services. In a few countries – Austria, Cyprus, Liechtenstein and San Marino – CE is provided exclusively by banks, and no independent currency exchanges exist. Although it is not obvious from the first sight, in Lithuania the system is quite similar. All CE businesses (approximately 60) in Lithuania are operated by banks. Furthermore, divisions and branches of banks as well as credit unions (22 at present) are also authorised to perform currency exchange.

37. In Mexico, the currency exchange service providers can be divided into two groups:

- 'Foreign exchange houses' (*casas de cambio*) are legal entities that require a license to engage in currency exchange services with the public; and

- 'Foreign exchange centres' (*centros cambiarios*) are either natural or legal persons that do not require a license in order to engage in currency transactions, but whose operations are limited to the equivalent of USD 10 000.00 per customer per day. They must be registered with the Tax Administration Service.

38. In Slovakia there are three types of foreign currency exchange providers:

- *Currency exchanges* – require a 'simple FX license' that authorises natural or legal persons to purchase or sell local currency against foreign currency (money transfers are not included);
- *FX business providers* I – legal persons with a minimum capital requirement of EUR 333 333. Their license allows them to both purchase and sell local currency against foreign currency on their own or their client´s behalf but only in cashless form. They are permitted to make only domestic money transfers; and
- *FX business providers II* – legal persons with minimum capital requirement of EUR 33 333. Their license authorises them to carry out or intermediate cross-border money transfers both in local or foreign currency in cash. They are permitted to make foreign money transfers through banks only.

39. Regarding customer identification, the same thresholds apply as for MR in most countries. The exceptions are:

Table 5. Threshold Exceptions to Applicable Customer Identification Requirements

COUNTRY	THRESHOLD (as of 2008)
Croatia	HRK 105 000, *i.e.* appr. EUR 15 000
Estonia	EEK 100 000, ie. appr. EUR 6 400
France	EUR 8 000
Japan	YEN 2 000 000, *i.e.* EUR 15 566
Germany	EUR 2 500 threshold applies if the transaction is carried out through an account other than the customer's account;
Georgia	GEL 3 000, *i.e.* appr. EUR 1 400
Greece (and Italy, Malta, Poland, Sweden, United Kingdom)	EUR 15 000
Latvia	LVL 5 000, *i.e.* appr. EUR 7 117
Lithuania	EUR 6 000
Moldova	MLD LEI 50,000 (approx. EUR 3 500)
Macau, China	MOP 20 000 , *i.e.* appr. EUR 1 740
Mexico	Thresholds vary for transactions involving cash or travellers' cheques
Slovakia	EUR 1 000
United States	USD 1 000, *i.e.* appr. EUR 820

Table Notes:

1. In Mexico there are three different thresholds in order to require information for individual cash operations or with travellers cheques, as follows:
   - between USD 500 - 3000, information is requested;
   - between USD 3000 – 5000, information is requested along with a copy of the official identification (identical threshold applicable also to MR);
   - for USD 5000 or more, information is requested and a whole file is integrated to the system (identical threshold applicable also to MR).

1.4 Licensing, supervision and sanctioning system of money remittance and currency exhange providers[15] in MONEYVAL / FATF member States

Licensing/registration

40. In most MONEYVAL and FATF member states the MR provider must be registered or licensed (see table 7 in annex 1)). In countries that require licenses in order to provide MR service, either the central bank, as in Albania, Bulgaria, Cyprus, Slovakia, Spain, or the financial supervisory authority, as in France, Germany or Malta, is the competent authority to grant licenses.

41. In the European Union, new rules on payment services in the EU internal market provide for an evolution regarding the licensing of providers of money remittance services. Directive 2007/64/EC on payment services in the internal market (which was due to be integrated into the EU legal framework in November 2009) establishes the obligation to licence payment service providers (except for certain financial institutions that already have a licence, such as banks). The Directive creates two levels of licences. Firstly, the EU-wide licence for the newly created category of 'payment institution'. This category includes payment service providers which are not allowed to accept deposits from the public (which banks do) and which do not issue electronic money (which is done by banks or so-called 'e-money' institutions). Obtaining an authorisation as a 'payment institution' is subject to a set of strict conditions, including prudential requirements. The authorisation granted by a EU Member State to a 'payment institution' is valid for the entire EU territory, which can, for instance, provide its services in other EU countries including through local agents. There is a specific procedure to approve agents, where AML checks can be done by the relevant competent authorities. Therefore, it is possible that a payment institution licensed in one EU country operates in another EU country without the need to obtain a second licence from that second EU country. Secondly, the EU directive on payment services allows EU Member States to establish a lower level (but this level is not compulsory): natural or legal persons unable to meet all the strict conditions for becoming 'payment institutions' may nevertheless carry out payment services in the Member State where they have their head office or legal residence after having been registered in that EU Member State. Some of the Directive requirements for 'payment institutions' are nevertheless applicable to this lower level. The goal of this lower level regime is to "bring all persons providing remittance services within the ambit of certain minimum legal and regulatory requirements" (cf. paragraph 15 of the preamble of the Directive). As a result, the provision of money remittance services in the EU is forbidden for other categories of undertakings or individuals.

42. In the countries that require registration of MR service providers, one of three entities generally oversees the registration process:

- The financial intelligence unit (FIU) (for example, in Chile; Hong Kong, China, and the United States[16]);
- The financial supervisory authority (for example, in Georgia); or
- Another government authority (for example, the Ministry of Economic Affairs and Communications in Estonia; State Provincial Office of Southern Finland in Finland; the Monetary Authority in Macau, China; the Tax Administration Service in Mexico; HM Revenue and Customs in the UK).

---

15 In this section we focus solely in independent money remittance /currency exchange providers, *i.e.* those that do not operate as a part of banks, post offices and/or agents of the MR providers.

16 In addition to federal registration, MSBs must be licensed or registered in 48 of the 50 US States.

43. Latvia is an exception, as money remitters need neither register nor obtain a license to operate; however, legislation addressing this matter was in the process of being drafted at the time of the survey.

44. As regards the provision of CE services, a license is required in most countries.[17] As a general rule, the authority responsible for issuing licenses is the central bank.

45. In a few countries, the CE businesses do not need to be licensed, but have to be registered in order to be permitted to provide currency exchange service. Usually the institution responsible for keeping the registry is a governmental authority (for example, National Revenue Agency in Bulgaria, the Commerce and Companies Agency in Denmark, the Ministry of Economic Affairs and Communications in Estonia, HM Revenue and Customs in the UK, etc.).

46. In Chile in 2009 there was no mandatory registering/licensing system for money remitters and currency exchange at the state level, and the FIU had in the interim taken on the task of keeping the record instead. The current system was considered to be ineffective and amendments to the legal framework were being discussed in order to introduce the statutory registering system.

47. In Japan there is no registering/licensing system for currency exchange at all. In Finland, there is a legal requirement to establish a registering/licensing system for currency exchanges, but its concrete implementation had not yet taken place at the time the survey was carried out.

48. In most countries (with the exception of Chile; Georgia; Hong Kong, China; and Japan where no specific 'fit and proper' controls apply to MR/CE businesses) the 'fit and proper' control is applied in some form at least during the licensing/registration process. As a minimum standard, this background check usually includes evaluating the qualification, creditworthiness (*i.e.* absence of tax duties) and criminal record (for serious offences) of the owners and managers of the company. In Denmark the 'fit and proper' controls cover beneficial owners, too.

49. However, there are countries that apply more in-depth control mechanisms. For example, in Armenia the central bank also checks the qualification through examination of the employees of the currency exchange business. The qualification document is valid for three years.

50. After granting the license/registration to the company, in most countries no permanent on-going monitoring is applied and further action is taken only if there is evidence of unlawful activities or a change in the company's management board. In some countries this system is somewhat standardised; for example, in Germany prosecution authorities and courts have to notify *Bundesanstalt für Finanzdienstleistungsaufsicht* (BaFin – the Federal Financial Services Supervisor) of criminal proceedings against managers. The same system is applied in Estonia, where the registration of the company is cancelled if the member of the administration of the company is convicted of criminal offences.

51. However, there are a few countries that monitor the eligibility criteria more or less on an periodic basis. For example, the information about meeting the eligibility criteria of the managers and owners is updated at least once a year in Albania, Croatia, Italy, Lithuania, Mexico, and Sweden.

AML/CFT supervision

52. In most countries, the central bank, the FIU and/or financial supervisory authority carries out AML/CFT supervision over the money remitters and currency exchanges.[18]

---

17 See Annex 3, Table 7.

53. In the countries that apply the registering system of money remitters/currency exchanges, usually the authority responsible for keeping the register also supervises the entities.

54. Typical sanctions applied to an unregistered /unlicensed money remittance providers are fines and/or imprisonment.[19] Maximum levels of fines imposed vary from EUR 5 000 in Bulgaria to unlimited amounts in the UK.

55. Most responding countries indicated that existing sanctioning regime was considered to be effective in deterring the illegal MR providers. In the United States, for example, there are federal and state sanctions for operating a money remitter or currency exchange that fails to become licensed or registered. For example, knowingly operating a money remittance business without a proper state license/registration and federal registration is subject to a fine of up to USD 5 000 a day and imprisonment for up to five years. Furthermore, an unlicensed or unregistered MR/CE service providers may be subject to civil and criminal penalties for violations of the Bank Secrecy Act. In contrast, in Denmark, the current system is considered to be relatively ineffective because it takes a long time for law enforcements to investigate and prosecute persons in the case of unregistered activities. However, Danish AML supervisors in close co-operation with the State Prosecutor have decided to intensify the sanctions in cases of non-compliance.

56. In Mexico, the Tax Administration Service, a decentralised entity of the Ministry of Finance and Public Credit) is in charge of the supervision of money remitters (*transmisores de dinero*) and currency exchange centres (*centros cambiarios*) regarding the AML/CFT preventive measures in Mexico. With regards to supervision, in the case of *casas de cambio*, these are by decree of law supervised by the National Banking and Securities Commission (CNBV).

57. Although there is no agency that supervises CE service providers in Japan, such businesses must report the volume and number of transactions to the Ministry of Finance when they exceed a certain volume.

---

18 See Annex 3, Table 4.

19 See Annex 3, Table 5.

CHAPTER II - MONEY LAUNDERING METHODOLOGIES INVOLVING MONEY REMITTANCE AND CURRENCY EXCHANGE PROVIDERS

58. This chapter describes some of ways in which money remittance and currency exchange providers have been exploited for ML/TF purposes through a series of selected case studies provided by responding jurisdictions. The focus of this material is primarily on "traditional" *i.e.* formal money remittance and currency exchange providers; however, a few observations have also been included about informal systems.

59. Generally, these MR/CE providers can be used for money laundering and terrorist financing in two ways: either by performing relevant transactions without knowledge of the illegal origin or destination of the funds concerned or by a direct involvement of the staff/management of the provider through complicity or takeover of such businesses by the criminal organisation.

60. Several features of the MR/CE sectors make them an attractive vehicle through which criminal and terrorist funds can enter the financial system, such as the simplicity and certainty of MR/CE transactions, worldwide reach (in case of money remitters), the cash character of transactions, low-thresholds, the often less stringent customer identification rules that apply to such transactions compared with opening bank account and reduced possibilities for verification of the customer's identification than in credit or other financial institutions , etc. The nature of the customer's relationship with the MR/CE service provider and the brevity of contacts is also a significant vulnerability.

61. Money remittance providers are used at all stages of the money laundering process. Currency exchanges specifically are an important link in the money laundering chain, particularly during the placement stage. Once the money has been exchanged, it is difficult to trace its origin. Also, it has been noted that considering that they are small businesses, currency exchanges can be easily prone to takeover by criminals and used to launder money.

62. From responses received to the survey questionnaire for this project, the most important factors that may indicate possible misuse of MR/CE service providers:

- Use of underground remittance systems;
- Use of mules / straw accounts;
- Mismatch between the economic activity, country of origin, or person and the money remittances received;
- Periodic transfers made by several people to the same beneficiary or related persons;
- Transfers over a short period of time of low amounts that together represent a large sum of money;
- Transfers from one or more senders in different countries to a local beneficiary.
- Sudden inflow of funds in cash followed by sudden outflow through financial instruments such as drafts and cheques;
- Structuring of transactions and/or changing of MR/CE provider for subsequent orders to keep a low profile; and
- False information during the identification procedure/lack of co-operation.

63. Many cases involve small value wire transfers, however, given that the total value of funds involved in these cases is quite significant, this could imply the involvement of highly organised criminal groups. However it is also interesting to note that a number of cases deal with high-value wire transfers. The information gathered highlights the links between money laundering in the money remittance sector and other criminal activities (*e.g.*, fraud, trafficking/smuggling in human beings, drug trafficking, economic crime, etc). The identified ML vulnerabilities associated with the MR/CE sectors can be related to customers, owners or agents as highlighted below.

2.1 Customers

64. Structuring or "smurfing" was frequently reported and appears to remains the most usual ML method identified in regard to MR/CE providers and the most frequently reported suspicious activity in many countries. Structuring occurs when a person carries out several cash transactions by breaking them into smaller amounts in order to avoid the mandatory threshold reporting and/or customer identification requirements. Such transactions can be carried out either in a single day or over a period of days, through the same or several agents.

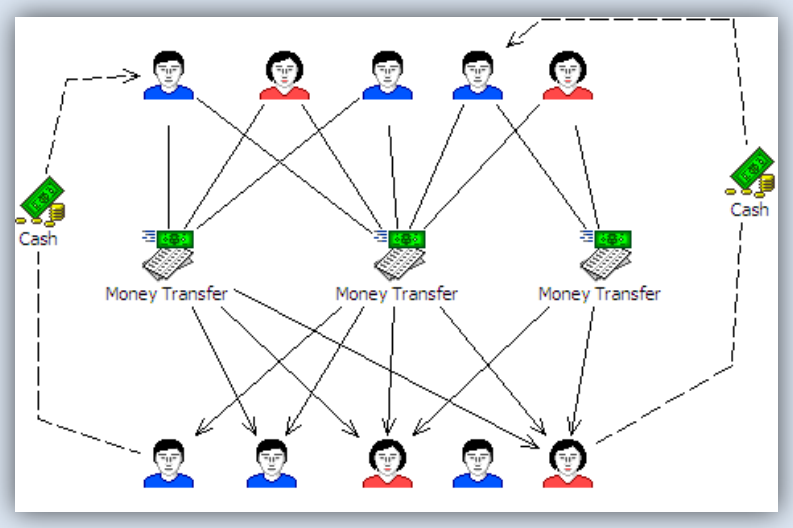
Box 1. Structuring

Customer: individual/ business

Mechanism: money remittance

Red-flag indicators: use of several currencies, structured transactions, a great number of persons involved, large number of transactions related to each other during a short time period.

Case description: Several Bulgarian individuals and companies sent/received a large number of remittances to/from different persons and destinations (often in a number of foreign countries) during a short period of time. Then they temporarily stopped their activities for a while and after a short period of time, the transfers started again. In this scheme large amounts were fragmented into smaller amounts, sent to a great number of persons in different countries and finally returned to the originators. The total sum of received and sent remittances was almost equal, and the persons declared they knew the persons who were the beneficiaries of the transfers ordered by them. Transfers were made in several currencies, where the change from one currency to another was performed between the transfers without any reasonable explanation. The investigation detected that many of the foreign persons involved in the scheme had a criminal background or had been convicted for drug trafficking, prostitution, etc.



Source: Bulgaria.

65. In countries where there are many MR/CE service providers, it is difficult to cross-match data, and the risk of being involved in "smurfing" schemes is therefore typically higher than in countries where there are few service providers. The abundance of MR/CE service providers makes structuring a relatively "safe" choice for the criminals in most countries and minimises the possibility that law enforcement agencies might detect such activity unless there is well-functioning co-operation at the national level that then helps to identify smurfing schemes that may be using multiple service providers.

66. It is often very difficult to find a link between persons using money remittance services for the transfer of funds because the transaction paper trail is often lacking. The nature of MR/CE business is that service providers often carry out one-off transactions with occasional customers, and many of the customer relationships that do exist are not of a durable nature. In the case of one-off transactions, some MR/CE service providers are not able to monitor the financial behaviour of their customers in the same way as a traditional bank is able to do with its customers.

67. As a consequence, due diligence measures applied by some MR/CE service providers in less developed markets are usually at most confined to identification and verification of the identity of the person, without the possibility of ongoing monitoring of the customer's activities. In addition to the name of the customer, the indication of the beneficiary (sender or receiver), the destination or origin of the funds, limited additional information is typically available for MR/CE providers.

68. Another method commonly identified in money laundering schemes is the use of straw men (so-called 'money mules'). A money mule is a natural person who makes his (bank) account available to a criminal or criminal organisation receiving some form of remuneration in return. A money mule is often solicited via a spam e-mail to accept a transfer of money –received from the victim(s) of a criminal or of a criminal organisation – which he/she then is instructed to transfer to the account of another person, whose personal details the money mule also receives via e-mail. The money mule is allowed to retain a part of the money for the services rendered to the criminal or criminal organisation.

Box 2. Use of 'money mules'

Customer: individual

Mechanism: money remittance

Red-flag indicators: use of straw men, organised criminals involved

Case description: An FIU from country A received a request for information from country B that involved among others company X, known to be alleged to have laundered funds by making multiple wire transfers to launder fraudulent card billing proceeds. According to this request a criminal network involved in credit card fraud schemes was using mules to transfer the profits of the illegal business to different parts of the world. The mules were instructed to send money only via money remittance services to hide the origin of the profits.

The undercover agent of country A succeeded to come in contact with one of the leading persons of this network (person C). The undercover agent convinced person C that it is better to use wire transfers through banking institutions instead of money remittance offices. This was done because the authorities of country A were trying to identify persons behind bank accounts instead of mules sending money via money remittance services.

Person C instructed the undercover agent to send money to company's X account in country A. From analysis carried out, it appeared that the money was transferred from country A to country B and most probably to accounts owned by the leaders of organised crime in that country.

Source: Cyprus.

69. The ultimate purpose for structuring transactions is to conceal the true beneficiary of the transaction and the origin of the money. Therefore, another potential risk for the MR/CE provider

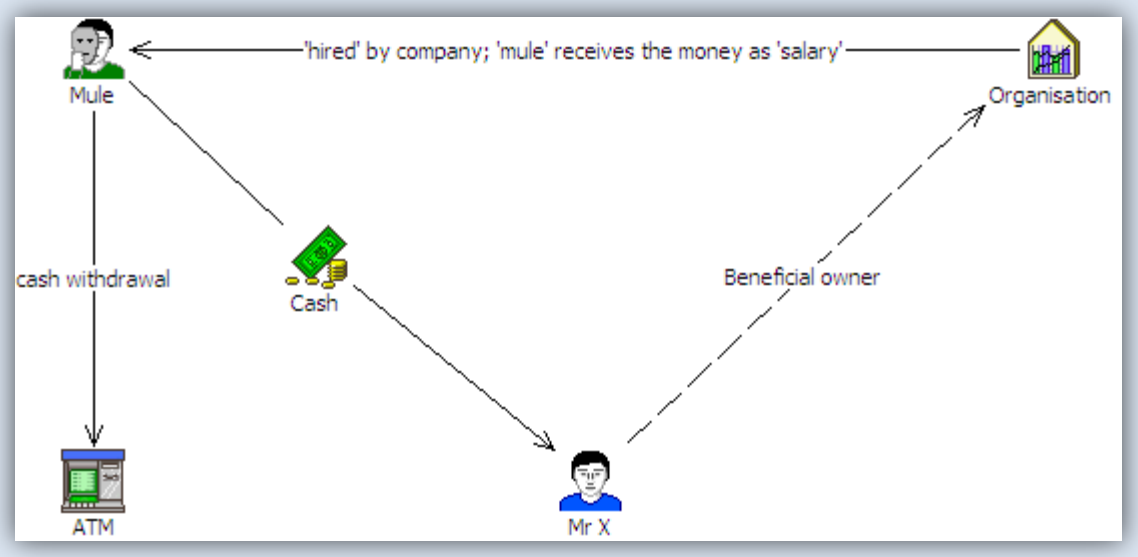
comes from accepting the money of straw men and persons identified on the basis of forged documents. Some examples of money laundering schemes obtained as part of this study involved straw men who were hired as 'employees' of a foreign company.

Box 3. Use of persons hired as employees to launder money originating from internet fraud

Mechanism: money remittance

Red-flag indicators: using 'money mules'

Case description: A person is 'contacted' (for example through the internet) for a job in a company established abroad. The person receives money on a personal bank account as a 'salary', withdraws most of money in cash immediately after the transaction (the 'commission', typically approx. 8% is often maintained in the bank account), and sends the money through money remittance abroad. Typically the true beneficiary of the transaction is a criminal and the scheme is used to launder money originating from internet fraud (phishing).



Source: Cyprus.

70. Yet another commonly reported method involves the use of a third person to transfer funds. Transactions carried out by the customer using (without a reasonable basis) multiple branches or agencies and third parties (for example relatives, minors) on behalf of another person are often aimed at concealing the sender and/or receiver (true beneficiary of the transaction).

71. Another way the MR/CE services may be misused in order to facilitate criminal or terrorist access to the financial system is through schemes with multiple money remittance transactions between persons not directly related. A reporting entity is not always able to effectively determine the connection between the transfers of funds and the related reason of the customer that sends or receives the funds. It is particularly difficult to understand the origin of the money and the scope of the transactions. For example, money transfer transactions initiated over a short time period by several persons to beneficiaries known to be linked to organised crime, executed in certain areas (in case of drug trafficking, in ports, for example), sent to 'dangerous' destinations (known as drug trafficking routes for example) should raise the concern of the remitter. It is often difficult for law enforcement agencies to detect whether the transaction is of a legal nature (for example, persons working abroad and sending income to his/her family via MR services) or as part of an illegal network (forced transactions, for example in relation to prostitution/human trafficking).

72. One of the patterns associated with such schemes also appears to be an indicator of possible ML is receiving transfers from unusually high number of people (often from different countries and in different currencies). The linked nature of the transaction often becomes apparent because several individuals go to the same institutions in the short time period to send money in the same countries and often to the same beneficiaries[20]. These elements usually indicate that the senders and/or receivers may be part of the organised networks[21].

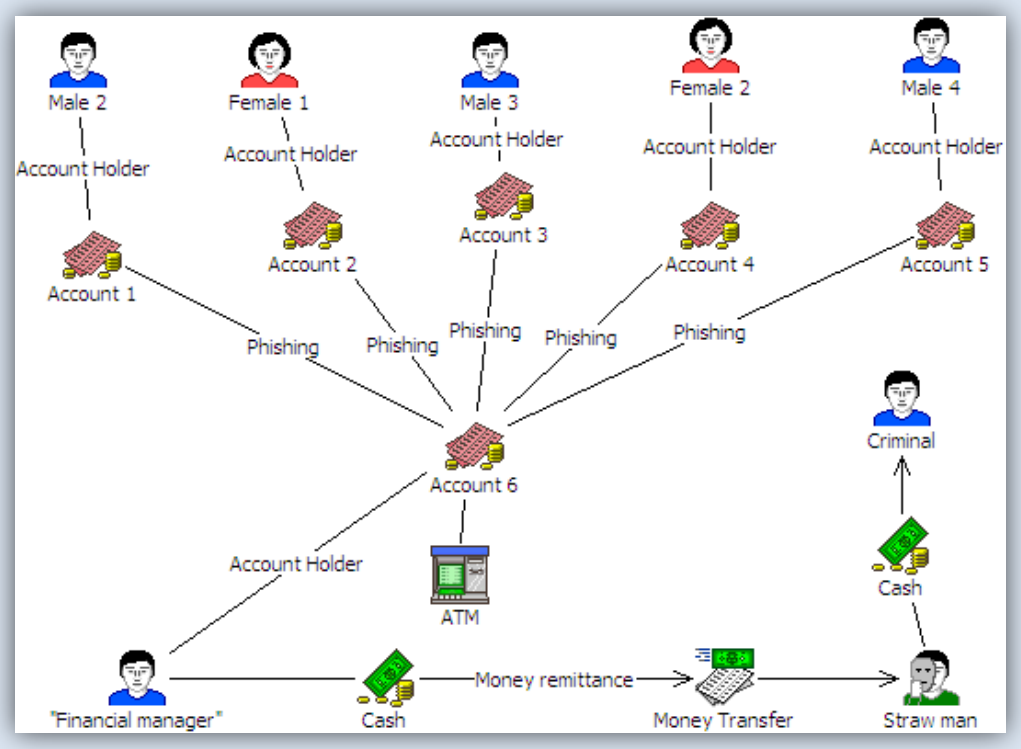
Box 4. Linked nature of the transactions

Customer: individual

Mechanism: money remittance

Red-flag indicators: receiving funds from high number of senders over a short period of time, large-sum transactions compared to person's living standard

Case description: A person is a beneficiary of a great number of remittances (often in relatively small amounts) during a short time period. Sometimes 'mules' are used as intermediaries to make the scheme more complex and harder to follow by the law enforcement agencies. In this case intermediaries re-order the remittances immediately again through the money remitter. Often the value of money remitted does not correspond to senders' economic profile.



Source: Bulgaria.

73. MR services offer widespread and legitimate services to immigrants. They serve the unbanked, provide a convenient, efficient and cost-effective means to send money to an immigrant's home country and often can reach remote areas and locations beset by political instability that are

20 See CTIF-CFI (2003), *pp* 106-107.

21 FATF (2005), *pp* 74.

otherwise outside the networks of the international banking system. However, investigations in some countries have shown that the services provided by some MR businesses have also been linked to human trafficking and the repayment of 'human trafficking agents'. As an example, in certain trafficking cases, money remittance providers have been used to pay mules, intermediaries, airplane tickets, etc.

74. Other ML methods detected in cases involving MR/CE services include transactions with companies incorporated in countries with low or no taxation (no or insufficient AML/CFT measures, known routes for ML/TF, etc.), the use of new payment methods to launder funds, often without a physical presence, and the potential for offshore service providers to access a foreign market online or via a wireless ATM network, evading AML/CFT requirements of jurisdictions.

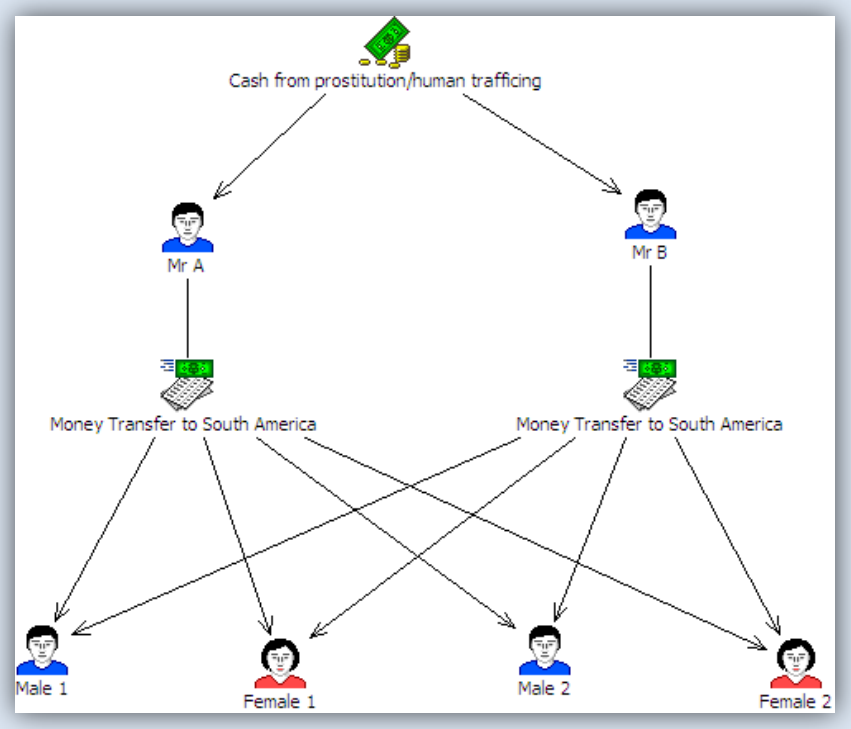
75. The use of forged identity documents is another method commonly identified and which appears to be to be increasingly used. This is particularly difficult to detect by MR/CE providers, especially due to the increasing quality of those forged papers or given that customers are often occasional and the business relationship is not of a continuing nature. False identities are often used to hamper further investigation on the transfers/ operations.

Box 5. Use of false identities

Mechanism: money remittance

Red-flag indicators: structuring, same beneficiaries, a large number of transactions during a short time period

Case description: Persons A and B repeatedly made cash deposits sent via money remittance to South America to the same recipients. In a few months time the money remitted amounted to several thousand EUR. There was no economic background for the transactions performed. None of the individuals resided at the stated address. The remittance forms revealed that most of the money was sent by A, after which B took over the transactions with the same beneficiaries. When the identification papers of the two individuals were compared, it turned out that A and B were in fact one and the same person. Police sources revealed that A's identity featured in an investigation regarding human trafficking and exploitation of prostitution.



Box 6. Remittances to high risk countries

Customer: individual

Mechanism: money remittance

Red-flag indicators: structured transactions, several beneficiaries, remittances to high-risk countries, use of straw men, people involved have a criminal background, the volume of remittance is not in accordance of the economic profile of the sender

Case description: The financial intelligence unit received several unusual activity reports from the postal bank regarding money remittance through a well known money transmitter that were done by a number of entities with no apparent relation between them, from country A to several countries in South America.

Analysis of information revealed that a number of transfers sent abroad were made in small amounts. Transfers were made from different branches of the postal bank all located in the same geographical region in country A to various beneficiaries located in several countries in South America, which are considered high risk countries with regard to the manufacturing of drugs. The entities that made money remittances had no criminal or intelligence record and were usually young people with low reported income and no property. Therefore, suspicions were raised that they were straw men. A connection was found between one of the persons involved and a large criminal organisation known to be operating in drug trafficking. A co-operation with one of the South American FIU revealed that one of the beneficiaries was in jail for drug trafficking.

Source: Israel.

2.2 Owners and agents

76. Obtaining an ownership over MR/CE company either directly or via sub-agent relationships provides criminals a perfect tool to manipulate the money transfer system and to launder money. Detecting such cases is particularly difficult for law enforcement agencies, and to a certain extent, it also depends on the capacity of the entity to apply know-your-customer and reporting requirements effectively. Several examples were provided in the survey responses gathered for this research which illustrate cases where the MR/CE company was owned and used by criminal organisations to launder money or where the company was complicit in providing services to an organised group.

Box 7. Use the ownership in MR/CE company to launder money

Mechanism: money remittance company/ currency exchange

Example 1 – Mr B is the owner and CEO of a money service business registered in country A. Mr B engaged in check discounting for a commission. He used the bank accounts of various companies and provided straw men to act as beneficial owners and authorised signatories of the bank accounts. Mr B discounted cheques for his customers using these bank accounts. Mr B made use of the services of other MR/CE service providers which recorded his transactions under another name. He discounted cheques in return for cash for his customers, and in turn, discounts the cheques received from his customers at an MR/CE, with instructions not to record his name so that a report would not be filed. Stolen cheques were brought to Mr B for discounting, and so as not to be connected with them, he gave them for discounting to another MR/CE, which recoded the transaction under the name of a straw man. Mr B instructed the customer to say that he delivered the cheques for discounting to the straw man, and instructed the straw man to say that he received the cheques from a customer, in order to hide his own involvement with discounting the stolen cheques. Mr B was indicted of money laundering offences.

Source: Israel.

Example 2 – Currency exchange business providing services to organised crime group

A currency exchange company in Sweden was identified as providing services for organised criminals. A lot of “runners” came to the exchange office several times a day and made large cash

withdrawals. Some "runners" had during a period of months made withdrawals for millions. The money was used for paying to black labour. STRs were received from banks indicating money flows from different companies' bank accounts to the bank account of the currency exchange-company. The owner of the currency exchange company was later prosecuted and convicted.

Source: Sweden.

Example 3 – Criminal group obtaining ownership over sub-agents of money remitters and exchange offices

Several Bulgarian citizens and companies where the citizens were beneficial owners were involved in large ML scheme. The companies received transfers to their bank accounts in different Bulgarian banks and transferred the money to foreign company A. The ultimate beneficiary of all money transfers was company B, one of the Bulgarian companies.

The investigation carried out by FIU detected that a group of Bulgarians bought up sub-agents of MR and CE. After a change in ownership, the total number of transfers received multiplied and a great number of transfers in small sums were ordered by foreign citizens. Beneficiaries of those transfers were typically Bulgarian citizens and the company B. It was also found out that the ultimate beneficiary of the transactions received by the individuals was company B.

It is suspected that the funds originated from drug trafficking. The scheme was of a significant scale, involving dozens of natural and legal persons from Bulgaria and foreign countries. The amount of funds transferred through MR system was several millions of Euros.

Source: Bulgaria.

Example 4 - In October 2008, 5 persons pleaded guilty to one count of operating an illegal money remitting business in the US. According to documents filed with the court and statements made in court, persons operated different enterprises. From December 2005 to March 2008, the defendants managed illegal and unlicensed money transmitting businesses in Connecticut. In exchange for remitting a total of more than USD 22 million from Connecticut to Brazil and for guaranteeing the anonymity of both their customer and their customer's intended beneficiary, the defendants took a percentage of the remitted funds for their own financial gain. Several other persons have been pleaded guilty in committing the crimes similar to this, the destination of the transfers have been to Middle East countries.

Source: United States.

Example 5 - Use of agents of money remittance business

A suspicious transaction report from a money remittance business was received in the FIU. The report revealed that one of the agents of the money remittance company was making operations with the following characteristics:

- Every remittance operation was sent to country B (Country B was a drug producing country).
- The amount sent in every remittance operation was higher than usual for money remittance operations to country B.
- In the period of time of one year, the senders of money never made more than three operations.
- Every sender sent money to different receivers.
- There were no apparent relationship between the sender and the receiver of the money.
- The receivers never received money from more than three or four senders.

After making a more comprehensive analysis, other agents of different money remittance companies with similar operational profile were discovered.

Police investigations revealed that those agents were working together in a joint action with the objective to launder money for a drug trafficking organisation. Money laundering and drug trafficking organisations were dismantled. The information was shared with country B, where several police operations were carried out.

Source: Spain.

Example 6 – Ownership of bureaux de change

A suspicious transaction report was received in the FIU. The report revealed that one person owned more than 15 businesses, and three of them were bureaux de change. The characteristics of the operations of the bureaux the change were the following:

- The bureaux de change mainly change European currencies, especially one.
- The amounts changed are higher than usual.
- There is no link between the amount of money changed and holiday periods.

Police investigations revealed that not so many people enter into the bureaux de change and, from time to time, a person made contact with the owner of the bureaux the change and gave him a bag with money in foreign currency. One or two days later the owner of the bureaux de change gave back the money in the local currency to that man. It was also established that the money laundered came from drug trafficking.

Source: Spain.

77. The following indicators could be relevant in this context:

- Reluctance by the MR provider to provide information about customers' identification to relevant stakeholders;
- Use of false identification and fictitious names for customers;
- Frequent transactions or purchases of negotiable instruments slightly under the legal threshold amount in order to avoid filing a STR/CTR;
- Turnover of the MR provider exceeds to a large extent the cash-flows of other comparable businesses;
- Suspicious connections of the MR provider owner; and
- Suspicious transactions performed on the bank accounts of the MR provider or its owner.

78. To deal with these vulnerabilities, most of the jurisdictions contributing information to this study require a 'fit and proper' test to be applied to the owners and managers of the MR/CE service providers at least as a component of a licensing/registration procedure. There are exceptions, as in Chile; Georgia; Hong Kong, China; Japan; and Mexico, where no specific requirements are applied for owners and managers of bureau de change. The most prevalent 'fit and proper' checks include determining that (1) the person has not been convicted for a criminal offence, (2) the person has not been denied the right to hold certain positions/undertake certain activities; and (3) the person has no outstanding tax obligations and not been in bankruptcy for a defined number of years.

2.3 Most common predicate offences identified

79. A number of law enforcement investigations have revealed that MR service providers are frequently used as a vehicle for laundering illicit proceeds. Laundered proceeds in such cases come primarily from drug trafficking, fraud (mainly IT-fraud like *phishing*); economic crimes (document forgery, malfeasance, tax evasion, etc); trafficking in human beings, smuggling of human beings; theft (credit card fraud, currency theft, etc) and smuggling (*e.g.*, tobacco, alcohol, arms). Previous FATF typologies have identified that ML schemes involving these types of crimes often appear to avoid using the banking system, and that systems for money remittance[22] are therefore sometimes specifically preferred as offering less risk of detection.

[22] FATF (2005), *pp* 73.

Drug trafficking

Box 8. Use of MR to launder money originating from drug trafficking

Mechanism: money remittance

Red-flag indicators: large scale of funds transferred compared to the socio-economic profile of the client, frequent transactions to different beneficiaries, transfers to high risk countries

Example 1 - A person made a large number of money transfer transactions to various persons over a short time period. The total amount of funds remitted amounted to a considerable sum of money. It was detected the ultimate beneficiary in the transactions was always the same.

Additionally it was noted that the individual had sent a considerable amount of funds to seven beneficiaries having the same surname as him. The financial intelligence unit noticed that the amount sent to three of them was significant compared to the general living standard of the recipient country. Another remarkable fact was that almost 25% of funds were transmitted to persons in the Netherlands. This could be indicative of an illegal operation to finance human smuggling or drug trafficking.

Source: Malta.

Example 2 – The financial intelligence unit received an STR from a commercial bank about suspicious money transfers through a well-known money transmitter. The report indicated that a group of persons systematically transferred sums averaging between 1000-5000 USD to a Latin American country, and that when conducting the transaction, these persons were always accompanied by an unidentified person. It also indicated that the names of the receivers of funds frequently are recurrent and almost always the same. The analysis established that in a period of 4 months (in 2005), 27 money transfers operations were performed by a group of 13 persons and that the transferred sum amounted to 111 400 USD. It was established links of group: 4 persons had criminal history background, 2 persons were cousins, others lived in the same street.

A special request for further information was sent to the criminal police. Answers received indicated that the persons had links with drug trafficking networks. A joint investigative group was established and with the use of operative and special investigative techniques, it was established that the group was linked to one of the most serious organised crime group. A drug trafficking channel from that country to Europe was identified, where the senders of cocaine are Lithuanian citizens. Cocaine was delivered by ship to ports in Varna (Bulgaria), Saint Petersburg (Russia) and Talinn (Estonia), with the major part of cocaine being delivered to Russia. After the drug deals, all the money was sent to Lithuania, and then transferred through the money transmitter back to Latin America. Overall, transfers were made by about 90 persons (mostly students, asocial persons). The total amount of transfers identified amounted to USD 540 000.

Source: Lithuania.

Example 3 – The financial intelligence unit received 38 STRs made by a money remittance business involving transactions made by 38 persons to Mr A, including relatives and friends of this person. Money received had similar characteristics and circumstances, such as:

- close date of transaction (between January and June of the same year)
- same amount (USD. 6000 and/or USD 5000)
- same country of the sender
- same name of the senders or with variations in their names.

The analysis of the database enabled to identify that persons related to Mr A. had purchased luxurious vehicles in cash; that there was an indirect link with Mr and Ms B, citizens of country Y, who were suspected to be part of a drug trafficking organisation (subject to another financial intelligence report) and that there was a link with the case of Mr C, who has been detected by national and international customs authorities relocating approximately USD 980,000.00

Source: Peru.

Box 9. Use of MR for cross border transfer to "unusual jurisdictions"

Mechanism: exchange bureau

Red-flag indicators: money transmitting by criminals, MR to unusual jurisdictions

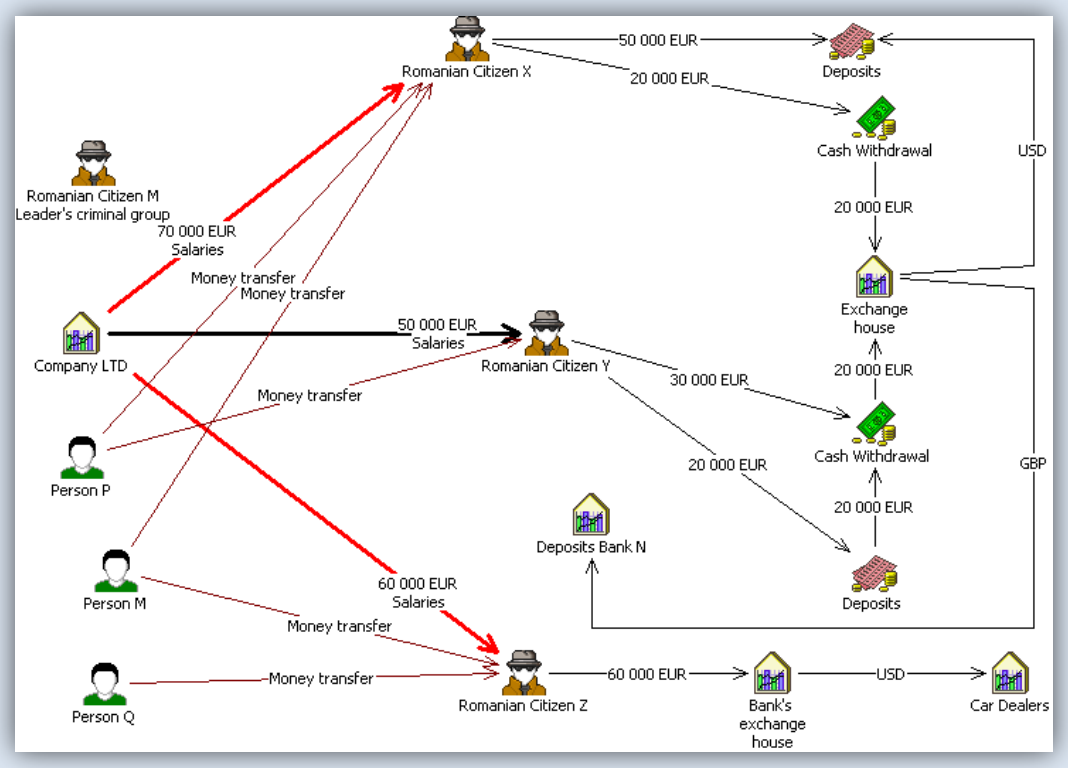
Example – the Romanian FIU received an STR sent by a bank regarding some suspicious cross-border transfers. Thus, three Romanian citizens (X, Y, Z) received small amounts from company LTD (established in country A), justified as "salaries". After receiving money, X, Y and Z used several schemes o launder money, some of which included exchange houses to change the currency. For example, on the same day when Mr X received a large bank transfer from Mr M, he withdrew the amount of EUR 20 000 in cash, went to the exchange office and changed Euros to USD dollars. At the same day he visited the bank used for receiving money once more and opened bank account where he deposited EUR 50 000. Mr Y withdrew the money received and opened bank accounts in smaller amounts in several other banks, exchange houses were used to change the currency. Mr Z changed EUR 60 000 in Bank's exchange house (whereas X and Y used private exchange houses) and used it to buy cars.

Suspicious elements:

- Cross-border transfers consisting in small amounts under the reporting threshold
- Frequency of cross-border transfers

In a short period of time amount received by the Romania citizens was around EUR 180 000.

The request of information was sent to country A and the answer revealed that company LTD was involved in funds transfers in Eastern Europe, the proceeds originated from drugs and weapons trafficking. The originator of the cross-border transfers originated by X, Y an Z was Romanian citizen Mr M, the person leading the company LTD, known as the leader of a criminal group involved in drug trafficking and skimming. It was also detected that Mr M used forged identity document in order to transfer money to Romania. It was also detected that X, Y, Z travelled to country A occasionally, but none of them worked or obtained legal income there. X, Y and Z could not prove that they worked or obtained any legal income from country A, they could not explain the large amount of money that were transferred to their accounts.



Source: Romania.

Fraud

80. The "advance-fee fraud is a classic scheme but still successful in many cases. Typically an e-mail is sent to victim where cash is promised (for example, "you won the lottery" or "please help us conduct a transaction"). The e-mail also indicates that certain costs must be paid before the winnings can be awarded and/or the transaction can place. In addition to bank transfers, money remittance agencies and agents of known money remitters (Western Union, MoneyGram, etc) are often cited as the means to effect the necessary payment. After the victim has transmitted the money, the criminals disappear, and of course the victim does not receive any reward. A variation of this type of fraud occurs when the fraud involves the offering of some sort of product or service.. In the case of dating scams, for example, fictitious profiles are created by the criminals on internet dating web sites. Through these fictitious profiles, the criminals gain trust of the victim and ask him/her to send money, for various expenses, such as plane tickets, family aid, etc. Often the potential victim is requested to send the funds through money remitters.

Box 10. Fraud

Mechanism: money remittance

Red-flag indicators: cost of receiving the winnings is asked to pay beforehand

Example - Telemarketing fraud using MR/CE service providers to launder the proceeds

Telemarketing sales persons defrauded victims mainly among older population, by posing as various officials. The victims were told that they had won the lottery and that they had to pay a certain sum as a handling fee before they could collect their winnings. These sums varied between 10.000 USD and 80.000 and were paid, among other ways, by bank cheques, or via Western Unions' postal service to fictitious beneficiaries. The cheques were apparently transferred to a professional money laundered who transferred them to MR/CE service providers in country A and territory B. The cheques were discounted and deposited in the MR/CE service provider's own bank accounts. The cheques were then sent to be cleared in the foreign banks from which they were drawn, at which time their source was revealed.

Source: Israel.

Trafficking in human beings and migrant smuggling

Box 11. Trafficking in human beings and migrant smuggling

Customer: individual

Mechanism: money remittance
Red-flag indicators: large number of transactions to the same beneficiaries, the person does not hold any bank accounts

Example 1 - An individual A residing in an Eastern Europe country received hundreds of funds transfers usually in small amounts through an MR/CE service provider initiated by more than 35 women of the same nationality as individual A. Typically the number of remittances initiated by one person was small (four on average). The addresses disclosed by the women referred to different hotels situated in Paris. Most of the women did not have a criminal record and did not hold a bank account. One of the women however had opened bank account in France and indicated as her address the address of a company whose manager was convicted for aggravated procurement some years ago.

The case was transmitted by Tracfin to the judicial authorities on a presumption of involvement in the procurement of prostitutes.

Source: France.

Example 2 - Use of MR to launder the money from prostitution mediating

The Cypriot financial intelligence unit in co-operation with the Cyprus Police conducted an investigation in relation to the activities of a lady from Asia working in Cyprus for the last eight years as a housekeeper. According the facts of the case and to information obtained from the Police, suspicions were raised that she was a prostitute. Co-operation with all the local and international financial institutions in Cyprus revealed that she did not hold any bank account in Cyprus. Further co-operation with all the Money Remittance offices in Cyprus revealed that she used MR instead. From analysis and investigation carried out from the information obtained from the Money Remittance Offices she sent a significant amount of money outside Cyprus. She also collected and sent small amounts of money from other nationals, women that according to information from the police were also involved in prostitution activities. According to the analysis the suspect sent money to her country and also to both E.U. and non-E.U. countries to different persons each time. The funds that she sent did not correspond with her salary.

Source: Cyprus.

Example 3 - A suspicious transaction report from a money remittance business was received in the FIU. The report revealed that different women were sending money to the same country. Most of the operations were sent to the relatives of the senders, but sometimes one or two operations were sent to two different persons (A and B) in the destination country in amounts higher than usual. After a first analysis other groups of women with the same operational profile were discovered and it was noticed that A and B also were receiving money from them.

A police investigation was undertaken which established that the senders were women that were working in prostitution activities and that the money sent to A and B was to pay the debt to the illegal immigration organisation in the country of origin.

Source: Spain.

Terrorism

Box 12. Terrorism

Mechanism: money remittance

Red-flag indicators: money transmitting by criminals, MR to unusual jurisdictions

Example 1 - Mr X was a defendant of operation CREVICE, a case concerning the purchase, transportation, concealment of fertilizers for use in the construction of an improvised explosive device. Mr X was found guilty in 2007 of conspiracy to murder and conspiracy to cause by an explosive substance an explosion of a nature likely to endanger life or cause serious injury and damage to property. He was sentenced to a custodial sentence of forty (40) years. Between 07/11/03 and 12/11/03 Mr X withdrew GBP 2540 (sterling) in cash from his Barclays Bank PLC account. On 12/11/03 Mr X sent £2471 to person Y in Kharian, Pakistan via UK Western Union money transfer, converting to 233,326.5 rupees. Mr Y is a US citizen and was arrested by the FBI in April 2004. He pleaded guilty to committing terrorist offences and was sentenced to a custodial sentence of seventy (70) years.

Source: United States.

Example 2 - In November 2008 a Pakistani national Mr X residing in the US was sentenced to 110 months in prison, followed by three years of supervised release, for conspiring to launder money and for concealing terrorist financing. He was also ordered to forfeit assets worth USD 2 208 000. Mr X operated company A, Inc., a money remitting business in Washington, D.C. Mr A, company X, Inc. and five other defendants allegedly conspired to launder over USD 2.208 million received from a cooperating witness working with ICE and FBI agents. The money was purported to be the proceeds of drug trafficking, terrorist financing and trafficking in contraband cigarettes.

Source: United States.

Example 3 – Between 2000 and 2007, Mr. A received 102 money transfers of a total amount of USD 203,768.91. During the same period, Mr. A sent 120 transfers abroad for USD 107,000.00. to various countries, primarily to the United States, Ecuador, Colombia, Guatemala, Mexico, India, Egypt and

Bolivia. Mr. A has been detained in 2007 by the authorities for being related to an alleged international criminal organisation responsible for smuggling persons illegally to the United States. Several persons coming from countries such as Malaysia, China, Korea, India, Iran, Irak and Egypt were sheltered in Peru by Mr. A and his local associates. Then, they followed the route to the United States through Ecuador, Guatemala and Mexico. According to the Peruvian police, there is a possible link between Mr. A and a member of the terrorist group, who is detained in Venezuela. Among indicators having triggered the suspicion was the fact that there was no link between the person making the transfers and the variety of countries to which transfers were being made.

Source: Peru.

2.4 Informal money remittance services

81. Informal money remittance systems can be used to send money around the world. They are often linked to a certain geographical region and go under specific names such as *hawala*, *hundi*, or *hawilaad*, depending on the geographical or cultural links of the persons who establish or use them. These are underground 'banking' channels in which the transactions are settled by offsetting an equivalent some at the receiving location. The transfer request is made in one location (where funds the funds to be transferred are received). The counter value is then distributed to a beneficiary at another geographic location through one of the network's correspondents. These systems have numerous advantages: they are quick, discreet and reasonably priced, which makes these services attractive for both legal and illegal use. In recent years it has become clear that informal money remittance systems play an important role in international terrorism financing and that they are a suitable medium for terrorists to transfer money[23] .

82. Detecting these underground systems is by definition very difficult. In countries with alternative money remittance systems, it is often difficult to prove illegal activities in these systems as they are often trust-based, secretive and unregistered, with indirect fund movements. It is therefore difficult to assess the degree of compliance even when informal value transfer service providers are legal. In most countries having experience with such systems, informal remittance services are illegal. In others (Denmark, Sweden, United Kingdom, and United States, and in some cases in Germany), their activities are regulated by the AML/CFT regime.

83. Underground remittance activity, particularly that which is carried out by immigrants, serves a legitimate need, but also offers a potential for misuse for ML/TF purposes. For instance, due to the lack of effective monitoring, anonymous customer transactions can take place and customer's beneficial owner can be hidden.

84. To guarantee that informal systems are not operating in an unregulated manner, the safeguards below are often used:

- Adoption of legislation, in compliance with FATF SR VI, requiring the licensing and/or registration of MR/CE services.
- Regulating the operations of the MR/CE services, including licensing and /or registration, identification and awareness-raising, the adoption of AML/CFT laws and regulations, monitoring of compliance with those laws and regulations; and creation and implementation of a sanctions regime.
- Implementation of an effective currency transaction report and suspicious transaction report system, which includes effective analysis by a supervisory agency that cooperates with law enforcement. Non-registered MR/CE services are often identified through

23 FATF (2003), *pp* 11

reports by other currency suppliers under the reporting regime; by tip-offs made to the supervisory agency; and by analysis of information coming to the supervisory agency's attention either from its own staff/activities or from that of other law enforcement/regulatory agencies.

- Effective supervision by regulatory authorities (on-site inspections; oversight over high volume/ number remittances with no apparent economic substantiation, risk-based examinations, timely law enforcement actions, etc.) and close co-operation between supervisory and law enforcement authorities.

85. Several countries, such as Austria; Hong Kong, China; France; Germany; Netherlands; Spain; and the United States indicate that they have prosecuted individuals for criminal activities related to informal money remittance service. As illustrated in the examples below, the reporting parties can play a very important role in this detection.

Box 13. Use of Informal MR System

Mechanism: informal money remittance system

Example 1 - An East African residing in Belgium, Mr X, stated that he performed Hawilaad banking activities. His account was exclusively credited by cash deposits and numerous transfers in small amounts. During several months the funds were transferred to company A in Eastern Africa. Shortly afterwards the funds were transferred to company B in Western Europe. Companies A and B performed money remittance transactions around the globe. Mr X claimed that he performed Hawilaad activities for fellow countrymen wishing to send money to Eastern Africa. However, he did not hold any position within Belgian companies and he was not registered as manager of an authorised exchange office. The individual did not have an authorisation from the CBFA (banking supervisor) either. Police sources revealed that he was known to be a member of a terrorist organisation. In this case the alternative remittance system may have been used for terrorism financing. The police are investigating.

Example 2 - In September 2008 Mr X, a Pakistani national residing in Canada, pleaded guilty in the U.S. to conspiring to launder money. According to his guilty plea, Mr X operated a money transfer business in Montreal, Canada to transfer monies abroad through an informal money transfer system called a "hawala," using a network of persons and/or businesses to transfer money across domestic and international borders without reliance upon conventional banking systems and regulations. A cooperating witness, acting at the direction of law enforcement, held himself out to Mr X and his associates to be involved in large scale international drug trafficking and international smuggling of counterfeit cigarettes. From January 2004 to November 2005, Mr X assisted co-defendant Mr Y in 10 hawala transfers from the U.S. totalling USD 828 000 in U.S. currency provided by the cooperating witness. The cooperating witness represented that the monies sought to be transferred were the proceeds of drug trafficking, and Mr X laundered these funds believing they were to be used to support those activities.

Source: United States.

CHAPTER III - KEY FINDINGS

4.1 Assessing ML/TF risks and threats within the MR/CE sector

86. Based on the analysis of information provided through the survey, the project team identified certain potential vulnerabilities in the money remittance and currency exchange sector.

Assessments by competent national authorities

87. From the responses received, it appears that so far only a few countries have conducted assessments of ML/TF risks or threats in the MR/CE sector[24]. Countries where the risk assessments have been made and where the risks have thus explicitly addressed can be divided into two groups:

- Countries where the financial intelligence unit assessed the ML/TF risks posed by money remittances and currency exchange (Bulgaria, Estonia and Poland, for example). These risk assessments are mainly based on analysis of suspicious transaction reports and the results of law enforcement actions.

- Countries where the national risk assessment was performed on an interagency basis (Netherlands, Spain, and the US, for example).[25] In these assessments, the expertise of the FIU and the investigative authorities was used; however, significant involvement from other relevant stakeholders (representatives of the private sector, scholars, etc) also occurred.

88. In conducting risk analysis for the MR/CE sectors, it appears that such analysis cannot be done solely by looking at individual STRs. Whilst relevant disclosures usually capture specific remittance transactions, this approach lacks a more strategic perspective that could help identify relevant flows and trends. A proactive approach appears to be needed that will allow the evaluation of relevant flows, coupled with the consideration of socio-economic factors such as the distribution of immigrant communities, the destinations of remittances, the extent and features of the informal sector, the strategic location of the country, etc. This appears to be an advantage that the interagency approach can provide.

89. In addition to the STRs, intelligence developed by those authorities with supervisory responsibility over the MR/CE sector has proven to be valuable source of information when analysing the potential threats and new and emerging trends.

90. The national experience derived from identified ML/TF schemes in which money remittance and currency exchange providers were involved (the intelligence emerging from STRs analysis) can

---

24 For a detailed overview of the ML&TF threat assessments in FATF member states, please refer to FATF (2008b).

25 In the US, the National Money Laundering Threat Assessment conducted in 2005 as an inter-agency initiative included MSBs as well as online payment systems, informal value transfer systems, insurance companies, trade-based ML and bulk cash smuggling. The U.S. published a follow-up national strategy in 2007.

contribute to reviewing the legal framework at national level (and supranational/ EU level as well) to guarantee the effectiveness of the system in the light of the new services.

91. For example, in Germany and the UK[26], a periodic overview of the AML/CFT threats posed by MR/CE businesses is published. The overview contains up-to-date information on threats and trends identified on the basis of STRs.

92. A specific example is related to the assessment of risks posed by the introduction of the euro. Of the FATF and MONEYVAL member States from the euro zone, the information provided indicated that only five countries had conducted an assessment of the related ML threats[27]. The scope of each risk assessment varied substantially, while in some countries a special committee was set up that co-ordinated the risk assessment and management, in other countries the process was rather informal.

Box 14. Examples of experiences in assessing risks posed by the introduction of the euro

In the Netherlands, the ML threat assessment was addressed by an official working party which was established by the Dutch Ministry of Justice. Typologies and risk indicators were developed from the results of this working party.

France set up a task force at the national level in 2000, coordinated by the FIU (Tracfin) and comprising representatives of the judicial police, the customs, the Bank of France and the banking supervisor. The task force was in charge of conducting risk analysis, raising awareness and coordinating prevention and detection of suspicious transactions in relation with the adopting euro. At the international level, Tracfin invited its EU counterparts concerned by the adoption of the euro to a meeting in 2000 to ensure the best and timeliest co-operation in exchanging information, on the basis of MoUs already signed or via the Egmont secure website. A contact person was designated in each of the twelve FIUs to deal specifically with any transaction and information related to the Euro.

In Italy the ML/TF risk assessment of adopting euro was analysed in-depth and involved both reporting entities and competent authorities. Indications were provided to reporting entities for the detection of possible suspicions, particularly related to the need to convert cash or other means of payment of illegal origin into the single currency within the set deadline. A peak of disclosures was registered in the change-over phase, leading to the detection of possible illegal financial transactions. Together with instances of money laundering, several cases of fiscal violations were identified.

In Malta, the FIU specifically addressed the ML threat to MR and bureaux de change in the period preceding the adoption of the euro. It carried out an assessment of the legislation in force at the time and consulted its EU counterparts, both in the euro area and prospective members of the euro area. The assessment revealed that the AML/CFT measures in place were sufficiently effective and there was no need to introduce additional measures. The FIAU recommended that only credit and financial institutions (as defined under Maltese law) be authorised to exchange Maltese liri into euro. Moreover the FIAU established a set of ad hoc guidelines for CDD for all financial and credit institutions. These guidelines directed mainly to credit institutions and money remittances/bureaux de change require, *inter alia*, to identify all persons requesting to exchange currency and any other person on whose behalf the person was acting, encourage the general public to deposit any amounts of cash into existing or new bank accounts prior to changeover, strictly comply with existing record keeping and reporting obligations and prepare staff by providing intensive training on AML/CFT procedures. Also, further to adopting the euro on 1 January 2008, a National Euro Changeover Committee was set up to

---

26 The UK threat assessment of organised crime 2009-2010 (SOCA (2009), *pp* 11) indicates that money service businesses (MSBs), which include bureaux de change, money transmission agents and cheque cashers, are frequently used by organised criminals to launder the proceeds of crime. Criminals may make small value transactions in high volume through legitimate MSB outlets that are not aware that their services are being abused, while complicit MSBs knowingly facilitate large volumes of currency exchanges on behalf of criminal customers.

27 The FATF examined the money laundering implications of Euro introduction in its 1998-1999 and 2001-2002 typologies reports.

oversee the process, in which the FIU was actively involved in this Committee

Although the UK is not a member of the euro zone the country has considered the specific ML threats associated with the introduction of the euro; UK experience has been that, as anticipated, demand for the 500 euro note in the MR/CE sector has been high (for smuggling/bulk reduction); UK reporting sectors were alert to the possibility of large quantities of stored legacy currencies surfacing for exchange, but there were few STRs about this in the event (and most were tax evasion focused).

93. Responding countries indicated that the ML/TF threat in the sector was primarily a result of both the direct penetration of organised crime group into operations of MR/CE providers and of the lax implementation of AML/CFT standards.

94. The absence of a formal risk assessment of the sector however does not mean that the vulnerabilities of the MR/CE have been completely ignored however. Several countries, where the risks to the sector have not yet been addressed through a national risk assessment emphasised that competent authorities constantly monitored the sector to identify the possible risks and vulnerabilities, meet to discuss the problems, and share their experiences.

4.2 Additional measures to be considered at national and international level

95. ***Knowledge of the sector, services offered and transaction channels***: Responses received point out that competent authorities in many countries do not have a comprehensive picture of the MR/CE sector and the services provided. The sector is very heterogeneous and remittance service providers innovate and evolve in developing new transaction channels. In certain jurisdictions, regulators do not engage in a continuous dialogue with MR/CE providers, thus they do not have a clear picture of the sector and measures taken by the businesses themselves regarding the control of their agents, of audit plans, how often agent locations are visited, the turnover of operators, etc.

96. ***Guidance and training*** – Money remittance and currency exchange providers tend to lack the capacity, experience and resources to implement AML/CFT requirements. Therefore regulators and/or supervisors have a key role to play in providing appropriate guidance to MRs and CEs. In this regard, adequate guidance for detecting false documentation appears to be a recurring issue of concern.

97. ***Implementation of CDD measures*** – Especially in countries where the AML/CFT legislation concerning MR and CE service providers is still relatively weak and developing (mostly due to the fact that countries are in the process of introducing the AML/CFT rules that are in accordance with international standards, such as in many countries of the former Soviet Union), the main problem found was weakness in implementing the necessary safeguards and control mechanisms relating to customer due diligence requirements (including adequate red-flag indicators for obligated persons). Because of the absence of durable relationships with customers and the nature of transactions, money remitters and currency exchange offices find it particularly challenging to perform ongoing monitoring with a view to detect anomalies and risk profiles.

98. ***Licensing / registration systems*** – Countries have not always clearly designated the regulatory or other authority to license and/or register MR/CE service providers and to monitor such business activity. When designation has occurred sometimes the licensing and control authorities are split between two agencies which can lead to weakness on oversight of the MR/CE.

99. The data gathered through this research did not permit a conclusion to be drawn on linkages between the abuse of MR/CE services and the type of regulatory framework, for example, whether the jurisdictions with a registration regime as opposed to a licensing regime tend to face more cases of the misuse of MR/CE services or whether jurisdictions with a higher threshold on CDD for wire transfers observe higher cases of abuse.

100. ***Supervision*** – The level of vulnerability of the MR/CE sector to misuse for ML and TF was found to be rather high, with some countries indicating high levels of non compliance. There appeared to be in some cases a lack of understanding on the particular nature of the MR/CE sector that make it vulnerable to misuse for ML/TF purposes.

101. ***Fit and proper*** – As described in Section II there is a risk in some instances that MR/CE operators or agents may be owned by criminals and that an adequate 'fit and proper' test should rule out as effectively as possible. One possibility used in some countries is the regular registration renewal obligation. This has helped to detect attempts at controlling the businesses and/or agents.

102. ***Agents*** – The monitoring of agents and sub-agents of MR/CE service providers appears to be lacking in some instances. Weakness in this area provides for a potential 'loophole' whereby agents might operate at 'arms length' on behalf of other CE service providers and/or are not subject to the 'fit and proper' test. The role of smaller and local players should not be underestimated.

103. ***Reporting systems –*** The implementation of reporting requirements, including the threshold-based reporting system, appears to have contributed to detecting ML in the MR/CE sector. It is noted that in several responding countries, MR/CE service providers rank among the top five in numbers of transactions reported as unusual or suspicious. In others, reporting in this area remains rather low, which may be explained by a variety of reasons (size of the sector, recent introduction of the reporting requirement, low understanding of the STR requirements).

104. ***Law enforcement action –*** The number of referrals, prosecutions and convictions based on STRs received from the sector appears to differ greatly from one jurisdiction to another. However overall, a discrepancy can be noted between the number of referrals and the number of prosecutions. The information gathered indicated that the law enforcement in many jurisdictions is unable to gather sufficient information upon which to act, mostly due to incomplete or insufficient records, and in some cases falsified ones. Following the money trail and seizing assets are a often a real challenge, and it may be impractical to focus on the individual MR/CE transactions between customers, rather than on the elements and data that the operator needs to collect and provide to the law enforcement.

CHAPTER IV – ISSUES FOR FURTHER CONSIDERATION

5.1 Assessing ML/TF risks and threats within the MR/CE sector

105. A non exhaustive list of issues and areas were identified by the project team as requiring additional efforts, in order to ensure that ML/TF risks are adequately addressed in the money remittance and currency exchange sector.

Assessments by competent national authorities

106. As indicated in the previous section, few countries have conducted assessments of ML/TF risks or threats in the MR/CE sector, and in certain cases, the analysis that has occurred has not taken been at a such a level that would help to identify related money flows and trends. It therefore seems logical that countries should be encouraged to carry out studies of their respective MR/CE sectors – using a strategic approach that integrates information and experience from a variety of sources – so as to better understand MR/CE activity and its potential vulnerabilities to misuse for ML and TF.

107. Furthermore, countries should also use their sector-specific threat/risk assessments to help identify gaps in the existing AML/CFT regulatory framework. When conducted on an inter-agency basis, national level assessments may derive the maximum benefit of the knowledge from different authorities, and the results can then be used as another input in the development of an overall national AML/CFT strategy. A sectoral risk assessment should not be just a one-off initiatives but rather on a continuing basis. Countries may want to consider the following factors, as noted in *FATF Risk-Based Approach: Guidance for Money Service Businesses* (FATF (2009)), when conducting a risk assessment:

- Political and legal environments.
- Country's economic structure.
- Cultural factors and the nature of civil society.
- Sources, locations, and concentrations of criminal activity.
- Size of the financial services industry.
- Ownership structure of MR/CE service provider.
- The scale of and type of business done by unregistered or unlicensed MSBs.
- Corporate government arrangements at MSBs and in the wider economy.
- The nature of the payment systems and the prevalence of cash-based transactions.
- Geographical spread of financial industry's operations and customers.
- Types of products and services offered by the financial services industry.

- Types of customers serviced by the industry.
- Types of predicate offenses.
- Amounts of illicit money generated domestically.
- Main channels or instruments for laundering or financing terrorism.
- Sectors of the legal economy affected.
- Underground areas in the economy.

Assessments by the MR/CE sector itself and measures at service provider level

108. It is also essential that MR/CE service providers assist in identifying, assessing and managing ML/TF risks associated with their products, services, customer groups, and geographical location. ML and TF risks should be assessed on a regular basis at a company level to ensure that the AML/CFT measures applied are up-to-date and appropriate. AML/CFT procedures to manage and mitigate these risks also need to be constantly under review and implemented.

109. It makes sense that MR/CE service providers should implement a risk-based approach that takes into account the particular ML/TF risks that their sector faces also in terms of the different players (for example, concerning MR/CE agents) and that they implement appropriate controls for higher-risk situations. On this issue, the FATF guidance on the risk-based approach lays out some of key factors and issues that should be considered by both the public authorities and the MR/CE service providers when implementing. For example, the guidance states that these businesses should pay particular attention to categories of customers that may indicate a higher risk, including:

- Customers conducting business or transactions in unusual circumstances;
- Customers who are politically exposed persons;
- Non face-to-face customers;
- Customers who structure their transactions;
- Customers who wire money to online gambling sites or high-risk jurisdictions;
- Customers who use agents or associates to hide beneficial ownership;
- Customers who know little about or are reluctant to disclose details about the payee;
- Customers or parties with no apparent ties to the destination country;
- Suspicion that the customer is acting on behalf of a third party but not disclosing that information;
- Transactions involving charities and other non profit organisations which are not subject to monitoring or supervision, like cross-border charities;
- Customers who have been subject of a law enforcement enquiry known by the MBS;
- Customers who use false identification;

- Customers who offer different identifications or identifiers on different occasions;
- Customers who receive transactions in a pattern consistent with criminal proceeds; and
- Customers who receive transfers in seasonal patterns consistent with criminal proceeds.

110. Regarding transactions conducted by MR/CE businesses, it is essential that there be control mechanisms that will permit the identification of any money flows or customers warranting closer scrutiny. This should also apply in cases of single-person businesses. In larger MR/CE businesses, the person responsible for compliance with AML/CFT measures should ensure that internal monitoring processes provide for effective controls and readily available information concerning, inter alia:

- Who approaches as a customer, how often, when, from where, remitting or receiving how much, and the probable and plausible rationale for that;
- Many customers sending to one beneficiary;
- One customer sending to several beneficiaries (and other similar schemes);
- The use of data and IT to scan for patterns of transactions.

111. There are a number of other areas which should be considered carefully by the MR/CE service providers. For example, the background of the employees should be carefully checked. Also, at the company level, it is important that employees regularly receive appropriate training on AML/CFT measures. Such training should ensure not only that they understand their responsibilities but also have sufficient knowledge to detect any suspicious activity. For this purpose, written compliance procedures are of paramount importance. Also, other issues include the need to prevent situations when data/ input by operators could be insufficient, incorrect or subsequently modified fraudulently without any possibility to track subsequent changes, which would impact on the usefulness or accuracy of the information kept by the MR/CE service providers.

5.2 Additional measures to be considered at national and international level

112. ***Knowledge of the sector, services offered and transaction channels***: There is clearly a need for competent authorities to understand fully how the sector operates and the services it provides, as well as developments in the sector, which could be exploited for ML/TF purposes. In order to further solidify understanding of the MR/CE sector along with its vulnerabilities, regulators should therefore engage in a continuing dialogue with MR/CE providers. Such a dialogue would also make them more aware of the measures that some service providers themselves already take to oversee the activity of their agents as far as compliance with AML/CFT measures.

113. ***Awareness raising*** – Outreach to the MR/CE sector, generally, to explain and reinforce AML/CFT obligations, as well as to enhance industry supervision, is important. Making the general public more aware of the need for AML/CFT measures to be applied to MR/CE services can be equally important however. Such awareness raising may assist in building trust in the regulated system and thus help to foster the use of the system rather than underground or unauthorised means for the movement of funds.

114. ***Guidance and training*** – Since many MR/CE service providers tend to lack the capacity, experience and resources to implement AML/CFT requirements, regulators and/or supervisors have a key role to play in this process by providing adequate guidance to the sector. Given the specific nature MR/CE activity where adequate knowledge of the customer is heavily reliant on effective

identification and record keeping procedures, training on the detection false documentation could be especially useful.

115. ***Licensing / registration systems*** – Countries should clearly designate the regulatory authorities delegated the authority to license and/or register MRs/CEs and to monitor MR/CEs. Due to the particular nature of the services they are providing, it is highly beneficial for the same institution to license or register and supervise them. The institution authorised to issue licenses or registering the MR and CE service providers should have access to public as well as restricted information. Often the information held in databases that have a restricted access (for example, police databases) is of great value. As indicated in the previous section, the advantages of one type of regulatory framework (licensing or registration) over another could not be determined by this study. This issue may be worth exploring further.

116. ***Supervision*** – Given the high vulnerability of MR/CE activity to ML and TF, reinforcing supervision should be considered as essential to prevent and deter the misuse of such businesses. Training should enable the staff of relevant supervisory authorities to assess the quality of internal procedures of MR/CE service providers. It should also enable them to determine whether or not risk management policies and processes are appropriate in relation to the business's profile and whether senior management has adequate risk management policies along with the necessary procedures and controls.

117. ***Fit and proper*** – It is vital to have an appropriate 'fit and proper' system in place to effectively identify the true beneficial owner of a company and to guarantee that MR and CE providers do not operate in an unlawful manner. The 'fit and proper' control should be of a continuous nature to effectively rule out any cases where the company is controlled by criminals. Using a regular registration renewal obligation is one way that this might be implemented.

118. ***Agents*** – There should be ongoing scrutiny and monitoring of agents and sub-agents of MR/CE service providers. Whether this can be achieved by a regulatory requirement on principals to undertake more detailed background checks on their agents, or the inclusion of agents within the requirements should depend on the particular circumstances of the country.

119. ***Reporting systems –*** The detection of ML/TF activity in the MR/CE sector can be improved only if reporting requirements, including the threshold-based reporting systems, are implemented effectively. Given the risk of receiving too many (or too few) STRs from the sector and in order to avoid over-reporting in threshold-based reporting system, automatic or semi-automatic control mechanisms could be integrated into the databases of the authority that collect such information.

120. ***Information sharing*** – The legal framework should clearly define information-sharing responsibilities between the regulatory authorities, law enforcement agencies, and the private sector. Information exchange between the public and private sector is essential for an effective national ML strategy to function.

121. ***At international level –*** Closer cross-border co-operation has sometimes found lacking in this area. MR/CE business activity by its nature often involves persons and activities (as well as currency) from different jurisdictions. MR/CE services are therefore frequently provided by multinational companies. Due to the cross-border aspect of money remittance there is sometimes confusion as to which authority in which country should intervene if suspicious activity is detected. Effective and prompt international co-operation between the law enforcement agencies has proven to be of paramount importance in guaranteeing that such attempts do not remain unpunished. FIU-to-FIU co-operation has proven to be particularly important in this respect, even beyond exchanges on specific STRs.

122. The MR/CE sector provides a service that meets significant and genuine economic needs, and its vulnerability to misuse for money laundering is closely linked to the effectiveness of AML/CFT preventive measures. As with other parts of the financial sector, it may take several years for the AML/CFT regime applicable to money remittance and currency exchange providers to evolve. Moreover, criminal networks often appear able to change their laundering methods more quickly than law enforcement authorities and supervisors can adapt their detection and enforcement capacities. Therefore it is inevitable that it frequently takes time for appropriate legislation to be drafted and agreed upon and still longer for legislation to be tested by the courts and proven to be effective.

123. It clear however that certain measures, if not properly adapted to the specific situation of country, could inadvertently drive the sector further underground, particularly in developing countries where the informal sector is commonly observed. From the regulatory and supervisory perspective, enhancing the level of requirements and controls, while certainly improving the capacity to prevent the misuse of legitimate entities, might in some cases increase the cost of compliance, thus creating greater incentives for marginal businesses to shift to the underground sector, which would then escape from monitoring.

ANNEX 1 – JURISDICTIONS PROVIDING INPUT TO THIS STUDY

Africa		
Egypt *		
Nigeria*		
Americas		
Argentina	Guatemala*	Paraguay*
Belize*	El Salvador*	Peru*
Chile	Honduras*	St Vincent & the Grenadines*
Colombia *	Mexico	United States
Costa Rica *	Panama*	
Asia		
Hong Kong, China	Korea *	Philippines*
India *	Macau, China	Chinese Taipei *
Indonesia *	Malaysia *	Thailand*
Japan		
Europe		
Albania	Greece	Serbia
Armenia	Latvia	Slovakia
Austria	Liechtenstein	Spain
Bulgaria	Lithuania	Sweden
Croatia	Italy	"The former Yugoslav Republic of Macedonia"
Cyprus	Malta	Turkey
Denmark	Moldova	Ukraine
Estonia	Monaco	United Kingdom
Finland	Netherlands	European Commission
France	Poland	
Georgia	Romania	
Germany	San Marino	
Middle East		
Qatar *		
Syria*		
United Arab Emirates *		

* Provided answers to the short version of questionnaire through the Egmont Group.

ANNEX 2 – LIST OF INDICATORS OF POTENTIAL MONEY LAUNDERING ACTIVITY

This section attempts to feature indicators which appear in the selected case studies in this report as well as additional indicators which have been developed in responding jurisdictions to assist anti-money laundering and counter-terrorism financing officers to identify and describe suspicious behaviours for inclusion in suspect transaction or suspicious matter reports. This is a non-exhaustive list. It should also be noted that the single indicators by themselves may not necessarily be linked to money laundering, as some indicators may be typically be found for many money service businesses not facilitating illicit finance.

1. Indicators for all money remitter and currency exchange (MR/CE) service providers

Transactions

- The transaction seems to involve unnecessary complexity.
- Use of front men and/or shell companies.
- Transactions in a series are structured just below the regulatory threshold for due diligence identity checks.
- The customer appears to be trying to avoid reporting requirements by using two or more MR/CE locations or cashiers on the same day to break one transaction into smaller transactions.
- Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions.
- Transactions are carried out by the customer on behalf of third parties without there being an appropriate business relationship with such parties.
- Frequent transaction orders are made by the same client
- Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.
- An unusually large (cash) transaction.
- The amount of the transaction is unusually large for the typical customer or for the MR/CE.
- The transaction has no apparent purpose or no obvious economic/financial basis.
- Unnecessary routing of funds through third parties.
- The customer uses intermediaries which are not subject to adequate AML Laws.
- A customers sends/receives funds to/from him/herself, for no apparent purpose.

- There is no genuine reason for the customer to use the services of an MR/CE business.
- Transfers of large sums of money to or from overseas locations with instructions for payment in cash.
- Customers send or receive (regular) payments from countries which are regarded as "tax havens" or non co-operating.
- One legal/natural person transfers sums to many legal/natural persons.
- One legal/natural person receives sums from many legal/natural persons (from various countries).
- Many legal/natural persons (who have no obvious blood/business relation) are beneficial owners of transfers ordered by one legal/natural person.
- An under-aged person receives funds from many legal/natural persons and/or from different locations.
- A customer sends/receives funds to/from counterparts located in jurisdictions which are known to be exposed to risks of, *i.e.* drug trafficking, terrorism financing, smuggling.
- Non face-to-face customers are not physically present for identification purposes.
- Transactions are accompanied by information which appears clearly false or contradictory.
- The customer is unwilling to provide routine information when requested or the information provided is insufficient, false, or hard for the MR/CE to verify.
- No or limited information about the origin of funds.
- The explanation for the business activity and/or the funds involved is not credible.
- Electronic transfers involving large sums of money does not include data allowing for the clear identification of such transactions.
- Rounded deposits of funds are followed by like-amount wire transfers.
- The customer is accompanied by others who keep a low profile or stay just outside.
- The customer reads from a note he apparently did not write himself.
- The customer receives instructions from others.
- The customer appears to be in doubt when asked for further details.
- Difficulty in obtaining details of the beneficial owners.
- No relationship between sender and beneficiary.
- Operations are irregular.

- The supporting documentation does not add validity to the other information provided by the customer.
- The customer is in a hurry to rush a transaction through, with promises to provide the supporting information later.
- The customer represents a business but seems to have no business experience.
- Authority for others to withdraw funds does not seem to be well-founded.
- Correspondence is to be sent to another person than the customer.
- The customer needs information on what has been deposited in the account before a large cash withdrawal or transfer to abroad.
- Form is filled in advance.
- The pattern of transactions has changed since the business relationship was established.
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings.
- Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.
- Instruction on the form of payment changes suddenly just before the transaction goes through.
- The customer, without a plausible reason, repeatedly goes to agents located far from his/her place of residence or work.
- Funds are sent at a time not associated with salary payments.
- Remittance sent outside migrant remittance corridors.

For cash transactions

- Unusually large cash payments in circumstances where payment would normally be made by cheque, bank draft, etc.
- Cash is in used notes and/or small denominations (possible indication that the money originates from the criminal offence).
- Customer refuses to disclose the source of cash.
- Customer has made an unusual request for collection or delivery.
- Banknotes brought by customer are in small denominations and dirty; stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty are, packaged carelessly and precipitately; when the funds are counted, there is a substantial

difference between the actual amount and the amount indicated by the customer (over or under); detection of counterfeit banknotes in the amount to be transferred or exchanged.

- Depositing funds in cash with further transfer of funds to other person on the same or next day.

Customer profile and behaviour

Customer profile

- Customer's area of residence is inconsistent with other profile details such as employment.
- The size or frequency of the transaction(s) is not consistent with the normal activities of the customer.
- The goods/currencies purchased, and/or the payment arrangements are not consistent with normal practice for the type of business concerned.
- The customer's address is a post office box or a c/o ('in care of') address.
- The customer's address is that of a company service provider (domiciliation service).
- The customer's address information is difficult to verify.
- The postal address for correspondence differs from the customer's official address.
- The stated address does not exist.
- A large number of persons are registered at the stated address, or there are a very large number of changing occupants, or other information is available indicating that it is not the real address of residence or domicile.
- The address of customer's residence does not correspond to the customer's financial arrangements.
- The customer changes address frequently.
- The customer is a business whose name and purpose do not correspond with its transactions.
- The customer cannot immediately provide additional identification documents.
- Identification documents appear to be unused.
- Identification documents are soiled making it difficult to read the necessary information.
- The customer is known to have a criminal past.
- The customer is close to a person who is known to have a criminal past.
- Sudden change in the customer's life style.

- The customer drives very expensive cars that do not correspond to his income situation;
- The customer hires or leases costly assets (*e.g.*, real estate or cars) that do not correspond to his income situation.

Customer behaviour

- The customer is unwilling provide details of his/her identity information and references.
- The customer needs information on what has been deposited in the account before a large cash withdrawal or transfer to abroad.
- Use of false identity documents to send money.
- Customer changes a transaction after learning that he/she must show ID.
- The customer shows no interest in costs or interests.
- The customer does not choose the simplest way to carry out a transaction.
- The customer has no connection with the area where the customer relationship is established.
- Transaction is a price-raising link in a series of transactions with no obvious reasons for the choice.
- The customer gives a rather detailed explanation that appears to be rehearsed concerning the reasons for the customer relationship or the transaction.
- The customer does not respond to letters to the stated address.
- The customer has many newly established companies.
- The customer contracts a loan secured on lodging of equivalent security.
- The customer has companies abroad that are not justified by the customer's business.
- The customer explains that expensive assets are a loan from or financed by a third party.
- The customer uses a payment card from a country which is not his country of residence.

2. Indicators for CE service providers

- Exchange of large quantities of low denomination notes for higher denominations.
- Exchange of large amounts or frequent exchanges that are not related to the customer's business.
- Structuring of large amounts.

- Repeated requests from an exchange office for foreign exchange purchasing-selling transactions in the amounts slightly less than the transaction limit for identification in a short period of time.
- The customer requests currency in large denomination notes.
- The customer buys currency that does not fit with what is known about the customer's destination.
- The customer buys currency from an unusual location in comparison to his/her own location.
- The customer apparently does not know the exact amount being exchanged.
- The customer looks around all the time and does not watch the counting of money.
- The customer is happy with a poor rate.
- Currency purchases with large cash amounts.
- Large exchanges between foreign currencies.
- Frequent exchange of cash into other currencies.
- Exchange of primarily one type of currency.
- The amounts exchanged are significantly higher than usual.
- There is no link between the amount of money exchanged and holiday periods.
- High frequency of currency exchange transactions over a period of time.
- Many currency exchange office used by a same person.
- Requests to exchange large amounts of foreign currency which is not convertible (or not frequently used) another kind of foreign currency.

3. Indicators for MR providers

- Transferring funds without any apparent economic reason.
- Unusual large cash payments in circumstances where payment would normally be made by cheque, banker's draft, etc.
- Transfers of funds without underlying transactions.
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings.
- Transfers paid by large cash amounts in different sums in a short period of time.

- Personal remittances sent to jurisdictions that do not have an apparent family or business link.
- Remittance made outside migrant remittance corridors (*e.g.*, Asian foreign domestic remits funds to South America).
- Personal funds sent at a time not associated with salary payments.
- The customer seems only after the counting to know which amount is being transferred.
- The customer shows no interest in the transfer costs.
- The customer has no relation to the country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there.
- The customer has a note with information about payee but is hesitating if asked whether to mention the purpose of payment.
- Large or repeated transfers between the account of a legal person and a private account, especially if the legal person is not a resident.
- Large amounts are transferred to companies abroad with a service provider address.
- Large or frequent transfers of money.
- Frequent transfer of value that is not related to the customer's business.
- Use of groups of people to send money.
- Use of different money remittance businesses.
- Amounts sent are higher than usual.
- There is not relationship between sender and the beneficial owner.
- The operations are irregular.
- Receiving money from different parts of the world (developed countries) from different people.
- Money is received during short periods of time.
- Money is received from different money remittance companies.
- Money is withdrawn in cash.
- Multiple senders toward a single individual.

Agents

- Reluctance to provide customers' identification to parent MR/CE business.

- Using false identification and fictitious names for customers.
- Frequent transactions or purchase of negotiable instruments under the reporting obligation.
- Each agent work with a different money remitter.
- Make false remittance operations.
- Use false identity documents to send money.
- Make too many operations.
- Not so many people enter into the agent office.
- Sending money to certain countries/cities.
- Amounts sent are higher than usual.
- Large volume of business in large person-to-person transactions.
- Unusual ratio of sent to received transactions (the direction of the flow of the suspicious ratio imbalance being determined by the context).
- High ratio of larger than normal transactions (the complicit operator attracts the larger-transacting criminal customers).
- Seasonal pattern of business that is different from other similar local businesses.
- High percentage of customers that are high dollar or value customers.
- High percentage of high-risk customers.
- High percentage of criminal activity corridor business, where the location is susceptible to involvement in known criminal activity, such as drugs, prostitution, certain fraud, etc..
- High percentage of total dollar business by high-risk customers.
- High volume of large or suspicious transactions in comparison to other MR/CE service providers in the same area.
- Turnover of the MR service provider, after changes in the management structure (with no development of services) exceeds remarkably the flows that were recorded before those changes.
- Conducting transactions before or after business hours.
- Common acceptance of false identification that permits structuring by customers that leave funds in the system for more than the average time before pick-up.
- Multiple transmissions to or receipts from a single customer in a high criminal activity corridor.

- Large volume of transactions for the same customer with multiple instances of using different name spellings, false addresses or identification that "evolves," *i.e.*, some parts of the identification change, while other parts remains the same, such as a person whose last name changes while his first name, date of birth, identification number and address remain the same.

- Transmission of funds by the same customer on the same day to several money transmitter locations to purportedly same or different recipients.

ANNEX 3 – TABLES : QUESTIONNAIRE RESULTS[28]

Table 1 – Overview of MR/CE service providers in jurisdictions contributing to this study

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Albania	X	X	X	X	X	X			
Argentina			X	X		X			
Armenia	0	X	X	X	X	0	0		Although the first field isn't marked, there are money remittance providers in Armenia (post offices, banks and others).
Austria	0	0	0	0	0	0	0	0	These activities may be carried out only by banks.
Bulgaria	X	0	0	X	X	X	0	X	Financial houses
Chile	X	0	X	X	X	X	0		
Chinese Taipei	0	0	0	X	0	0	0	0	
Croatia	X	X	0	X	0	0	0	0	

28 Tables below reflect data and information received from responding countries in 2008.

29 And other anonymous means of payment.

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Cyprus	0	0	0	0	0	0	0	X	Companies (legal persons) specifically licensed by the Central Bank of Cyprus to provide exclusively "money transfer services" (MTS means the operation of a business whose activities consists of the acceptance of money, exclusively for their speedy transfer from and to the Republic of Cyprus by any means)
Denmark	0	0	0	0	0	0	0		
Estonia	X	X	X	X	X	X	X		providers of payment services , money broker service providers
Finland	X	X	X	X	X	X	X	0	
France	X	X	X	X	X	X	X		MR conduct as a business is under the provision of the banking regulation.
Georgia	X	0	0	X	0	0	0	0	
Germany	X	X	0	X	X	X	0	X	
Greece	X	0	0	X	0	X	0	X	Electronic money institutions
Italy	X	0	0	X	0	0	X		*There are no such entities in our jurisdiction. Nevertheless these activities may be carried out by banks and supervised financial institutions.

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Japan	0	0	0	0	0	0	0	0	*As the definition of MR/CEs is not provided in this questionnaire, Japan assumes that MR/CEs are non-banking financial institutions providing money remittance services. In our jurisdiction, money remittance services are provided only by banks based on the Banking Act.
Latvia				X		X		X	Others – banks. Moreover, the Latvian Post is the only national MR provider.
Liechtenstein									There is no separate definition of MR/CEs in Liechtenstein. All services listed below can only be offered by Banks, Bureaux de change, or the Postal Services
Lithuania	0	0	0	0	0	0	0	X	Other – banks. Lithuanian Post provides MR services.
Macau, China	0	0	0	X	0	X	0	-	
Malta	0	X		X	X	X	X		Agents of authorised financial institutions – see point 4 below - such as the Post Office, travel agencies, stationeries, and others as may be authorised in terms of Article 8A of the Financial Institutions Act.
Mexico	X	X	X	X	X	X	0	0	
Moldova	X								
Monaco	0	0	0	0	0	0	0	X	"*Banque Postale"*
Netherlands	0	X	X	X	0	0	0	-	
Nigeria	X	X		X	X	X	X		

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Peru	X	X	X	X	X	X	X		
Poland	X	-	-	X	X	X	0	-	
Romania	X	X	-	X	-	X	-	-	
San Marino	X	0	0	X	0	0	0	0	The activity of MR is performed by banks and post offices, while CE is only performed by banks
Serbia	X	X	X	X	X	X	X	-	
Slovakia	X	0	0	X	X	X	0	0	
Spain	0	0	0	X	0	X	X		
Sweden	X	X	X	X	X	X	X	0	
"The former Yugoslav Republic of Macedonia"	0	X	X	X	X	X	0		
Turkey									Money service businesses are not defined specifically in Turkish legislation. These activities are carried out by banks in Turkey
Ukraine	X	0	X	X	0	X	0		
United Kingdom	0	X	X	X	0	X	0	X	Money Transmitters
United States	x	X	X	X	X	X	X	X	Money transmitters[1] and the United States Postal Service

Table 2 - Overview of the MR/CE service providers in jurisdictions contributing to this study

	Post Offices	Bureaux de change	Banks	Money transaction offices	Travel agencies	Hotels	Other	National MR providers	International MR providers
Albania	x	x	x						
Argentina		x	x						
Armenia	x		x				x		
Austria	x	x	x	x	x				
Bulgaria	x	x	x				Financial houses		
Chile	x	x	x						
Chinese Taipei			x						
Croatia	x		x						
Cyprus			x	x	x				
Denmark			x				miscellaneous shops		
Estonia	x	x	x	x	x				
Finland		x		x	x				
France	x		x						
Georgia	x		x						
Germany	x	x	x	x					
Greece	x	x	x	x					
Hong Kong, China	x	x	x				x		
Italy	x	x	x	**	x	x	Phone centres, internet centres, news agents, stationers		
Japan									
Latvia	x		x	x					
Liechtenstein	x								
Lithuania	x		x						

	Post Offices	Bureaux de change	Banks	Money transaction offices	Travel agencies	Hotels	Other	National MR providers	International MR providers
Macau, China	x		x				x		
Malta	x*	x	x		x*	x*			
Mexico	x	x	x	x	x				
Moldova	x		x						
Monaco							Banque Postale		
Netherlands		x	x	x	x	x	-		
Nigeria	x	x	x		x				
Peru	x		x	x					
Poland	x		x				x		
Romania	x	x	x	x		x	x		
San Marino	x		x						
Serbia			x						
Slovakia	x	x	x	x					
Spain	x		x	x					
Sweden	x	x	x	x	x	x			
"The Former Yugoslav Republic of Macedonia"		x	x	x	x	x			
Turkey	x		x						
Ukraine	x		x	x					
United Kingdom	x		x	x	x		outlets (*e.g.,* restaurants, general stores)		
United States	x	x	x	x	x	x			

* As agents of MR service providers.

Table 3 - Regulatory framework of MR service providers in jurisdictions contributing to this study

Country[30]	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Albania	NA	Central bank	NA
Argentine	NA	NA	NA
Armenia	Yes (licensing)	NA	No
Austria	None since there operate no independent money remittance service providers		
Bulgaria	Yes (licensing)31	Bulgarian National Bank	NA
Chile[32]	Yes (registering)	FIU	NA
Croatia	No		NA
Cyprus	Yes (licensing)	Central Bank	NA
Denmark	Yes (registering)	NA	NA
Estonia	Yes (registering)	Ministry of Economic Affairs and Communications	No
Finland	Yes (registering)	State provincial Office of Southern Finland	NA
France	Yes (licensing)	French Banking Commission	NA
Georgia	Yes (registering)	Georgian Financial Supervisory Authority	NA
Germany	Yes (licensing)	BaFIN (Federal Financial Supervisory Authority)	NA
Greece	Yes	NA	NA
Hong Kong, China	Yes (registering)	FIU	NA
Italy	Yes (registering)	NA	NA
Japan	None since there operate no independent money remittance service providers		
Latvia	No**		NA
Liechtenstein	NA		NA

30 For European Union/ EEA members, please see the explanations provided under Section 1.3 regarding licensing requirements as set out in the EU Directives.

31 During the licensing process, Bulgarian National Bank (BNB) also enters the agents and branches of the money remitter to the register. Agents and branches may not commence operations prior to the registration thereof. BNB shall not register and, respectively, delete from the register any agents and branches of money remittance companies if the BNB determines that the persons who manage and represent the said agents and branches do not possess the required qualifications, professional experience or reliability. A company licensed to operate a money remittance business shall notify the BNB upon the discontinuance of the execution of money remittances by any agent or branch of the said company not later than seven days before the date of discontinuance of the operation.

32 No registration/licensing required at country level.

Country[30]	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Lithuania	None since there operate no independent money remittance service providers		
Macau, China	Yes (registering)	Monetary Authority of Macau	NA
Malta	Yes (licensing)	Malta Financial Services Authority[33]	NA
Mexico	Yes (registering)	*Servicio de Administracion Tributaria* (Tax Administration Service)	No deregistration system
Moldova	None since there are no independent money remittance service providers operating		
Monaco	None since there are no independent money remittance service providers		
Netherlands	Yes (licensing)	NA	NA
Poland	Yes (registering)	NA	NA
Romania	Yes (registering)	National Commerce Register	NA
San Marino	None since there are no independent money remittance service providers		
Serbia	None since there are no independent money remittance service providers		
Slovakia	Yes (licensing)	National Bank of Slovakia	NA
Spain	Yes (licensing)	Central Bank*	NA
Sweden	Yes (registering)	NA	NA
"The former Yugoslav Republic of Macedonia"	NA	NA	NA
Turkey	None since there are no independent money remittance service providers		
Ukraine	Yes (licensing)	State Commission on Regulation of Financial Services Markets	NA
United Kingdom	Yes (registering)	HM Revenue and Customs	NA
United States	Yes (registering)***	FinCEN	Yes (every 2 years)

Remarks:
* In order to get the license from central bank, the positive report from FIU is also mandatory.
In Italy agents of MR service providers must be registered as well, provided that similar integrity and expertise requirements are met.
**The appropriate legislation is at the process of drafting.
*** A business operating as an MSB solely because that business serves as an agent of another MSB is not required to register, but an MSB that engages in activities requiring registration on its own behalf must register even if it is also engaging in activities as an agent for others. See paragraph 10 of main report for explanation of difference between MSB and MR/CE.

33 In Malta the activity of money remittance (as well as currency exchange) or transmission service forms part of a wider category of entities defined as "financial institutions"* that fall under the regulatory and supervisory responsibilities of the Malta Financial Services Authority (MFSA) for prudential purposes.

Table 4 - AML/CTF supervision [34]

Country	Central bank	FIU	Financial Supervisory Authority	Other
Albania	+	+		
Argentina			+	
Armenia	+			
Austria	No independent money remittance service providers			
Bulgaria	+	+		
Chile		+		
Croatia	+			+ (Financial Inspectorate of the Ministry of Finance)
Cyprus	+			
Denmark			+	+ (Danish Commerce and Companies Agency)
Estonia		+		
Finland				+ (The State provincial office of Southern Finland)
France			+	
Georgia			+	
Germany			+	
Greece	+			
Hong Kong, China	No supervision			
Italy	+			+ (*Guardia di Finanza*/Financial Police: on-site inspections, supervision over agents)
Japan	No independent money remittance service providers			
Latvia				+ (Ministry of Transport)
Liechtenstein		+	+	
Lithuania				+ (Financial Crime Investigation Service, Communications Regulatory, both supervise post offices)
Macau, China				+ (Monetary Authority of Macau)
Malta		+	+	
Mexico				+ *Servicio de Administracion Tributaria* (Tax Administration Service)
Moldova	No independent money remittance service providers			
Monaco	No independent money remittance service providers			
Netherlands	+			

[34] Other than banks and postal services.

Country	Central bank	FIU	Financial Supervisory Authority	Other
Poland		+		+ (Ministry of Infrastructure)
Romania		+		
San Marino	No independent money remittance service providers			
Serbia	No independent money remittance service providers			
Spain	+	+		
Sweden			+	
"The former Yugoslav Republic of Macedonia"	+			+ (Ministry of Finance)
Turkey	No independent money remittance service providers			
Ukraine	+			+ (State Commission on Regulation of Financial Services Markets)
United Kingdom				+ (HM Revenue and Customs)
United States				+ (FinCEN, Internal Revenue Service, state local authorities)

Table 5 - Sanctions applied to unlicensed /unregistered MR service providers

Country	Sanction
Albania	Fine or up to 3 years of imprisonment
Argentina	NA
Armenia	Fine or up to 3 years of imprisonment or the deprivation of the right to hold certain positions or practice certain activities for up to 5 years
Austria	Fine up to EUR 50 000.
Bulgaria	Fine up to EUR 5 000
Chile	Fine
Croatia	NA
Cyprus	Fine up to EUR 85 430 or imprisonment up to 2 years
Denmark	Fine
Estonia	Fine up to EEK 500 000 (appr. EUR 31 956)
Finland	Fine
France	Fine up to EUR 75 000 and/or imprisonment up to 3 years
Georgia	NA
Germany	Fine
Hong Kong, China	HK$ 50 000 (appr. EUR 717)
Italy	Up to 4 years of imprisonment
Japan	None since only banks may provide money transfer service
Latvia	Fine
Liechtenstein	Fine or imprisonment up to 1 year
Lithuania	Public works fine or imprisonment up to 4 years
Macau, China	Fine up to MOP 5 000 000 (appr.EUR 451 891)
Malta	Fine up to EUR 465 875 and/or imprisonment up to 1 year
Mexico	Fine
Moldova	There operate no independent money remittance service providers
Monaco	NA
Netherlands	Fine
Poland	None since only banks and Polish Post may provide money transfer service
Romania	NA
San Marino	Second-degree imprisonment (6 month to 3 years) and a fine as well as by third-degree disqualification from holding the offices of director holder of representative powers internal auditor external auditor actuary liquidator or commissioner in companies or other bodies with legal personality
Serbia	NA
Slovakia	Fine up to EUR 333 333 or imprisonment

Country	Sanction
Spain	Fine
Sweden	NA
"The former Yugoslav Republic of Macedonia"	NA
Turkey	Fine (up to 5 000 days salary) or imprisonment up to 5 years
Ukraine	NA
United Kingdom	Fine (unlimited) or imprisonment
United States	Sanctions vary by state. At the federal level: fine up to $ 5 000 (appr. EUR 3 476) per day and/or imprisonment for up to 5 years. There are several civil and criminal penalties for violations of the Bank Secrecy Act as well.

Table 6 - Threshold for identifying the customer

Country[35]	Threshold (CE)	Threshold (MR)
Albania	EUR 12 000	EUR 12 000
Argentina	obligatory	obligatory
Armenia	appr. USD 1300	appr. USD 1300
Austria	EUR 15 000	No threshold mandatory
Bulgaria	BGN 10 000 (appr. EUR 5 000)	BGN 10 000 (appr. EUR 5 000)
Chile	USD 5 000	USD 5 000
Croatia	HRK 105 000 (appr. EUR 15 000)	EUR 1 000
Cyprus		No threshold mandatory
Denmark	EUR 1 000	EUR 1 000
Estonia	EEK 100 000 (appr. EUR 6 400)	No threshold mandatory
Finland	EUR 15 000	EUR 15 000
France	EUR 8 000	No threshold mandatory
Georgia	GEL 3 000 (appr. EUR 1 400)	GEL 1 500 (appr. EUR 700)
Germany	EUR 2 50036	No threshold mandatory
Greece	EUR 15 000	EUR 1 000
Hong Kong, China	HK USD 8 000	HK USD 8 000
Italy	EUR 15 000	No threshold mandatory
Japan	YEN 2 000 000 (appr. EUR 15 566)	YEN 100 000 (appr. EUR 700)
Latvia	LVL 5 000 (appr. EUR 7 117)	EUR 1 000
Liechtenstein	CHF 5 000 (appr. EUR 3 271)	CHF 5 000 (appr. EUR 3 271)
Lithuania	EUR 6 000	EUR 600 (for local or cross-border post remittances) EUR 1 000 (for banks according to EU Regul No 1781/2006)
Macau, China	General rule: MOP 20 000 (appr. EUR 1 740) MOP 8 000 (appr. EUR 695) for wire transfers	No threshold for cash remittances MOP 8 000 (appr. EUR 695) for wire transfers
Malta	EUR 15 00037	EUR 1 000
Mexico	USD 3 000 (appr. EUR 2 086)38	USD 3 000 (appr. EUR 2 086)

35 In EU/EEA countries, there is a difference on the identification of customers depending on whether the money remittance provider is a bank (with the customer holding an account) or not.

36 If the transaction is carried out through an account other than the customer's account.

37 For one-off transactions. Customer identification is not subject to a threshold in the course of establishing a permanent business relationship.

38 *For Centros Cambiarios.*

Country[35]	Threshold (CE)	Threshold (MR)
Moldova	MDL 50 000 (appr. EUR 3 500)	MDL 50 000 (appr. EUR 3 500) for cash transfers and MDL 15 000 (appr. EUR 1 000) for electronic and wire transfers
Monaco	No threshold mandatory	No threshold mandatory
Netherlands	No threshold mandatory	No threshold mandatory
Poland	EUR 15 000	EUR 1 000
Romania	No threshold mandatory	No threshold mandatory
San Marino	EUR 15 000	EUR 15 000
Serbia	EUR 15 000	EUR 15 000
Slovakia	EUR 1 000	EUR 2 000
Spain	No threshold mandatory	No threshold mandatory
Sweden	EUR 15 000	EUR 1 000
"The former Yugoslav Republic of Macedonia"	EUR 2 500	EUR 2 500
Turkey	TRY 2 000 (appr. EUR 948) for wire transfers; TRY 20 000 (appr. EUR 9480) for cash transactions[39]	Mandatory when establishing the business relationships; TRY 2 000 (appr. EUR 948) for wire transfers; TRY 20 000 (appr. EUR 9480) for cash transactions
Ukraine	No threshold[40]	UAH 5 000 (appr. EUR 434)
United Kingdom	EUR 15 000	No threshold mandatory
United States	USD 1 000 (appr. EUR 696)	USD 3 000 (appr. EUR 2086)

39 Mandatory when *establishing* the business relationships.

40 Except for banks that may not identify their customers if the financial transaction is conducted to the amount of UAH 50 000 (USD 6 250) without *opening* an account.

Table 7- Regulatory framework for CE service providers in contributing jurisdictions

Country	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Albania	Yes (licensing)	Central Bank	NA
Argentine	Yes (licensing)	Central Bank	NA
Armenia	Yes (licensing)	NA	No
Austria	Not applicable as only banks provide money exchange		
Bulgaria	Yes (registering)	National Revenue Agency	NA
Chile[41]	Yes (registering)	FIU	NA
Croatia	Yes (licensing)	Central Bank	NA
Cyprus	Not applicable as only banks provide money exchange		
Denmark	Yes (registering)	Danish Commerce and Companies Agency	NA
Estonia	Yes (registering)	Ministry of Economic Affairs and Communications	NA
Finland	Legal requirement for licensing/registration in place but not yet implemented		
France	Yes (registering)	Central Bank	NA
Georgia	Yes (registering)	Georgian Financial Supervisory Authority	NA
Germany	Yes (licensing)	NA	NA
Greece	Yes	Bank of Greece	NA
Hong Kong, China	Yes (registering)	FIU	NA
Italy	Yes (registering)	Central Bank	NA
Japan	No		NA
Latvia	Yes (licensing)	Central Bank	NA
Liechtenstein	Not applicable as only banks provide money exchange		
Lithuania	Yes (licensing)	Central Bank	NA
Macau, China	Yes (registering)	Monetary Authority of Macau	NA
Malta	Yes (licensing)	Malta Financial Services Authority	NA
Mexico	Yes (licensing) Yes (registering)	Ministry of Finance and Public Credit Tax Administration Service	NA

41 No registration/*licensing* required at country level.

Country	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Moldova	Yes (licensing)	National Bank	Yes, every 5 years
Monaco	Yes (registering)	Directorate of Economic Development	NA
Netherlands	Yes (licensing)	NA	NA
Poland	Yes (registering)	Central Bank	NA
Romania	Yes (registering)	Central Bank	NA
San Marino	Not applicable as only banks provide money exchange		
Serbia	Yes (licensing)	Central Bank	NA
Slovakia	Yes (licensing)	National Bank of Slovakia	NA
Spain	Yes (licensing)	Central Bank (+positive report from FIU)	NA
Sweden	Yes (registering)	NA	NA
"The former Yugoslav Republic of Macedonia"	Yes (licensing)	Central Bank	NA
Turkey	Yes (registering)	Undersecretariat of Treasury	NA
Ukraine	Yes (licensing)	Central Bank	NA
United Kingdom	Yes (registering)	HM Revenue and Customs	NA
United States	Yes (registering)	FinCEN	Yes (every 2 years)

Table 8 - Number of referrals, prosecutions and convictions based on STRs received from MR/CE sector (2006-2008)

	2006			2007			2008		
	Number of Referrals	Number of Prosecutions	Number of Convictions	Number of Referrals	Number of Prosecutions	Number of Convictions	Number of Referrals	Number of Prosecutions	Number of Convictions
Bulgaria	12	0	0	26	0	0	32	1	0
Chile	2			1			5		
Croatia	NA			12			11		
Estonia				10	0	0	49	0	0
Finland	1 069			1 293			445		
France	27	6		32	1		26		
Germany									
Greece	1			1			1		
Hong Kong, China	51	0	0	26	0	0	55	0	0
Latvia[42]	155*	25**	0***	146*	62**	3***	151*	29**	10***
Liechtenstein	1	0	0	0	0	0	1	0	0
Lithuania	2		0	2		0	5		0
Macau, China				1					
Malta	5	-	-	5	1	-	6	-	1
Moldova	12	2	0	18	3	0	29	0	0
Monaco							2	2	

[42] * Referrals are based on all received reports, not only on received from MSB sector.

** Only prosecutions sent to court in that year.

*** For convictions the number is for cases where ML is the main accusation.

	2006			2007			2008		
	Number of Referrals	Number of Prosecutions	Number of Convictions	Number of Referrals	Number of Prosecutions	Number of Convictions	Number of Referrals	Number of Prosecutions	Number of Convictions
Netherlands[43]	28 894	320	275	40 893	515	427			
Nigeria	2	1	1	1	1	0	1	1	0
Peru				4			18		
Poland[44]	5 (20)*	3 (12)	1 (2)	5 (24)	5 (21)	1	5 (59)	5 (48)	
Slovakia	2			2			2		
Spain	169			196					
Ukraine	446	163	1	520	242	25	641	326	76
United States		87			115				

43 *Note*: the authorities indicated that they could not establish that any single one of these prosecutions and convictions was based on an STR related to a MSB.

44 Data in parentheses encompass also reports to the public prosecutor which concern cases of money laundering connected with schemes ending transactions of money remittance (especially laundering of money stemming from unauthorised access to the bank accounts -"phishing attacks").

REFERENCES AND BIBLIOGRAPHY

Financial Action Task Force and FATF style regional bodies reports

FATF (2003) *Report on Money laundering and terrorist financing typologies - 2002-2003*, FATF, Paris

FATF (2005), *Money Laundering and Terrorist Financing Typologies 2004-2005*, FATF, Paris

FATF (2006), *Report on New Payment Methods*, FATF, Paris

FATF (2008a), *Terrorist Financing*, FATF, Paris

FATF (2008b), *Money Laundering and Terrorist Financing Risk Assessment Strategies*, FATF, Paris

FATF (2008c) *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems*, FATF, Paris

FATF(2009), *Risk-Based Approach – Guidance for Money Service Businesses*, FATF, Paris

MENAFATF (2005), *Best Practices Concerning Hawala*, MENAFATF, Kingdom of Bahrain, www.menafatf.org/Linkcounter.asp?rid=646&attached=best practices on Hawala.pdf (accessed September 2011),

Regulatory guidance and reports

CTIF-CFI (2003), *10th Annual Report 2002-2003*, (Dutch and French versions), CTIF-CFI, Brussels

FinCEN (2009) [United States], *Notice of Proposed Rulemaking – Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, Financial Crimes Enforcement Network, United States.

HM Treasury (2006) [United Kingdom], *The Regulation of Money Service Business: A Consultation*, HM Treasury, United Kingdom

International Monetary Fund (2005), *Regulatory Frameworks for Hawala and Other Remittance Systems*, International Monetary Fund, United States

International Monetary Fund (2005), *Approaches to Regulatory Framework for Formal and Informal Remittance Systems: Experiences and Lessons*, International Monetary Fund, United States

Madinger, J. (2006), *Money Laundering. A Guide for Criminal Investigators*, 2nd edition, CRC Press.

SOCA (2009) [United Kingdom], *The United Kingdom Threat Assessment of Organised Crime*, SOCA, United Kingdom

US Department of Justice, National Drug Intelligence Center (2006). *Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*, October 2006, US Department of Justice

US Department of the Treasury (2007) [United States], *Money Laundering Strategy 2007*, US Department of the Treasury

US Department of the Treasury (2005), *United States Money Laundering Threat Assessment*, December 2005, US Department of the Treasury

Articles and papers

Carroll, L. C. (2007), *Alternative Remittance Systems distinguishing sub-systems of Ethnic Money Laundering in INTERPOL Member Countries on the Asian Continent*. Interpol, 2007.

Chene, M. (2008), *Hawala Remittance System and Money Laundering. U4 Expert Answer*, Anti-Corruption Resource Centre, Norway, 2008.

Choo, K-K. R. (2008), *Money Laundering Risks of Prepaid Stored Value Cards*. Australian Government, Australian Institute of Criminology, Sept 2008.

Jost, P. M., H. S. Sandhu (2000), *The Hawala Alternative Remittance System and its Role in Money Laundering*. Interpol, Jan 2000.

KPMG (2005), *2005 Money Services Business Industry Survey Study*. KPMG, 2005

Sienkiewicz, S. (2007), *Prepaid Cards: Vulnerable to Money Laundering?* Payment Cards Center, Federal Reserve Bank of Philadelphia, Discussion Paper, Feb 2007.

GLOSSARY OF TERMS

Agent — any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). (*This definition is drawn from the Interpretative note to the FATF Special Recommendation VI*).

Alternative remittance systems (ARS) — Any system used for transferring money from one location to another that operates in part or exclusively outside conventional banking channels.

Beneficiary — The person who receives transferred funds.

Beneficial owner — The natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Cheque casher — A person that accepts cheques or monetary instruments in return for currency or a combination of currency and other monetary instruments or other instruments.

Currency — Banknotes and coins that are in circulation as a medium of exchange

Currency exchange (CE) — Activity that involves accepting currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries.

Financial institutions — *Financial institutions*[45] means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[46]
2. Lending.[47]
3. Financial leasing.[48]

---

45 For the purposes of Special Recommendation VII, it is important to note that the term *financial institution* does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.

46 This also captures private banking.

47 This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

48 This does not extend to financial leasing arrangements in relation to consumer products.

4. The transfer of money or value.[49]
5. Issuing and managing means of payment (*e.g.*, credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:

   (a) money market instruments (cheques, bills, CDs, derivatives etc.);

   (b) foreign exchange;

   (c) exchange, interest rate and index instruments;

   (d) transferable securities;

   (e) commodity futures trading.

Participation in securities issues and the provision of financial services related to such issues.

Individual and collective portfolio management.

Safekeeping and administration of cash or liquid securities on behalf of other persons.

Otherwise investing, administering or managing funds or money on behalf of other persons.

12. Underwriting and placement of life insurance and other investment related insurance[50].
13. Money and currency changing.

(Source: FATF)

Funds transfer

Series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order.

Hawala

A specific form of an alternative remittance system.

Informal value transfer system (IVTS)

Any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. Informal value transfers generally take place outside of the conventional banking system through non-bank financial institutions or other business entities whose primary business activity may not be the transmission of money.

---

49 This applies to financial activity in both the formal or informal sector *e.g.*, alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

50 This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Issuer, seller, or redeemer of stored value	A person that issues stored value or sells or redeems stored value.
Money remittance (MR)	Activity that involves accepting currency, or funds denominated in currency, or other value that substitutes for currency from one person and transmission of the currency or funds, or the value of the currency or funds to another location or person, by any means through a financial agency or institution, or an electronic funds transfer network. Often postal service providers fall into this category if they provide fund transfer services.
Money service business	According to the generally accepted definition, *money service businesses* (MSBs) are non-bank[51] financial institutions that provide certain types of financial services. Although the precise scope of the activities that fall into category "money service" vary from country to country (for example, the requirements for MSBs may only apply if the value of individual transactions and/or its turnover exceeds a certain value limit.[52] They may also only apply to businesses that carry out the specified activities on regular basis or as an organised business concern, etc). Typically, the following types of financial activities are carried out by MSBs: • Currency dealing or exchange. • Cheque cashing. • Issuance of traveller's cheques, money orders or stored value. • Selling or redeeming of traveller's cheques, money orders, or stored value • Money transmitting.
Originator/ transmitter	The sender of the payment order in a funds transfer.
Stored value	Funds or monetary value represented in digital electronics format (whether or not specially encrypted) and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically.

51 According to the US financial intelligence unit (FinCEN), the definition *money services business* does not include financial institutions, nor does it include persons registered with, and regulated or examined by, the Securities and Exchange Commission or the Commodity Futures Trading Commission.

52 For example, in US rules applicable to MSBs apply to those currency dealers/exchangers, cheque cashers, issuers of traveler's cheques, money orders or stored value who exchange currency or issue/sell/redeem cash cheques/money orders/stored value in an amount greater than USD 1 000 in currency or monetary or other instruments for any person on any day in one or more transactions.

MONEYVAL and FATF/OECD
July 2010

www.fatf-gafi.org

Appendix FF:

FATF, *FATF Report: Money Laundering and Terrorist Financing in the Securities Sector* (Paris: FATF, 2009)

FATF • GAFI
Financial Action Task Force Groupe d'action financière

FATF Report

Money Laundering and Terrorist Financing in the Securities Sector

October 2009

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. The securities industry plays a key role in the global economy. Participants range from multinational financial conglomerates that employ tens of thousands of people to single-person offices offering stock brokerage or financial advisory services.

2. New products and services are developed constantly, in reaction to investor demand, market conditions, and advances in technology. Product offerings are vast, and many are complex, with some devised for sale to the general public and others tailored to the needs of a single purchaser. Many transactions are effected electronically and across international borders.

3. Some of the features that have long characterised the industry, including its speed in executing transactions, its global reach, and its adaptability, can make it attractive to those who would abuse it for illicit purposes, including money laundering and terrorist financing. Moreover, the securities sector is perhaps unique among industries in that it can be used both to launder illicit funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Transactions and techniques associated with money laundering and the specific predicate securities offences are often difficult to distinguish, which is why specific indicators and case studies for insider trading, market manipulation and securities fraud are relevant and included in this study.

4. The case studies presented in this report illustrate the risks associated with the various types of intermediaries, products, payment methods and clients involved in the securities industry. Unlike other sectors, the risks lie mainly not in respect of the placement stage of money laundering, but rather in the layering and integration stages. Typical securities-related laundering schemes often involve a series of transactions that do not match the investor's profile and do not appear designed to provide a return on investment.

5. Some areas of vulnerability (for example, rogue employees) are not peculiar to the securities industry, and thus this study is of relevance to the wider financial services sector. In particular, some money laundering schemes involve products and transaction types that exist in the banking and insurance sectors as well.

6. Suspicious transaction reporting in the sector remains relatively low, which can be explained by a number of possible factors, including a lack of awareness and insufficient securities-specific indicators and case studies; issues that this report attempts to address. Consultations with the private sector conducted for this project outlined the need for enhanced securities-specific guidance by international organisations and national authorities.

7. The reported incidents of money laundering in the securities industry far outweigh those relating to terrorist financing. However, the sector remains vulnerable to both money laundering and terrorist financing.

CHAPTER 1: INTRODUCTION

1.1 Introduction

1. The securities industry, along with banking and insurance, is one of the core industries through which persons and entities can access the financial system. This access provides opportunities for criminals to misuse the financial system to engage in money laundering (ML) and terrorist financing (TF).

2. Whilst the securities industry has been the subject of international and domestic efforts relating to anti-money laundering (AML) and combating the financing of terrorism (CFT) for several years, ML/TF vulnerabilities specific to this industry have not been subject to global typology research.

1.2 Need for the Typology

3. The securities industry evolves rapidly and is global in nature. It provides opportunities to quickly carry out transactions across borders with a relative degree of anonymity. It is thus imperative to highlight and share current information about potential vulnerabilities.

4. The report previously published by the FATF in 2003[1] on the securities industry provided a relatively limited overview of ML/TF vulnerabilities due to the limited availability of securities typologies. In addition, MONEYVAL and the Asia/Pacific Group (APG) on money laundering, both FATF-Style Regional Bodies (FSRBs), have carried out work in this area. MONEYVAL published a securities typology report in 2008 and the APG incorporated a section on securities into its 2009 yearly typologies report. Both reports are limited in scope to those FSRBs' regional jurisdictions.

5. The FATF decided to conduct a global study in June 2008 in order to better understand the ML/TF vulnerabilities in the securities industry. It is anticipated that this study will be of benefit to the industry, law enforcement and regulators.

6. The need for this latest typology report is also driven by the comparatively low levels of suspicious transaction reporting in the securities industry relative to other industries, such as banking. The reason for lower levels of reporting is not entirely clear, but some possible explanations are explored later in the report.

7. The variation in the securities industry particular to different jurisdictions also contributes to the need for a global typology that addresses these variations. For example, jurisdictions differ in the types of products that they define as securities, as reflected in the numerous types of securities products mentioned in the current FATF Glossary definition linked to the activities of "financial institutions."

8. Moreover, while securities intermediaries in many jurisdictions do not accept cash for securities transactions, which is traditionally used in the placement stage of ML and where potential ML/TF activities may be easier to detect and report, some do. Finally, depending on the jurisdiction, trading in securities is often not limited to securities broker-dealers, but can also involve the banking and insurance industries.

---

1 FATF (2003).

9. The following countries and international organisations joined the project team and contributed to the study: Australia, Belgium, Brazil, Canada (as project co-leader), France, Japan, Luxembourg, the Netherlands, Spain, Switzerland, the United Kingdom (U.K.) (as project co-leader), the United States (U.S.) (as project co-leader), the Asian Development Bank, the Offshore Group of Banking Supervisors ("OGBS"), the International Organisation of Securities Commissions ("IOSCO") and the World Bank. In total, over 40 countries and international organisations participated in the study.

1.3 Scope

10. The objectives of this typology report are to:

- Raise overall awareness of the ML/TF risk in the securities industry for industry participants, regulators and law enforcement;
- Identify specific ML/TF risks based on product type, intermediary, market type and payment/distribution channel;
- Provide a comprehensive set of suspicious indicators and case studies that are applicable to the securities industry; and
- Identify any current and emerging issues which would benefit from further consideration by the FATF.

11. This project examines ML/TF vulnerabilities in the securities industry based on typical products, markets, payment methods and intermediaries associated with the industry. Where practicable, the report seeks to identify the particular vulnerabilities, whether at the placement, layering or integration phase, associated with a particular product, market, payment method or intermediary. Where possible, particularly in the case studies, the report identifies the source of funds used in money laundering and any predicate offence used to generate the funds.

12. Importantly, this report highlights several situations that are of particular relevance or are unique to the securities industry.

13. For example, while money laundering generally encompasses the *introduction* of illicit assets into the financial system, securities can also be a vehicle for *generating* illicit assets within the financial system itself. The FATF glossary includes among the "designated categories of offences", three offences that are predicate offences to money laundering: insider trading, market manipulation, and fraud. Insider trading and market manipulation are particular to the securities industry, as is securities-related fraud.[2] Because these illicit activities are particular to the securities industry, they are addressed in this report in the hope that ML/TF can be reduced when these activities are themselves detected and prevented.

14. Also, the relatively detailed customer information many securities intermediaries collect as part of other regulatory obligations, such as suitability or know-your-customer (KYC), may allow for particular insights into potential ML/TF activities.

15. Although the focus of this report is on the unwilling use of the securities industry in ML schemes, typologies have demonstrated that, at times, securities industry professionals can also be complicit in

[2] Whilst insider trading and market manipulation can also occur in the commodities industry, in at least some jurisdictions commodities trading is included under the securities regulatory regime.

perpetuating ML schemes and securities-specific predicate offences. Accordingly, this report will address both phenomena.

16. Finally, although the report's primary focus is on issues particular to the securities industry, it is worth noting that a number of the vulnerabilities and suspicious indicators identified in this report overlap with those that occur in other financial services sectors, such as banking. Moreover, whilst the report is intended to be a comparative survey, it is not an exhaustive overview of all aspects of this wide-ranging industry.

1.4 Methodology

17. This report is based on four main sources. The first is a review of literature and related guidance that has been produced or undertaken by international groups, domestic regulators, trade associations, self-regulatory organisations (SROs)[3] and academia. The second is a compilation and analysis of the responses to a questionnaire that the project co-leaders distributed to FATF members and observers in November 2008. The third and fourth are the results of a typology workshop and consultations with the private sector, respectively.

18. The questionnaire results were obtained in December 2008 and January 2009 from 38 jurisdictions in the Americas, Asia, Australia, Europe, the Middle East, and two international organisations, giving a total of 40 respondents. [4] The responding jurisdictions varied in the size and organisation of their securities markets. These variations were taken into account to the extent practicable.

19. In November 2008, at about the same time that the questionnaire was distributed, a workshop on money laundering and the securities industry was held in Monaco as part of the 2008 FATF/MONEYVAL Typologies meeting. This workshop was very well supported by members of the FATF, MONEYVAL, and representatives of several international organisations. The following participants examined the issue in depth during a break out session: Australia, Belgium, Brazil, Canada, the European Commission, Finland, France, Germany, Luxembourg, the Netherlands, Norway, Russia, Switzerland, the U.K., the Ukraine, the U.S., the APG Secretariat, IOSCO, the MONEYVAL Secretariat and the Organisation for Economic Co-operation and Development ("OECD").

20. This study is also based on consultations with non-governmental persons, including the Investment Industry Regulatory Organization of Canada ("IIROC"), representatives of the private sector in the U.K. and U.S., and the Financial Industry Regulatory Authority, Inc. ("FINRA"), a U.S. SRO, and representatives of the private sector in some core group countries.

21. The project team would like to acknowledge the thoughtful work of all participants, including the FATF Secretariat. Their input has been greatly appreciated.

[3] An SRO is a non-governmental organisation that has the power to issue and enforce industry regulations and standards.

[4] The questionnaire and a list of the countries and jurisdictions that responded to it are attached as Annex D.

CHAPTER 2:
LITERATURE AND ACTIVITIES REVIEW

2.1 Overview

22. Information on ML/TF typologies, trends and techniques in the securities industry can be found in various sources. As previously mentioned, both the FATF and some FSRBs have conducted typologies in the past. In addition, financial intelligence units (FIUs), law enforcement and other agencies publish suspicious transaction indicators, trends and sanitised ML/TF cases. Significant materials have also been produced by international groups, domestic regulators, trade associations, SROs, and academics. A review of this material is provided below.

2.2 Previous Typologies Exercises

2002-03 FATF Typologies Report

23. In February 2003, the FATF published a general report on ML typologies (FATF Typology).[5] That report contained four chapters, including one devoted to ML through the securities industry. Other chapters of the 2002-03 FATF typology addressed terrorist financing, the gold and diamond markets, and other ML/TF trends.

24. The securities chapter in the FATF Typology made the following overall observations:

- The ability of the FATF to examine ML vulnerabilities in the securities industry was hampered by the lack of information regarding how, or indeed whether, the securities industry was being used for ML;
- ML in the securities industry occurs primarily at the layering and integration stages; and
- The securities industry provides the money launderer with a double advantage – the ability to launder illicit assets generated from outside the securities industry and the ability to use these external illicit assets to generate additional illicit assets within the securities industry, for example through market manipulation and securities fraud.

25. The FATF Typology also provided eight examples of the different stages through which the securities industry can be used for ML/TF, and illustrated the illicit activities that can generate illicit assets from within the industry.

26. The FATF Typology, however, did not provide a comprehensive set of suspicious indicators that compliance professionals in the securities industry could use when evaluating the particular risks that a client or series of transactions could pose. This may have been the result of the lack of information about how or whether the securities industry was actually being used for ML/TF purposes.

5 FATF (2003).

2008 MONEYVAL Typologies Report (MONEYVAL Typology)[6]

27. The MONEYVAL securities typology report focuses on countries predominantly in Eastern Europe that, in some cases, have a developing securities industry.

28. The MONEYVAL typology identified the following areas as presenting the greatest ML vulnerabilities in the securities industry:

- Wholesale markets;
- Unregulated funds;
- Wealth management;
- Investment funds;
- Bearer securities; and
- Bills of exchange.

29. MONEYVAL acknowledged that, in rare instances, cash can be placed through the securities industry. Significantly, MONEYVAL devoted a section of its report to market manipulation and insider trading, providing a number of case studies to illustrate these illicit activities.

30. The MONEYVAL typology presented a number of sanitised case studies as well as schematics to illustrate the flow of funds and the relationships between persons and entities. The MONEYVAL report also addressed suspicious indicators at the account opening stage, the execution and settlement of transactions, and the use of fictitious companies.

31. The MONEYVAL typology also described how information is shared amongst and between financial regulators, FIUs and law enforcement. In particular, MONEYVAL identified information sharing as an important issue given that certain securities transactions are effected in different sectors and may be subject to different regulatory oversight. The report provided guidance on analysis and investigation techniques as well as information on how the FIUs of specific countries perform their analysis and how cases are investigated by law enforcement.

APG Typology Workshop and 2009 Report[7]

32. In October 2008, the APG held a typologies workshop during which several member countries provided presentations. A portion of the workshop featured the securities industry and was attended by several securities regulators. The cases and suspicious indicators included in those presentations focused more on predicate offences to money laundering, such as securities fraud, than on money laundering itself. This may be because fewer APG countries require the securities industry to report suspicious transactions. Where such requirements exist, securities related suspicious transaction reporting (STR) reporting levels are low, potentially impeding the ability of these jurisdictions to investigate money laundering. In any event, the overall experience of some APG countries is that the securities industry is a method of generating illicit assets instead of a conduit for laundering illicit assets generated outside of the industry.

6 MONEYVAL (2008)

7 APG (2009)

33. Instances where ML was detected and reported were mostly at the placement stage because many APG countries still utilise cash as a payment method for securities transactions. For example, some APG country ML case studies focused on the laundering of proceeds of corruption through investments in the capital markets. As with the other typologies mentioned, the APG typology report did not present case studies where the securities industry was used for terrorist financing.

34. As reported by APG member countries, the following were the most common suspicious indicators and methods related to money laundering and predicate offences involving the securities industry:

- Changing share ownership in order to transfer wealth across borders;
- Redeeming a long-term investment within a short period;
- Opening multiple accounts or nominee accounts;
- Using brokerage accounts as long term depository accounts for funds;
- Effecting transactions involving nominees or third parties;
- Engaging in market manipulation, e.g. "pump & dump" schemes; and
- Engaging in boiler room operations.

35. There appeared to be a consensus that APG countries need to better understand the ML/TF risks and vulnerabilities of the securities industry. It was noted that although APG mutual evaluation reports have some useful information on the sector, they do not address securities related ML/TF risks in a significant manner.

2.3 International Activities and Materials

International Guidance and Best Practices

36. A number of guidance documents issued by international organisations and/or domestic authorities provide useful information on ML/TF vulnerabilities in the securities industry.[8] International organisations, such as IOSCO, the Basel Committee on Banking Supervision and the International Association of Insurance Supervisors have produced documents that set out standards and best practices that national regulators and supervisors as well as banks, securities firms and insurance companies should follow.

37. Vulnerabilities identified by these organisations requiring enhanced due diligence or a particular focus on supervision are listed below:

- Transactions involving accounts in multiple jurisdictions;
- Securities accounts introduced from one intermediary to another without adequate customer due diligence/know your customer (CDD/KYC) investigations or from high risk jurisdictions;
- The use of front persons or entities (e.g. corporations, trusts);

[8] These documents are listed in the references and bibliography section.

- Entities with complex corporate structures;
- Politically-exposed persons (PEPs);
- Dealings with financial institutions and intermediaries or customers operating in jurisdictions with ineffective AML/CFT systems;
- Unregistered or unregulated investment vehicles;
- Cross-border omnibus and correspondent accounts; and
- Fictitious trading schemes.

38. Additional areas that are identified as low risk (and where reduced due diligence can, in some jurisdictions, be acceptable) also provide useful information on ML/TF vulnerabilities. These are generally products or accounts with restrictions, such as where:

- Cash withdrawals are not permitted;
- Redemption or withdrawal proceeds are not permitted to be paid to a third party; or
- It is not possible to change the characteristics of products or accounts at a future date to enable payments to be received from, or made to, third parties.

2.4 Domestic Material

Published Law Enforcement Cases

39. Some jurisdictions publish sanitised ML or other financial crime cases. Generally, these cases are published as part of an FIU's annual report, or as specific-topic trends or as typologies reports, and provide insights into ML or TF trends and methods, including statistics and other information. Such information is extracted from STRs and other reports, as well as investigations and other enforcement actions. These sources provide essential guidance to financial institutions and can be used by regulators and other government agencies to help develop their supervisory programmes, as well as in the assessment of AML/CFT system effectiveness.

40. Although the Egmont Group also posts sanitised cases on its website, they contain relatively few references to securities.[9]

Regulatory Guidance and Reports

41. Domestic regulators, FIUs and/or SROs produce guidance to assist their financial institutions and intermediaries in meeting their AML/CFT obligations. Some countries provide industry-specific guidance, including the securities industry, while other jurisdictions provide guidance that is applicable to financial institutions more generally. Guidance in respect of customer due diligence and risk assessment is intended to provide an indication of the types of transactions, customers and delivery channels that present higher ML/TF risks.

[9] The Egmont Group, www.egmontgroup.org/library_sanitized_cases.html

42. This regulatory guidance can involve, for example, a discussion of enhanced due diligence measures that are often recommended for specific types of products/customers, such as:

- Offshore trusts;
- Non-profit or charitable organisations;
- Significant cross-border activity;
- Internet/on-line accounts; and
- Omnibus and private banking accounts.

43. Other guidance appears in the form of published suspicious transaction indicators. These indicators are often developed and published by FIUs and can be industry-specific or apply generally to all financial institutions and designated non-financial businesses and professions (DNFBPs). Some FIUs present the indicators in the context of specific cases that they have built and analysed. Each indicator individually is not an automatic trigger for reporting, but rather serves as a tool for determining whether a suspicious transaction report (STR) should be filed. A comprehensive list of such indicators has been compiled using responses to the project questionnaire, published sources, and consultation with the private sector, and is available in Annex B.

Articles and Papers

44. Specialised periodicals in the area of law, crime or finance publish research or analytical papers on topics related to money laundering written by regulators, law enforcement representatives, academics and members of the private sector. Even among such sources, little is found concerning securities. A few papers discuss the vulnerabilities of the securities industry, in particular at the layering stage, and provide indicators, cases, and discuss implications for regulators and broker-dealers.[10]

2.5 Main Gaps in Existing Material

45. In comparison to several other sectors and financial products, there is significantly less documentation on the ML risks and vulnerabilities related to the securities industry. In many jurisdictions, the literature on TF is less still.

46. By contrast, there is much more abundant information on predicate crimes committed using securities, such as market manipulation and insider trading, in particular with respect to investigations, prosecutions and convictions. The possible connections between predicate offences and money laundering in the securities industry will be examined in this report.

47. As noted above, a number of sanitised cases involving securities have been published, some of which provide detailed information on persons and entities involved and on the flows of funds. However, published cases rarely include information on the suspicious indicators or circumstances that led, or should have led, to the filing of an STR. In some cases, this limited information may be the result of the disclosure restrictions applicable to the STR filing itself. Also absent is information on any enforcement actions, e.g. prosecution or seizures, in respect of the specific case.

[10] A list of articles and papers is provided in the references and bibliography section.

CHAPTER 3:
ML/TF VULNERABILITIES IN THE SECURITIES INDUSTRY

3.1 Introduction

48. The FATF Glossary defines a "financial institution" as including a person or entity that, among other things, conducts as a business the following activities:

- The transfer of value or money;
- Trading in :

  (a) money market instruments such as cheques, bills, certificates of deposits (CDs), derivatives, etc.;

  (b) foreign exchange;

  (c) exchange, interest rate and index instruments;

  (d) transferable securities;
- Participation in securities issues and the provision of financial services related to such issues;
- Individual and collective portfolio management;
- The safekeeping and administration of cash or liquid securities on behalf of other persons;
- Otherwise investing, administering or managing funds or money on behalf of other persons; and
- Underwriting and placement of life insurance or other investment related insurance.

49. While the activities of securities industry participants do not constitute a distinct activity category under the 40+9 Recommendations[11], the activities described in the questionnaire responses fall squarely within the FATF's definition of a financial institution. However, and perhaps not surprisingly, the full scope of securities industry activity is broader still. As such, a more detailed overview of the industry is needed in order to fully appreciate its ML/TF vulnerabilities. As the complexity of products and the diversity of the actors in the securities industry continue to expand, it is suggested that the FATF keep under consideration the extent to which the definition of "financial institution" still covers persons engaged in activities associated with the securities industry.

50. The content of this chapter is principally based on the 40 responses to the questionnaire, which asked participant jurisdictions to use the definition of "financial institution" in the FATF Glossary as a point of reference for identifying:

- Products that are classified as "securities" within a jurisdiction;

[11] The FATF 40 and 9 Special Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering and the financing of terrorism. They are available at www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html.

- The type of market access and payment methods involved e.g. securities exchanges, over-the-counter markets, use of cash or cheques for payment;

- The type of intermediaries involved in the offer, sale, recommendation, or distribution of securities e.g. broker-dealers, financial advisers, banks, insurance companies; and

- The vulnerabilities associated with each, as well as some relevant case studies.

Organisation of Material

51. This chapter is organised into eight topical sections: (1) products classified as securities according to questionnaire responses; (2) markets and other means of access; (3) payment methods; (4) securities intermediaries; (5) client and account types; (6) determination of value; (7) rogue employees; and (8) terrorist financing. Each section provides an overview of the topic area, followed by a discussion of its particular ML/TF vulnerability. When available, these sections also present case studies.

3.2 Securities Products as Described in Questionnaire Responses

52. The FATF Glossary does not define the term "security." Because of jurisdictional differences in defining the term, this report will not attempt to provide a universal definition. However, this report does provide an overview of the products that were identified as securities by the jurisdictions that responded to the questionnaire.

53. The questionnaire asked that respondents categorise securities products under the following three broad categories: (1) ***Transferable Securities****;* (2) ***Units in Collective Investment Schemes****;* and (3) ***Derivatives***.[12]

Transferable Securities

54. The questionnaire listed: (1) equities; (2) bonds and similar debt instruments; (3) certificates of deposit; and (4) bills of exchange as transferable securities. Jurisdictions were asked to include in their questionnaire responses any other products that were considered transferable securities in their jurisdictions or indicate which, if any, of the broad categories were not.

55. Most jurisdictions indicated that the products listed in the questionnaire as transferable securities were designated as such under their laws. However, jurisdictions also identified additional products to those identified in the questionnaire that were considered transferable securities, such as:

- Bank bills and guarantees;

- Bonds that are convertible to other shares;

- Bonds with a share warrant;

- Certificates of participation;

- Commercial notes;

- Debentures;

12 A glossary is provided in Annex A that defines selected terms used in this report.

- Mortgage bonds, securities and certificates;
- Notes issued in a series that obligates a corporation to pay a certain sum at a certain date; and
- Share warrants.[13]

56. It should be noted that, while most jurisdictions treat certificates of deposit as securities, seven did not. In addition, only twelve jurisdictions treat bills of exchange as securities. The fact that they are not defined as a "security" does not in itself mean that there is any gap in the regulatory or supervisory system of the jurisdiction concerned, but highlights the complexity of the terminology used to define these products, and that different authorities (for example a banking supervisor) might be responsible for AML/CFT supervision of these products.

Units in Collective Investment Schemes (CISs)

57. The questionnaire listed: (1) unit trusts; (2) investment trusts; (3) mutual funds; (4) open-ended investment companies (OEICs); (5) open-ended collective investment schemes (SICAV/Fs); and (6) closed-end companies as units in collective investment schemes (UCIS).

58. Although jurisdictions included some variants, many of these differences may be attributable to regional language differences.[14]

Derivatives

59. The questionnaire listed: (1) options; (2) futures; (3) swaps; (4) forward rate agreements; and (5) commodity derivatives contracts; and (6) foreign exchange contracts as derivatives.

60. As with transferable securities and CISs, most jurisdictions consider these instruments to be securities, with some variations.[15]

61. In most jurisdictions where instruments are not treated as securities by law, they are generally treated as "financial instruments" or "derivatives." In some jurisdictions where particular products were not considered to be securities, it was not necessarily clear what alternative regulatory regime (if any) applied to those products. This gives rise to concerns that ML/TF risks relating to those products might not be fully identified. In any event, the complexity of and ability to customise derivatives products makes it difficult to assess the full scope of products in the marketplace.

---

13 While jurisdictions identified other instruments as transferable securities, the products listed here are intended simply to illustrate the wide scope of the instruments that were included in the questionnaire responses.

14 For example, a number of jurisdictions do not treat unit trusts as securities. In addition, OEICs, SICAV/Fs, and closed-end companies are treated as securities in 18 (mainly European) jurisdictions, but do not exist in a small number of jurisdictions.

15 Five jurisdictions do not define options as securities; six jurisdictions do not define futures as securities; seven jurisdictions do not define swaps as securities and one jurisdiction indicated that swaps do not exist in its jurisdiction; ten jurisdictions do not define forward rate agreements as securities, and three jurisdictions indicated that forward rate agreements do not exist in their jurisdictions; ten jurisdictions do not define commodity derivatives contracts as securities and three jurisdictions indicated that commodity derivatives contracts do not exist in their jurisdictions.

Other

62. The questionnaire also asked jurisdictions to list any other products that would be classified as securities but that were not captured in the categories listed in the questionnaire. Jurisdictions identified:

- Annuities;
- Credit-default swaps;
- Equity-indexed annuities;
- Profit sharing agreements/certificates;
- Subscription rights; and
- Variable life insurance and variable annuities.

63. Foreign exchange (Forex) trading is an example of an activity that is technically covered by the FATF definition, but is not always consistently treated as an activity undertaken in the securities sector. Limited suspicious indicators and typology information were available for this activity. This is an area that may benefit from further study. [16]

3.2.1 Vulnerabilities Associated with Particular Types of Securities Products

64. As illustrated by the responses to the questionnaire, different jurisdictions classify a wide range of products as securities. In this respect, any of the products listed above can be utilised in the layering and integration stages of money laundering once illicit assets are placed in the financial system. As noted above, however, the securities industry is relatively inhospitable to the placement of illicit assets into the financial system Nevertheless, as discussed below, certain securities products do pose identifiable ML/TF vulnerabilities even at the placement stage.

Physical Securities (Including Bearer Securities and Bills of Exchange)

65. Although many jurisdictions have dematerialised securities, the questionnaire responses indicated that physical and bearer securities are still available in some jurisdictions. Bearer securities consist of both physical equity and debt securities that, unlike registered securities, do not necessarily require that the owner be registered with an issuer or a transfer agent. The transfer of bearer securities can be as simple as handing the security over to a new owner. It is important to note that the transfer of ownership can, in some jurisdictions, be almost as easily accomplished through electronic means that inhibit tracking any change of ownership.[17] In addition, some bearer bonds are almost equivalent to cash because they can be easily redeemed at financial institutions.

66. The anonymity and easy transferability of bearer securities presents a significant ML/TF vulnerability at all three stages of money laundering. Illicit assets can be placed in the securities industry through the purchase of bearer securities. Once a bearer security has been issued, money launderers or terrorist financiers can hold these securities or transfer them to an intended recipient without necessarily having to use facilities that would record a transaction, conduct CDD or impose KYC obligations.

16 Ten jurisdictions do not define foreign exchange contracts as securities and four jurisdictions indicated that foreign exchange contracts do not exist in their jurisdictions.

17 *Marco Arnone* & *Pier Padoan* (2008).

Recipients of bearer securities can deposit them into brokerage accounts in order to purchase other assets, or liquidate them and withdraw or wire transfer their proceeds out of the jurisdiction, thus layering and integrating the illicit assets. Bearer securities can also be used to conceal the identities of the beneficial owners of shell companies, as discussed below.

67. In some jurisdictions, bills of exchange are treated as securities. A bill of exchange (e.g. cheque, bank draft) is a written unconditional order by a drawer to a drawee to pay money on demand or at a fixed or determinable future time to a payee (the specified person or to the bearer). Bills of exchange can be payable on sight or at a future date and can be transferred by making an endorsement or signature. The risk posed by a bill of exchange is similar to that of a bearer security: ease of transfer and redemption. Although jurisdictions did not provide specific suspicious indicators for bills of exchange, those for bearer securities may be applicable.

Suspicious Indicators for Physical Securities*[18] *(including Bearer Securities and Bills of Exchange)

68. The following are suspicious indicators that are applicable to physical securities, including bills of exchange:

- The customer deposits a large number of bearer securities at the securities firm and quickly redeems the securities or sells them in the open marketplace;
- The customer requests cashing of bearer securities without first depositing them into an account;
- The customer frequently deposits bearer securities or bills of exchange into an account;
- The bearer securities or bills of exchange, if titled, are titled differently than the name on the account;
- The customer's explanation regarding the method of acquiring the bearer securities or bill of exchange does not make sense or changes;
- The customer frequently deposits bearer securities in amounts just below a jurisdiction's threshold reporting requirement;
- Payments for bills of exchange made by way of third party cheques are payable to, or endorsed over to, the customer; and
- The physical security does not bear a restrictive legend, even though the history of the security and/or the volume of shares being traded suggest that it should have such a legend.

Insurance Products

69. In some jurisdictions, insurance contracts that contain an investment component are considered to be securities, and thus are sold through a securities intermediary. For example, a variable annuity is a contract issued by an insurance company under which an investor provides the insurer with a lump-sum premium payment or series of periodic payments. In return, the insurer agrees to make periodic payments to the investor beginning immediately or at some future date. The investor is usually permitted to invest the purchase payments in a range of investment options, such as mutual funds or unit investment trusts.

[18] Physical securities are also implicated in market manipulation, as discussed in Chapter 4.

The value of the variable annuity will vary, depending on the performance of the investment options that have been chosen.

70. In addition, variable annuity contracts typically have a "free look" or "cooling off" period of ten or more days during which the investor may terminate the contract without paying any penalties and receive a refund for the amount of the contract. The amount of the refund may equal either the account value when the contract is terminated or the amount of purchase payments, depending on the terms of the contract and applicable legal requirements.

71. This "free look" period gives rise to a particular risk: a money launderer can purchase a variable annuity and then seek a refund during the free look period. The cheque received from the insurance company may not draw suspicion when deposited at a bank.[19]

72. From a supervisory or regulatory perspective, there is potential duplication, but also a potential gap, if countries have two separate supervisory authorities looking at the insurance and securities industries. Although this is outside the scope of the current study, this is an area which might benefit from further investigation.

Suspicious Indicators for Insurance Company Products

73. The following have been identified as suspicious indicators involving insurance company products:

- The customer cancels an insurance contract and directs that the funds be sent to a third party;
- The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of the funds;
- The customer cancels an annuity product within the "free look" period;[20]
- The customer opens and closes accounts with an insurance company only to open a new account shortly thereafter with the same insurance company, but with new ownership information;
- The customer purchases an insurance product with no concern for investment objective or performance;
- The customer purchases an insurance product with unknown or unverifiable sources of funds, such as cash, sequentially numbered money orders, traveller's cheques, and/or cashier's cheques;
- The customer is particularly interested in the product's early surrender and in the amount that he will then have at his disposal;
- The customer purchases an insurance contract using a single large premium payment, particularly with an unusual payment method, such as cash or cash equivalent;

19 The placement stage risks of cheques and money orders are discussed more fully below in Section 3.4 on payment methods.

20 Although this will often be a legitimate transaction, it could also signal a method of laundering funds if accompanied by other suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders, traveller's cheques, or cashier's cheques and/or the customer's having a history of cancelling annuity products during the "free look" period.

- The customer purchases a single premium policy using cash, money orders, traveller's cheques, or cashier's cheques for an amount that is clearly out of proportion to the customer's income;

- The customer enters into a contract for a considerable sum subject to payment of the premiums from abroad, particularly from an offshore financial centre;

- The customer substitutes, during the life of the contract, the initial beneficiary for a person without any apparent link to the policyholder;

- The customer cancels the contract without concern for the considerable tax or other cancellation charges that he or she has to pay as a result; and

- The customer secures a policy loan against the cash value soon after the policy is issued and repays the loan with cash or various monetary instruments.

Low Priced Securities and Private Issuers

74. Low priced securities, also known as penny stocks, refer to low-value equity interests in companies that are publicly traded or are about to become so. The issuers of these shares generally have legitimate business operations and revenue streams. However, some publicly traded penny stocks are really shell companies that may be used for a reverse merger. In any event, shares in these issuers will often be represented with physical securities that can be deposited with a securities intermediary. These shares are not likely to be traded on traditional exchanges, but rather in over-the-counter ("OTC") markets or on bulletin boards, which are discussed below. Penny stocks typically have very low trading volume but, unlike bearer securities, ownership of these shares will often be registered with the issuer and/or a transfer agent.

75. The ML/TF vulnerabilities posed by these securities are two-fold. First, these types of securities are often used to generate illicit assets through market manipulation, insider trading, and fraud. Illicit actors can either use existing shares that are already publicly traded, or start a shell company for the express purpose of engaging in those illicit activities. In addition, criminal organisations have also been known to use illicit assets generated outside the securities industry to engage in market manipulation and fraud. This first vulnerability is discussed more fully in Chapter 4.

76. Second, these securities can be acquired by investing illicit assets into a company that is about to become public. Once the company goes public, the money launderer can sell his or her stake, thereby giving funds the appearance of having been derived from a legitimate securities transaction. Moreover, criminal organisations can also initially invest in a private company that they can then use as a front company for comingling illicit and legitimate assets. They can then take this company public through an offering in the public securities markets, thus creating what appear to be legitimate offering revenues. Alternatively, criminal organisations can acquire a publicly traded company and use it to launder illicit assets.

Suspicious Indicators and Case Studies for Low Priced Securities and Private Issuers

77. The suspicious indicators associated with low priced securities and private issuers are, for the most part, identical to those that are discussed in the market manipulation section of Chapter 4.

Case Study 1: Laundering by acquisition of publicly traded shell company

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Israel
Subject:	Individual
Instruments, methods and techniques:	Front companies, publicly-traded shares of a shell company
Indicators:	• Use of a public shell company (traded on the stock exchange); • Use of a front company/straw man to perform the acquisition; • Transferring funds through several accounts; • Use of a money services business (MSB) to transfer funds; • Withdrawing the funds shortly after the acquisition by means of loans; and • Transferring funds to the same MSB.

Suspicious transaction/activity report information

The FIU received an STR from a bank regarding D, a man in his twenties with a student account. The STR stated that D bought a controlling interest in public shell company X and then proceeded to open a bank account in the name of that company. A few days later, the account received a deposit of approximately US$2.5 million.

Case description

In addition to company X, D was also the sole owner of a private company, Y. D used company Y to purchase a controlling interest in company X through the OTC market. Part of the US$2.5 million that was credited to company X was derived from a company Y account. Company Y received large deposits from several private accounts managed by criminal entities involved in drug trafficking. In one case the funds were transferred from the person known to be involved in criminal activity through an MSB account to the account of company X to further distance the source of the funds. The new controlling owners appointed new directors, including family members.

Shortly after the US$2.5 million was transferred to the account of company X, it was transferred back to the MSB account. Some of the money was transferred as a loan to company W, which was associated with the same criminal organisation that originally transferred funds to Company Y.

D and his family were well-known to the FIU for having acquired public shell companies in the past for money laundering purposes, including committing other predicate offences. They were also suspected of fraudulently influencing the movement of the stock share prices of companies owned by them, performing circular transfers of funds, and fraudulently removing funds from the companies.

Options

78. An option is a contract where one party (option seller) agrees to either buy a specified number of securities from, or sell a specified number of securities to, another party (option buyer) at a specified price per share (strike price). The option seller receives an upfront payment (premium) in exchange for assuming the obligations under the option. A put option gives the option buyer the right to sell the securities to the option writer at the specified price. A call option gives the option buyer the right to buy the securities from the option writer at the strike price. Typically, the option buyer has the right, but not the obligation, to exercise the option contract. Options can be traded on exchanges or OTC. They can be physically-settled (i.e. settled by delivering the securities) or cash-settled (i.e. settled by making a cash payment equal to the difference between the strike price and the market price of the security times the number of securities specified in the contract).

79. An OTC option presents a ML/TF vulnerability if one party agrees to enter into an options contract on terms worse than those available in a rational market to guarantee that the counterparty receives a net payment. In this respect, an OTC option can be used as a method of transferring funds.

80. For example, assume Party A has funds in a brokerage account that he wants to transfer to Party B. Assume there is a security with a market price of $7 per share. Instead of transferring the funds via a wire transfer or cheque, Party A may sell for a nominal premium to Party B, a cash-settled put option on the security with a strike price of $15 per share for 10,000 shares. Party B exercises the option

immediately, and because the option is cash settled, Party A pays Party B the difference between the strike price and the market price of the security, or $80,000. In addition, funds transfers using options may be accomplished without exercising an option, such as by charging a high premium for a worthless contract (e.g. a call option with a strike price hundreds of times higher than the market price), by exercising an out-of-the money option, or through other options contract variations.

3.3 Markets and other Means of Access

81. With the demise of the traditional trading floor located in a bricks-and-mortar securities exchange, many securities transactions are now effected electronically. In addition, some securities transactions are not conducted through an exchange at all. The following section examines the markets and mechanisms through which securities are sold and purchased.

Traditional Exchanges

82. The term securities exchange typically refers to centrally organised entities that operate as trading markets for publicly held securities. Exchanges generally have listing standards, such as minimum operating histories and revenue streams. While some exchanges only trade equity securities, other exchanges specialise in particular products, such as debt, options, and other types of derivative instruments. In addition, exchanges may require that intermediaries, such as broker-dealers, become exchange members and adhere to certain financial and operational standards.

Over-the-Counter (OTC) Markets

83. Many equity securities are traded in the OTC market and not on exchanges. The OTC market generally refers to all trading of securities otherwise than on an exchange, including various arrangements by which securities intermediaries arrange trades amongst themselves. Some OTC markets are organised and have automated quotation systems. Penny stocks, as discussed above and in Chapter 4, are also traded on the OTC markets, with their prices sometimes quoted on electronic bulletin boards.

84. Unlike traditional exchanges, organised OTC markets generally do not establish listing requirements and may not regulate issuers or trades, or have members. In some jurisdictions, however, there may be a regulator for the OTC markets as a whole. Securities traded on OTC markets may be more speculative than the securities listed on more traditional exchanges.

Alternative Trading Platforms (ATPs), Electronic Communications Networks (ECNs) and Internet-Based Trading Accounts

85. While trading on exchanges and OTC markets typically requires the use of a securities intermediary, new technologies permit institutional investors and some retail investors to engage in securities transactions with limited involvement of an intermediary.[21] Alternative trading platforms and electronic communications networks can operate in a way that, in some instances, may permit investors to trade with relative or complete anonymity.

86. Broker-dealers and others institutions licensed to effect securities transactions offer their clients the ability to transfer securities held electronically (e.g. from broker to broker, or from one customer to the account of another, such as a spouse). Some jurisdictions have indicated that this service can be abused and poses a ML vulnerability. This vulnerability results from the relative ease of the instrument's transfer,

[21] ATPs and ECNs, however, are traditionally registered as securities intermediaries.

the lack of transparency associated with some transfers, the ability to effect cross-border transfers, and even unjustifiable reliance on the CDD/KYC investigations done by others.

87. A particularly attractive feature (in some jurisdictions) to persons who wish to abuse this service for ML purposes is its lack of transparency. In some instances, a transfer can be effected without the individual having an account with the financial institution, for example through a breach in the financial institution's data security, or through the transfer of an instrument similar to a bearer security. Payment for the transferred securities can also be made in cash. As such, account statements may not reflect the fact that a share transfer has taken place. In some cases investigated, transfers of securities were confirmed to the customer by separate statements that were not consecutively numbered. Moreover, such statements were not included as part of the year-end bank reconciliation effort.

Case study 2: Securities transfers

Offence:	Tax evasion
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	The Netherlands
Subject:	Individuals and service providers
Instruments, methods and techniques:	Transfer of securities held electronically
Indicators:	• Misuse of service provided by financial institutions; • Ante-dating of documents; • Transactions without an apparent economical rationale; and • Use of false documentation.

Case description

The Tax Administration and the Fiscal Intelligence and Investigation Service has discovered methodologies involving the allocation of securities as a means to effect tax fraud. These activities involved the use of false documents, in violation of tax and criminal laws. To date, 14 cases have been detected, involving six different financial institutions. Seven cases have been investigated in greater depth. The key role played by the facilitating financial institutions in these cases was examined by the Dutch Central Bank and The Netherlands Authority for the Financial Markets.

The cases investigated have in common the misuse of a normal and legitimate service provided by banks, broker-dealers and other institutions licensed to trade in securities: the ability to transfer securities held electronically.

The misuse in the Dutch cases was triggered by a difference in the way capital gains and losses were treated for the income and corporate tax purposes. In short, capital losses are not deductable for income tax purposes, but are included in the tax base for corporate tax.

In these cases, individuals transferred securities between their personal portfolio and a corporate securities portfolio over which they had control. Depending on what was necessary in the specific case, securities were transferred in either direction. In the case of a loss that occurred in the personal portfolio, the relevant securities were transferred to the corporate stock portfolio and vice versa.

The attractive feature of the misuse of the securities-transfer service is its lack of transparency. In a transfer there is no mandatory current account relationship. As is the case with regular sale and purchase instructions, payment for securities transferred can be arranged by other means, such as cash payments. As a consequence, bank statements do not have to show that a share transfer has taken place. In the different cases that were investigated, transfers of securities were communicated to the client by separate statements that were not consecutively numbered and that did not have any connection with the year-end bank reconciliation.

What was surprising in the cases investigated was:

1. The number of cases detected;
2. The similarity of modus operandi;
3. The relative ease in which employees of financial institutions were persuaded to co-operate in the scheme;
4. The fact that the cases took place at different players in the financial sector;
5. The involvement of accountants and tax advisors;

6. The lack of AML/TF monitoring for this specific kind of transactions; and

7. The possible AML/TF risks related to share transfers were perhaps not sufficiently familiar to supervisory bodies.

Enforcement actions

All cases investigated resulted in administrative or criminal sanctions. Some financial institutions also were required by financial regulators to amend their internal procedures.

88. Although case study 2 involved tax fraud, the transfer of securities can also play a role in insider trading. It is also a vulnerability in the context of money laundering, due to the relative ease of transfer, lack of transparency, lack of indicators and the international dimension.

89. It would be possible for criminals to approach individuals and offer them cash for their securities portfolio. Subsequently these individuals could transfer their securities from their securities portfolio to the securities portfolio of the criminal. This would give criminals access to the financial system while circumventing existing AML/CTF measures.

3.3.1 Vulnerabilities Associated With Particular Types of Market Access

90. Although the survey results did not identify actual abuses involving internet trading platform services, several areas of vulnerability were noted. For example, with the continued development of technology, the number of firms providing internet trading platform services has increased. Such firms offer trading in financial contracts (so-called contracts for difference or CFD) on their trading platform linked to different kinds of underlying reference points: mostly Forex but also market indexes, and commodities (such as oil and precious metals), as well as on shares of companies. The investors are typically required to pay a margin deposit into the bank account of the firm.

91. Such website trading platforms are often designed for day trading, and can have substantial transaction volumes. As such, the trading platform could turn into a "black box" for the financial institution (often a bank) with which the trading platform firm holds its accounts, making it very difficult for the financial institution to understand transactions occurring in the account.

92. Moreover, obtaining a licence for a trading platform has become increasingly inexpensive. By providing a trading platform through a company registered in an unregulated jurisdiction, a criminal organisation could pose as a securities dealer and use this structure to launder money and/or defraud investors.

93. Internet-based securities trading accounts pose particular challenges to the implementation of CDD/KYC procedures because of the lack of face-to-face interaction between the intermediary and the customer when an account is opened. This can hamper the ability of a firm to establish an adequate customer profile, which in turn can hamper the firm's ability to detect suspicious activity. Moreover, although investors must open accounts with intermediaries to access their systems, some of these accounts allow the investor to directly access an exchange or trading system, potentially hampering the ability of an intermediary to identify suspicious transactions and trading patterns. Because positive identification of an individual can be more difficult with internet-based account opening methods, identity thieves and other illicit actors have been known to open these types of accounts to engage in market manipulation, insider trading, securities fraud, or to deposit illicit assets that can be wire transferred out of that account.[22]

[22] Please see Chapter 4 for a fuller discussion of market manipulation, insider trading and securities fraud.

94. In addition, legitimate internet-based brokerage accounts are often compromised by online intrusions from unauthorised persons. To cite one example, a criminal can effect an intrusion into multiple customer accounts. The intruder can liquidate securities in those accounts and use the proceeds to buy a penny stock. This has the effect of "pumping" up the price of the penny stock, which the intruder then liquidates at the inflated price, with profits transferred out of the intruded accounts.

Case study 3: Rapid transactions using an internet-based trading account

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Insider trading
Jurisdiction:	Austria
Subject:	Individuals
Instruments, methods and techniques:	Internet-based trading account, shares
Indicators:	• High profits within one day; • Rapid purchase and sale of shares; and • Use of the same password by several clients.

Suspicious transaction/activity report information

The FIU was informed by an Austrian internet bank about suspicious bank accounts. The suspicions were prompted by the suspicious behaviour of several clients (high profits within one day, purchase of shares and sale of the shares one day later, purchase of calls, five different clients from the same country, use of the same passwords, the same shares/calls, etc).

Case description

A number of securities deals were made in connection with a company sale (takeover of shares) yielding a stock price gain of around US$6 million. These sales were later found to have been facilitated by insider trading; Austrian accounts were used for buying and selling shares.
Thorough investigations revealed that several accounts were linked to this securities deal, i.e. the account owners (Croatian nationals residing in Germany, Croatia, and the U.S.) obtained huge profits within a very short time by (almost simultaneously) buying and selling these shares.

Enforcement actions

The FIU initiated not only the necessary financial analysis but also analysis regarding the shares (company based in the U.S. press information – insider trading) and evidence regarding the involved persons.
It was rather urgent to secure evidence (including seizure of banking accounts and/or transmitting information to other agencies to trace the money flow) therefore the FIU met the FBI to cooperate in the case.
The FIU immediately informed the prosecutor of potential money laundering and insider trading charges.

Suspicious Indicators and Case Studies Associated with Market Access

95. The questionnaire responses did not specifically identify suspicious indicators associated with market types and other means of access. However, the suspicious indicators associated with market manipulation, insider trading and securities fraud may have some relevance in this area for detecting money laundering. Accordingly, Chapter 4 contains a fuller discussion, including case studies, regarding OTC markets and internet-based securities trading. In addition, the suspicious indicators related to Customer Due Diligence in Annex B are also generally relevant.

3.4 Payment Methods Relating to Securities Transactions

96. Many of the payment methods associated with securities transactions are not unique to the securities industry, and are to be found in other areas of the financial services industry. However, there are certain peculiarities in the purchase of securities which benefit from further elaboration.

Cash

97. The questionnaire responses indicated that the use of cash in the securities industry is uncommon. However, in some jurisdictions cash is still a permissible payment method. In addition, in some jurisdictions securities can be purchased through depository institutions, where acceptance of cash is much more prevalent.

Vulnerabilities and Suspicious Indicators for Cash

98. Depository institutions and securities intermediaries that permit the use of cash for the purchase of securities products can be used to place illicit assets in the securities industry, as well as integrate and layer the assets through securities trading and redemptions.

99. The following, which are not necessarily unique to the securities industry, were identified as suspicious indicators involving the use of cash:

- The customer refuses to identify a legitimate source for the funds or provides the securities firm with information that is false, misleading, or substantially incorrect;
- The customer makes many small cash deposits that are eventually used to purchase a particular securities product which is sold or redeemed shortly thereafter;
- The customer deposits a large amount of small-denomination currency to fund the account or make securities purchases;
- There are many incoming cash deposits into a customer's account from third parties that coincide with or are close in time to outgoing cheques or wire transfers to other third parties; and
- The customer has accounts primarily used for deposits and other accounts primarily used for outgoing payments.

Case study 4: Structuring of cash deposits

Offence:	Money laundering (structuring)
Securities Related Predicate Offence (if any):	Fraud
Jurisdiction:	Australia
Subject:	Individual
Instruments, methods and techniques:	Cash deposits, contract for difference account
Indicators:	• Abuse of internet registration systems; • Multiple same day transactions; • Structuring of cash deposits; and • Use of false identification documentation.

Suspicious transaction/activity report information

D became the subject of a STR submitted to the FIU that detailed activity involving the structuring of cash deposits into an account.

Case description

A "contract for difference" (CFD) is a type of derivative where an agreement is made to exchange the difference in value of a particular security (or other financial instrument) between the time at which a contract is opened and the time at which it is closed. In this particular investigation, the profits were deposited in a major Australian bank.
D used false identification documents, including a false citizenship certificate and driver's licence, to open a trading account over the internet.
The individual became the subject of an STR because of the structuring of cash deposits into an account. The STR highlighted that over an eight-day period, approximately AUD$ 400,000 was deposited into the account in amounts

below the jurisdiction's threshold reporting requirement (i.e. structuring), and in some instances deposits were made on the same day at branches in two different locations.
The investigation identified that the account had traded and increased in value to over AUD$ 750,000, which was subsequently restrained by means of crime restraining orders.

Enforcement actions

An investigation into this resulted in criminal restraining orders being placed on the individual's assets

Cheques and Wire Transfers

100. Questionnaire responses indicated that cheques can be used to fund a securities account with a securities intermediary or used to directly purchase some securities products without an intermediary. In addition, jurisdictions indicated that the use of cheques is not limited to those drawn from a depository account, but also can involve money orders, traveller's cheques, and cashier's cheques (i.e. bank drafts).

101. While many wire transfers occur through and between banks, in some jurisdictions a securities account can be used in lieu of a depository account to wire funds.

Vulnerabilities and Suspicious Indicators for Cheques and Wire Transfers

102. Money launderers can purchase money orders, traveller's cheques, and/or cashier's cheques with cash over a period of time or through a series of transactions in order to avoid threshold currency reporting requirements. These cheques can then be deposited into securities accounts until a desired amount is reached and used to purchase a security, which is then sold or transferred. Alternatively, a money launderer can also wire the illicit assets out of a jurisdiction.

103. Cheques or wire transfers from a depository account also present an ML/TF vulnerability because they may unreasonably affect the securities intermediary's risk analysis, in particular with respect to CDD/KYC obligations. For example, if a cheque or wire transfer originates from another financial institution subject to an AML/CFT regulatory regime, a securities firm may not conduct a thorough CDD/KYC investigation because it believes that the originating financial institution has already conducted its own CDD/KYC investigation, or because the firm perceives a reduced risk because the customer was able to open an account at another financial institution. This vulnerability can become systemic if numerous securities intermediaries perceive a reduced risk based on the activities of others.[23]

104. In addition, even if the financial institution from which the cheque or wire transfer originated has conducted thorough CDD/KYC and not detected anything suspicious, there may still be an ML/TF risk that the securities intermediary, through its own knowledge of the investor, may be in a unique position to identify. In particular, CDD/KYC not only involves mere customer identification but establishing the purpose and intended nature of the business relationship.

105. Another vulnerability identified is the increasing use of the securities industry in offshore jurisdictions by criminals attempting to avoid domestic seizure of their assets. The ease by with which funds could be transferred electronically facilitates this. The use of this method of disguising funds has resulted in a reduction in the effectiveness of domestic seizure/forfeiture actions, marking a change in the laundering techniques used by criminals. The advantage of this method over, for example, the purchase of domestic real estate is that it is more difficult for law enforcement to trace and seize assets held offshore.

[23] It is noted that reliance on CDD/KYC investigations undertaken by a foreign financial institution should also involve an assessment of the AML/CFT regime operating in the country from which the institution relied upon operates. Given the global nature of the securities industry, this issue may be of particular importance.

106. The following, which may not be unique to the securities industry, have been identified as suspicious indicators involving the use of cheques and wire transfers:

- Many small incoming deposits are made using cheques, money orders, traveller's cheques, and cashier's cheques;
- Incoming payments are made by third-party cheques or cheques with multiple endorsements;
- Money orders, traveller's cheques or cashier's cheques are sequentially numbered in denominations that avoid threshold reporting requirements (i.e. structuring);
- Outgoing cheques to third parties coincide with or are close in time to incoming cheques from other third parties;
- Wire transfers are made to or from financial secrecy havens, tax havens or high-risk geographic locations (i.e. jurisdictions known to produce illegal narcotics/psychotropic drugs or are related to terrorism);
- Wire transfers or payments are made to or from unrelated third parties (foreign or domestic) or where the name or account number of the beneficiary or remitter has not been supplied;
- Many small, incoming wire transfers are made, either by the customer or third parties, that are almost immediately withdrawn or wired out in a manner inconsistent with customer's business or history;
- There is wire transfer activity that is unexplained, repetitive, unusually large or shows unusual patterns or has no apparent business purpose;
- The securities account is used for payments or outgoing wire transfers with little or no securities activities i.e. account appears to be used as a depository account or a conduit for transfers;
- Funds are transferred to financial or depository institutions other than those from where the funds were initially directed, specifically when different countries are involved;
- Transfers with no apparent business purpose are made between different accounts owned by the customer;
- Wire transfer logs, when viewed over a period of time, reveal suspicious or unusual patterns;
- The customer requests that certain payments be routed through nostro or correspondent accounts held by the financial intermediary instead of its own account; and
- Outgoing wire transfers to third parties coincide or are close in time to incoming wire transfers from other third parties.

Case study 5: Use of foreign exchange broker

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Mexico
Subject:	Individual
Instruments, methods and techniques:	Deposits of cheques, currency exchange, wire transfers
Indicators:	• Activity reported by senders to financial institutions is not related in any way to the beneficiary of funds; • Amounts transferred are not congruent with the purchase of products; • FX dealer/broker or bureau de change order the transfers abroad (and not the senders); • Common beneficiaries with other customers using the same operating procedure; and • Same day withdrawal of funds.

Case description

During the course of an investigation made by the FIU regarding proceeds from drug trafficking, an individual was identified acting as branch manager of a local foreign exchange broker involved in ML activities and, later on, acting as account executive for a broker-dealer who was arranging wire transfers for one of his customers.
Accordingly, the FIU informed the broker-dealer of this activity, and it submitted an STR, with no specific information. Further investigations showed that an account at this broker-dealer was used to send money abroad in the following way:
The broker/dealer received several cheques in local currency, in the name of different persons but all of them endorsed to the same account holder (the sender). Funds were withdrawn immediately (the same day) with a purchase of US$ and a further wire transfer abroad was arranged for one single beneficiary (different from the sender). This money was ultimately used to partially pay for the acquisition of real estate properties in the USA.

Enforcement actions

The outcome of this investigation was the seizure of many assets, including among others, bank accounts and aircraft, and the closing of the foreign exchange broker involved.

Case study 6: Company director misused family trust

Offence:	Tax evasion / False Invoicing
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Australia
Subject:	Individual / Company
Instruments, methods and techniques:	Purchase of shares in foreign jurisdiction
Indicators:	• Several significant wire transfers into Australia from a tax haven.

Case description

An Australian resident company that was receiving funds from a known tax haven was the subject of an audit. The director/shareholder of the company was also connected to a company established in a tax haven. This tax haven company had purchased shares in a U.K. company and then sold them for a substantial capital gain. Some of the profits were repatriated to Australia via the use of false invoices issued by the Australian resident company. The funds entered the country through large wire transfers.

Enforcement actions

The director/shareholder was assessed on income earned from world wide sources and agreed, as part of a settlement, to cease his involvement in the tax haven based company and repatriate all funds held in overseas jurisdictions.
As a result, approximately AUD$ 1.4 million in tax and penalties were raised.

Case study 7: Unlicensed securities intermediary

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Providing investment services without a licence
Jurisdiction:	Belgium
Subject:	Individuals, company
Instruments, methods and techniques:	Cross-border funds transfers, use of third parties
Indicators:	• Significant wire transfers by multiple individuals; • Messages accompanying the wire transfers referred to investments; • Transactions happening shortly after opening of the bank account; • Account opened for personal use; and • Account not used as anticipated.

Suspicious transaction/activity report information

X and Y were managers of company A, active in purchasing securities for third parties. Shortly after company A's establishment, X and Y opened an account in their name for personal use. A few days later this account was credited with several transfers by order of third parties for a total amount of several thousand EUR.
The parties to the transfers were not linked to the individuals in any way. Furthermore, the references of these transfers referred to an investment fund. The name of the account also referred to an investment fund. The debit transactions consisted of transfers to accounts opened abroad in tax haven countries and the registration to investment products.

Case description

Information from the supervision authorities showed that company A did not have a licence to offer investment services.
The name of the individuals' personal account, the person receiving the transfers, the regularity and the references accompanying the transfers as well as the destination of the funds showed that the transactions were not performed for X and Y but for a third party. The money was laundered through transfers abroad and registration to investment products.

Enforcement actions

The case for providing investment services without a licence was referred in 2005 to the public prosecutor for ML.

Exchange of Securities as Means of Payment

107. One payment method that is unique to the securities industry is the use of securities in exchange for other securities. This can occur when shares of a different type are issued or new shares issued in a take-over. The exchange of shares is a potential way of moving value from one company to another, and the possibility for disguising the origin of funds is clear. For example, if illicit funds are used to purchase shares in the initial company, these may be harder to trace once the shares are exchanged for those in another company. The situation can be exacerbated when other factors are involved, such as shares traded off exchange or those from countries without robust AML/CFT controls.

3.5 Entities Involved in the Offer, Sale, Advice, Management or Distribution of Securities ("Securities Intermediaries")

Broker-dealers

108. One of the most active participants in the securities market is the broker or dealer in securities. A broker typically acts in an agency capacity for an investor, and enters the securities markets on behalf of an investor to buy or sell a security. In some jurisdictions, a dealer acts in a principal capacity and sells to investors from the dealer's own inventory or buys from an investor in order to add to the dealer's inventory. In buying and selling in this manner, some dealers also provide liquidity to the market.

109. Based on the questionnaire responses, brokers and dealers exist in most of the jurisdictions that responded to the survey. However, they are often referred to using a variety of terminology such as:

- Financial Instruments Business Operator;
- Firms for Placement in Orders in Financial Instruments;
- Investment Firms;
- Investment Service Provider; and
- Underwriters.

110. A common type of brokerage relationship involves an introducing broker-dealer and a clearing broker-dealer who allocate among themselves the tasks that would normally be performed by a single broker-dealer. Under this sort of relationship, the introducing broker-dealer typically interacts directly with the customer, opening and monitoring the customer's account and accepting orders. The clearing broker provides securities record-keeping, trade execution, clearing and settlement services, custodial services, account statements and extensions of credit in margin accounts. In contrast to a clearing broker, an introducing broker usually cannot maintain custody of a customer's cash and securities.

Vulnerabilities Associated with Broker-Dealers

111. A specific vulnerability associated with broker-dealers is their reliance on another financial institution's CDD/KYC investigation, as discussed in Section 3.4 regarding payment methods. A broker-dealer might assume that, because another financial institution has opened an account for a customer, the customer does not raise ML/TF issues. The CDD/KYC vulnerability is most problematic in relation to the funding of a securities account. If illicit assets are successfully placed at a depository institution, the broker-dealer may assume that, because the funds are from an institution which is subject to AML/CFT rules, the customer does not pose a ML/TF risk and therefore will accept cheques or wire transfers from that institution to fund a securities account. Once a securities account is funded, a customer can engage in a number of transactions that further conceal the source of his or her illicit funds, thereby successfully layering and integrating illicit assets that were placed through a depository institution.

112. With respect to introducing and clearing broker-dealers, in some jurisdictions introducing brokers delegate the responsibility of monitoring for suspicious transactions to their clearing brokers. However, it is important to note that in some jurisdictions, while a task may be delegated to another entity, responsibility for that task's execution cannot be. As a result, it may continue to be the responsibility of both the introducing broker and the clearing broker to monitor transactions for suspicious activity in brokerage transactions that occur through their respective institutions.

113. Furthermore, some jurisdictions explicitly permit a clearing broker to rely on the introducing broker to conduct certain parts of the CDD/KYC process. Some of these jurisdictions may also extend this reliance to allow the clearing broker to rely on the CDD/KYC undertaken by a *secondary* introducing broker that has itself introduced accounts to the primary introducing broker. ML/TF vulnerabilities are amplified when any of the introducing brokers come from jurisdictions that have lax AML/CFT regimes, in particular with respect to correspondent or omnibus accounts, as discussed below. As a result, some jurisdictions allow reliance on another intermediary (whether foreign or domestic) *only if* that intermediary has in place adequate AML/CFT controls.

114. Although most broker-dealers do not accept cash payments, some do. For those broker-dealers that do, the relevant suspicious indicators associated with cash have been addressed in Section 3.4. In addition, because most securities transactions require the use of a securities intermediary, the majority of the suspicious indicators listed in previous sections, as well as the indicators in Annex B, are applicable to broker-dealers. Accordingly, specific indicators are not listed here.

Case study 8: Account held by an institution located in a high risk area/jurisdiction

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Proceeds of various crimes (including drug trafficking) invested in the securities industry
Jurisdiction:	Canada
Subject:	Individuals (lawyers), bank and trust company
Instruments, methods and techniques:	Wire transfers, bank drafts
Indicators:	• Accounts used as pass-through; • Involvement of several jurisdictions; and • Transactions below the reporting threshold.

Suspicious transaction/activity report information

Securities dealers have identified transactions involving accounts in the name of what appeared to be a bank or a trust company incorporated in an island in the Pacific. Money was moving from the Asia-Pacific region to investment accounts in Canada then to beneficiaries in the U.S.

Case description

The bank was incorporated in an island in the Pacific know for the ease of setting up financial institutions.
A securities dealer reported that the client (bank or a trust company)'s account was managed (activity of buy, sell, wire transfers, etc) by two individuals employed by a law firm in a major Asian city. The two individuals were suspected to be lawyers.
In a notice issued by a regulator of financial institutions, the Canadian public was warned that the bank or trust company was not authorised to conduct banking services in Canada.
An analysis of the financial transactions involving the institution and information retrieved from public documents led to suspicions that the bank was facilitating deposits of funds generated by various criminal activities (particularly heroin and opium trade in Asia), then transferring the money to accounts at securities dealers in Canada under the supervision of the two lawyers in Asia.
The two individuals in Asia were ordering numerous wire transfers on behalf of the bank from accounts held at different locations in the Asia–Pacific region, to investment accounts in Canada and other beneficiaries. Once received, the money was transferred to different individuals whose addresses were at different locations in the United States. The purpose of the wire transfers and the relationship between the bank and the beneficiaries of the transactions could not be determined.
Although not mentioned by the securities dealers when reporting the suspicious activity, it was suspected that the primary purpose of the wire transfers from the Asia-Pacific region was to send funds to beneficiaries in the United States. The beneficiaries in Canada were just acting as intermediaries in the money laundering process; an analysis of the transaction flows revealed that they were in fact nominees.

Enforcement actions

The case was referred to law enforcement for investigation.

Case study 9: Use of margin account with little trading

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Hong Kong
Subject:	Individual
Instruments, methods and techniques:	Deposit and withdrawals of funds
Indicators:	• Client deposited funds into the broker's account and requested repayment of funds within a short period of time with no apparent reason; • Little or no trading was recorded during the period; and • The amount of funds deposited was not in line with the client's profile.

Case description

Profits from illegal bookmaking were transferred from the bank account of the syndicate head's wife and sister-in-law to the margin account of the syndicate head.
Little or no trading occurred in the margin account.
Funds were then withdrawn as cashier's cheques and subsequently deposited into the bank account of the syndicate head.

Case study 10 : Activity of wash trading

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Stock manipulation
Jurisdiction:	Canada
Subject:	Insiders
Instruments, methods and techniques:	Securities accounts, wire transfers, cheques, bank drafts
Indicators:	• Insiders conducting similar transactions; and • Purchases and sales involving stocks of specific companies in a short period of time.

Suspicious transaction/activity report information

A number of suspicious transaction reports were filed by securities dealers on three individuals suspected of involvement in wash trading. The individuals were purchasing and selling shares of three public companies for no apparent reason. The three individuals had accounts at different securities dealers.

Case description

Three individuals, who appeared to be associates, were purchasing shares of three companies (A, B, and, C) and selling them a short time later.
One of the individuals was listed as a CEO of Company A, the other two as members of the senior management team of Company B. According to public documents, Company A was linked to Company B and Company C.
The group traded shares of the companies through personal accounts held at different securities dealers.
The three individuals were conducting the same transactions at the same time. The activity was similar to a money laundering technique known as "structuring" since the three individuals in reality were dividing the purchase-sale scheme between them.
The proceeds of sales were deposited into personal securities accounts and moved shortly to bank accounts held by the same individuals or others that are suspected to be nominees.

Proceeds of crime (wash trading) in the case

- Money from the sales of shares of Company A, Company B and Company C conducted by the three associates.

Specific money laundering transactions

- Movement of money from the securities account to bank accounts (that can be used to purchase other assets or make wire transfers).

- Movement of money to suspected nominees.

Enforcement actions

The case was referred to law enforcement for investigation.

Case study 11: Rapid purchase and sale of shares

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Stock manipulation
Jurisdiction:	Canada
Subject:	Individuals, corporations
Instruments, methods and techniques:	Wire transfers, use of multiple securities accounts
Indicators:	• Buying and selling securities with no discernible purpose in circumstances that appear unusual; • Use of multiple accounts at a single securities dealer for no apparent reason (movement of funds from one account to another); and

- Proceeds of sale used to purchase monetary instruments payable to nominees.

Suspicious transaction/activity report information

A bank reported that large wire transfers ordered from a securities dealer were received into a business account administered by Person A. Once received, money was used to purchase bank drafts, and cheques were issued payable to various individuals and entities. The purpose of the transfers between the securities dealer and the bank is not known, since the individual has refused to respond to questions asked by the bank's anti-money laundering section. It was suspected, however, that the client was "dumping" in the market a large number of shares purchased earlier (evidenced by previous wire transfers sent to the securities dealer) once they reached a certain value.
The securities dealer that sent the wire transfers also reported the following on Person B:

- Listed investment advisor: Person A;
- Was the signing authority of 24 accounts held by two corporations located in two Central American countries. The review of the accounts activity revealed movement of funds from one account to another;
- Was purchasing shares of specific companies, selling them a short time later and wiring the proceeds to bank accounts held by the corporations at financial institutions located in Central America and the Caribbean; and also to a bank account administered by Person A; and
- Never held stocks long enough to take advantage of future dividend distributions.

Another securities dealer reported that an individual, whose investment advisor was also Person A, purchased a large number of shares and sold them a short time later with no economic gain. When purchasing the stocks, the client never used wire transfers but rather cheques drawn on an account held in a financial institution located in a foreign country. The transactions always involved one particular company.

Case description

The case relates to eight individuals and two corporations involved in a stock manipulation scheme:

- Person A was the investment advisor of a group of 7 individuals.
- Person B was listed as the signing officer of two corporations.
- The two corporations had addresses in two different Central American countries but also held bank accounts in other Caribbean locations.

According to information posted in a market regulator's website:

- Person A was the main subject of a stock manipulation investigation.
- One person of the group was under investigation for banking fraud in an Asian country; the fraud cost investors close to CAN$100 million (awaiting extradition).

Person A appeared to be providing information on when to purchase and sell stocks of specific firms to the rest of the group. The investors did not hold the stocks enough to take advantage of dividend distributions. Proceeds of stocks sold were:

- Wired to bank accounts held overseas;
- Used to purchase banks drafts or to issue cheques payable to individuals and entities (it was suspected that the beneficiaries were nominees).

Analysis of the financial transactions of the remaining individuals of the group revealed constant purchases and sales of securities whose proceeds were deposited in bank accounts followed by issuance of cheques or bank drafts payable to individuals and entities. Some transactions involved penny stocks and stocks traded on the pink sheets (which are less regulated, and therefore more easily manipulated).

Proceeds of crime (stock manipulation) in the case

- Wire transfers received into a business account administered by Person A.
- Money received from the sale of securities conducted by Person B and other members of the group.

Specific money laundering transactions

- Funds wired by Person B to accounts held by the corporations in financial institutions located in Central America and the Caribbean.
- Funds wired by Person B to the business account administered by Person A.
- Movement of funds between accounts (review of Person B's accounts activity).
- Purchase of bank drafts and issuance of cheques payable to individuals and entities.

Enforcement actions

The case is being investigated by law enforcement and a provincial securities regulator.

Investment Advisers and Wealth Managers

115. Brokers and dealers in securities can be distinguished from those securities intermediaries that are regulated as advisers and wealth managers. In some jurisdictions, the role of a broker and a dealer are clearly delineated from those of advisers or managers. In fact, different registration and regulatory standards may apply. Nonetheless, functions can be housed in the same entity by means of multiple registrations. In other jurisdictions, advisory functions and broker-dealer functions may be conducted under the same registration.

116. Regardless of whether a jurisdiction has dual registration regimes, the role of the investment adviser and wealth manager is generally to advise on the composition of an investment portfolio or to manage the contents of investment accounts for retail or institutional clients.

117. Wealth management typically involves the provision of financial services in a managed relationship with clients who are often of high net worth. The value and complexity of products offered to high net worth clients, together with the international nature of the business, make the provision of wealth management services potentially attractive to money launderers.

Suspicious Indicators Associated with Advisory Services/Wealth Management

- Wealthy/powerful and PEP clients – who are reluctant to provide full CDD information, and who seek confirmation that their affairs will be kept confidential;
- Clients with multiple and complex accounts in more than one jurisdiction, either within the same firm or group, or with different firms;
- Clients using wealth management services in conjunction with offshore trusts/shell companies to disguise beneficial ownership;
- Wealth management activities in countries with a tradition of banking secrecy;

- The transmission of funds and other assets by private clients that involve high value transactions, requiring rapid transfers to be made across accounts in different countries and regions of the world; and

- The use of pooled/omnibus type accounts that are used together to collect funds from a variety of sources and clients for onward transmission.

Depository Institutions

118. The survey responses indicated that in some jurisdictions, depository institutions also serve as intermediaries for transactions in securities or provide investment advice/financial planning services.

119. The most common vulnerability associated with depository institutions involves the placement of illicit assets into the financial system. Once these illicit assets are placed they can be wire transferred out of a jurisdiction or used to purchase different assets, such as securities products. The risk that illicit assets will be used to purchase securities products is increased in jurisdictions where customers can purchase securities directly through the depository institution or through an affiliated securities intermediary. Moreover, as discussed above, if illicit assets are successfully placed at a depository institution, a securities intermediary, whether affiliated or not, may unjustifiably rely on the depository institution's CDD/KYC investigation and assume that the customer poses no ML/TF risk.

120. In this regard, the vulnerabilities and suspicious indicators associated with payments methods, market access and securities intermediaries are all applicable.

121. In addition, as discussed in Chapter 4, depository institutions may be in the best position to identify and report on securities fraud that may not necessarily require the use of a securities intermediary.

Insurance Companies

122. Insurance companies issue products that in some jurisdictions are considered to be securities. The vulnerabilities and suspicious indicators associated with these products were discussed above in Section 3.2.1. In addition, where permitted, insurance companies can also serve as a securities intermediary. The vulnerabilities and suspicious indicators associated with payments methods and the previously discussed securities intermediaries are all applicable to insurance companies that engage in comparable activities.

Use or Creation of a Financial Institution for ML/TF Purposes

123. The criminal use of a financial institution for the purpose of laundering money or financing terrorism is possible in any area of the financial services system. Criminal elements can either create or gain direct control of such an entity or seek to exert influence over the management or staff in furtherance of their aims.

124. It is possible for a securities broker-dealer, for example, to be created or used for the specific purpose of laundering funds/financing terrorism. The FATF 40 + 9 Recommendations require measures to prevent criminals or their associates from "holding or being the beneficial owner of a significant controlling interest or holding a management function."[24] Clearly the risk of criminal penetration of the securities market is heightened by opaque corporate structures, but also increases when dealing with other financial institutions from countries with lax AML/CFT measures.

[24] FATF Recommendation 23.

Suspicious Indicators Associated with Criminal Influence in a Financial Institution:

- Corporate structures where beneficial ownership is difficult to determine; and
- Companies incorporated in countries without adequate AML/CFT controls.

Case study 12: Criminally-controlled securities intermediary

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Canada
Subject:	Individuals, companies
Instruments, methods and techniques:	Wire transfers, bank drafts (i.e. cashier's cheques)
Indicators:	• "Shady" or criminally-associated or criminally-convicted officers, directors and/or major shareholders. One individual was associated with a South American criminal organisation; • Cash was used to pay dividends to investors; • Establishing multiple corporations: one individual was the administrator of several corporations, all located at the same address; • Several transactions between associated and related companies: funds wired to associated entities and then quickly sent outside the group; and • Minimal movement in share price: investment in an entity whose financial statements show no economic activity.

Suspicious transaction/activity report information

In 2004, a MSB reported to the FIU financial transactions that were conducted for the benefit of a securities company operating from a Caribbean country. Two individuals (a husband and a wife) were reported to have used cash to purchase two drafts payable to the securities company. The individuals appeared to be structuring the transactions to fall below the $10,000 reporting threshold.
A foreign FIU, law enforcement agencies in Canada and the United States and a Caribbean newspaper indicated that the securities company was incorporated by a Canadian citizen suspected of being involved in laundering, through stock markets, proceeds of a cocaine trafficking operation which was believed to be controlled by a South American criminal organisation.
According to its website, the Caribbean securities company appeared to be operating worldwide; however information on the management, contact persons, names or phone numbers, and type of services offered, were not provided.

Case description

According to information provided by law enforcement to the FIU:

- intelligence sources suspected that the South American criminal organisation had set up securities companies in the Caribbean and in Canada, and used nominees to run the operations;
- money generated by cocaine trafficking worldwide on behalf of the criminal organisation was deposited in bank accounts in Western Europe in a country known for its bank secrecy as well as in the Caribbean.

In Canada, all methods used to launder the proceeds of cocaine trafficking for the organisation were not known, but one channel used to introduce the drug trafficking money into the system was the purchase of drafts at MSBs payable to the securities company in the Caribbean.
Once in the system (in the Caribbean or in Europe), the drug money was transferred to securities companies in Canada.
Eight securities companies were found to be the beneficiaries of wire transfers totalling approximately US$30,000,000.00 over a period of two years. These EFTs were ordered by the company in the Caribbean from accounts held in Western Europe and the Caribbean. The eight companies were sharing the same address and administered by the same person, who was listed as a lawyer. The suspicious movement of funds between the Caribbean company and the eight securities companies were reported by a number of financial institutions in Canada; examples of suspicious transactions or behaviours include:

- the lawyer did not want to explain the relationship between the two companies and the purposes of the financial transactions from one entity to another;
- a securities company was the beneficiary of an EFT and the lawyer withdrew the full amount in cash and

claimed that the money would be used to pay dividends to investors; and

- after receiving funds from the Caribbean, the eight companies issued cheques, bank drafts or ordered wire transfers payable to entities and other established securities companies in Canada but also in the United States and Asia: after receipt of a wire transfer, one securities company ordered a wire transfer (same amount) to the benefit of an oil and gas company that was operating in South East Asia. According to a database maintained by a non-governmental entity, the beneficiary did not have any assets or liabilities, changed name three times, was a medical equipment supplier, a music video producer and games wholesale distributor, and there was no movement in the share price for five years.

Enforcement actions

The case was referred to law enforcement for investigation.

3.6 Clients and Account Types

Trust, Nominee, and Omnibus Accounts

125. Trust and nominee accounts present ML/TF vulnerabilities in the layering and integration stages. A particular risk involves jurisdictions where the formation of a trust or nominee account does not require the collection of beneficial ownership information for individuals. Moreover, while some jurisdictions may require beneficial ownership information, the information required can be limited to information regarding non-natural persons. As with shell companies, a lack of beneficial ownership information regarding the individuals who benefit from the account may mask an individual's identity such that he or she would gain access to a financial system when such access would otherwise be restricted or forbidden.

126. An omnibus account is an account established for an entity that is acting as an intermediary on behalf of multiple individuals or entities. For example, a bank in jurisdiction X could open an omnibus account with a securities intermediary in jurisdiction Y through which the bank in jurisdiction X manages a portfolio for its clients. In this scenario, the ML/TF vulnerability is that the securities intermediary may not know who the beneficial owners of the investment portfolio are.

127. One jurisdiction reported that "hub and spoke" arrangements involving jointly held accounts posed a particular vulnerability. In these arrangements, the primary accountholder opens accounts with numerous others (secondary accountholders), who in turn open accounts with others (tertiary accountholders). This can give the primary accountholder access to dozens or hundreds of accounts, decreasing transparency and making it difficult for a financial institution to determine exactly who is originating a transaction.

Charitable and Other Non-Profit Organisations

128. Whilst most charitable and non-profit organisations are reputable and provide legitimate services or funding for their causes, some organisations have been and can be used for ML/TF. Although not unique to the securities industry, a particular vulnerability involves organisations that may be used as a front for transferring funds to suspect beneficiaries located in high-risk areas/jurisdictions or conflict zones deemed to harbour or support terrorists. For example, legitimate funds may be used to purchase securities that are donated to a charitable organisation. The charity, in turn, could liquidate the securities or use the income generated by the securities to transfer funds to, or to purchase material for, individuals who further terrorists' activities.

Shell Companies

129. The term "shell company" often refers to a non-publicly traded corporation or limited liability company that might have no physical presence and generates little or no independent economic value. These companies are commonly organised in a way that makes their ownership and transaction information easier to conceal. Thus, transactions involving shell companies present a high ML/TF vulnerability.

130. Whilst publicly traded shell companies can be used for illicit purposes, ML/TF vulnerabilities associated with shell companies are heightened when the company is privately held, such that beneficial ownership can be more readily obscured.

131. For example, a domestic or international shell company securities account can be used to evade CDD/KYC investigations regarding the beneficial owners of certain assets. In particular, individuals or entities in high-risk areas/jurisdictions or conflict zones can disguise their true identities through a series of shell companies located in various jurisdictions to participate in a financial system that they otherwise would not be able to access.

132. Shell companies can also be used to introduce illicit funds into a financial system and/or generate illicit funds through manipulative or fraudulent securities activities. For example, a brokerage account can be opened in the name of shell companies and used to engage in fraudulent conduct with regard to low priced, illiquid, low volume or privately placed securities. In addition, a shell company can be established to accept payments from criminal organisations for non-existent services. These payments, which appear legitimate, can be deposited into depository or brokerage accounts and either wire transferred out of a jurisdiction or used to purchase securities products that are easily transferable or redeemable.

Unregulated Investment Funds and Pools (i.e. Hedge Funds)

133. Generally, hedge funds are vehicles established to hold and manage investment assets. Because of the way they are structured, they may not be subject to regulatory oversight. Hedge funds may receive funds domestically or internationally, and some (feeder funds) are established to invest into other hedge funds. A hedge fund will often utilise the services of a regulated securities intermediary.

134. Hedge funds present an ML/TF vulnerability because the regulated entity that the hedge fund is using to effect transactions (e.g**.** a broker-dealer) may not know the identity of the underlying hedge fund investors. Typically, hedge fund investors are of higher net worth than other retail investors. This anonymity of ownership can also result from the opacity associated with some feeder funds.

135. In addition, some hedge funds may be used to perpetuate a securities fraud, such as a Ponzi scheme. Securities fraud is discussed in Chapter 4.

Suspicious Indicators Associated with Trust, Nominee, and Omnibus Accounts, Charitable Organisations, Shell Companies and Hedge Funds

136. The questionnaire responses did not specifically identify any suspicious indicators associated with trust, nominee, and omnibus accounts, charitable organisations, shell companies and hedge funds. However, the following general suspicious indicators (also appearing in Annex B) may be useful when evaluating risks posed by these types of accounts, organisations and entities:[25]

[25] In addition, the FATF typology entitled "The misuse of corporate vehicles, including trust and company service providers" published in 2006 contains relevant background information.

- During the account opening process, the person opening the account refuses to provide information to complete CDD/KYC (e.g. occupation, prior financial relationships, etc.), in particular with respect to beneficial ownership;

- The person opening the account is reluctant to provide complete information about the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, the entities' officers and directors or business location; and

- The trust or beneficial owner of a nominee account is located in a high-risk area/jurisdiction or conflict zone.

Case study 13: Fictitious transactions involving publicly-traded shell company

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Israel
Subject:	Individuals, companies
Instruments, methods and techniques:	Shell company, third parties

Suspicious transaction/activity report information

The STR indicated that there may have been a violation of the jurisdiction's money laundering law in relation to identifying the beneficial owner of a company.

Case description

The FIU detected a connection between D, a young businessman, and an organised crime group. Person A was active in local politics and owned several businesses. Together with another very wealthy businessman whose source of wealth is unknown, he purchased a public shell company X that traded on the local stock exchange for a small fraction of its true worth. D used a shell bank account managed by the wife of someone related to D. The shares of company X were transferred to several entities, none of which constituted a "party of interest" according to the stock exchange's reporting threshold. Some of the shares were transferred on the same day they were credited to different accounts managed by related parties in what appears to be a fictitious transaction, since the debited account did not receive any funds in return. The owner of the account debited declared there were no beneficiaries. This public company later attempted indirectly to win a government bid regarding a natural resource.

Case study 14: Securities intermediary failed to identify beneficial owners of offshore trust accounts

Offence:	Regulatory violation
Securities Related Designated Offence (if any):	N/A
Jurisdiction:	United States
Subject:	Broker-dealer
Instruments, methods and techniques:	Offshore trusts; wire transfers
Indicators:	• Offshore Trusts; and • Wire Transfers.

Suspicious transaction/activity report information

None

Case description

An SRO found that an introducing broker-dealer failed to obtain beneficial ownership information relating to accounts for high risk offshore trusts, as required by the firm's AML/CFT procedures. The accounts were used in millions of dollars of international wire transfers. In addition, even though the introducing broker-dealer's clearing broker-dealer made repeated requests for information regarding the beneficial ownership of the accounts, the introducing broker-dealer did not obtain this information. It was also unable to analyse the transactions identified by the clearing broker-dealer for suspicious activity because it did not have information identifying the beneficial owners of the accounts.
In addition, the introducing broker-dealer did not have sufficient procedures in place to ensure that there was adequate communication between the firm and its parent corporation, a bank, as to whether, in general, STRs should be filed and whether a particular STR had in fact been filed. Consequently, the firm's processes did not make certain that its independent obligations regarding the filing of an STR were met. The firm was also unable to reliably

incorporate the information that STRs had been filed into an ongoing risk assessment of its customers and to evaluate account activity going forward.

Enforcement actions

The firm was censured and fined US$3 million.

Case study 15: Purchase and sale of shares of a public shell company

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Israel
Subject:	Individual; private company
Instruments, methods and techniques:	Cash deposits, shell company, use of a nominee
Indicators:	• Buying the shares of a shell public company using a bank cheque purchased with cash by a third party; • Reluctance to expose buyers of the shares to the bank; • Shares bought using a straw man (i.e. a front for the true purchaser); • Shares resold after a very short period of time; and • Withdrawing funds from the shell company by means of loans or deals with interested parties, sometimes via MSBs.

Case description

Natural Person N is suspected of buying a public shell company (company A) traded on the stock exchange and hiding his involvement in the company for the purpose of money laundering.

The FIU received an STR regarding N who previously held shares through a “straw man” in two public companies, "B" and "C”. N was suspected by the securities regulator of manipulating the share price in order to artificially push it upwards, and of transferring funds for no apparent legitimate purpose by crediting the accounts of companies B and C by transfers from related private companies and shortly afterwards withdrawing money from the accounts of B and C for no apparent legitimate purpose. Some of the funds were drawn as loans and transferred to MSBs.

In order to purchase company A, N purchased two bank cheques using large amounts of cash: one written to the order of a law firm that was dealing with the acquisition and one written to the order of the public shell company A. N informed the bank that he represented the potential buyers and received the cash from them. He was reluctant to provide any information regarding the "investors".

A week after N purchased the bank cheques, 81% of company A shares were purchased by person M, who is believed to be a "straw man" for person N. Also, 50% of the shares were purchased by person M on behalf of unidentified third parties, none of whom were actually related to the transaction. Three weeks after the acquisition, N's wife was named Secretary of company A. Two months later, the remaining shares were again sold to person O and to another family member of N.

During the first months after the acquisition of the company, several cash deposits (amounting to approximately one million dollars) were made. This was unusual for a company that was a public shell and was not performing any activity until the acquisition. Another pattern followed by firm A was the acquisition of shares of a foreign company whose activity was not related to the alleged activity of company A. Company A lent funds to the foreign company by means of an international transfer and the loan was repaid from an account abroad managed by the foreign company after a short period of time.

Several months after the acquisition, the funds were drawn from the account by different means: Loans to related parties, transfers to MSBs (company A's financial reports showed as an asset on the balance sheet large amounts of money to be paid by factors other than clients).

The company also reported the loss of millions of Israeli Shekels due to an investment in derivatives.

Case Study 16: Use of Omnibus accounts and fictitious account names to facilitate sanctions evasion

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	United States
Subject:	Entity
Instruments, methods and techniques:	Omnibus account/fictitious account names
Indicators:	

Suspicious transaction/activity report information

References to “code names” in transactions processed through an omnibus account of a third country broker maintained at a securities firm in the United States.

Case description

An entity subject to an asset freezing order established an account with a securities firm in a third country. The third country firm agreed to use a fictitious name for the sanctioned party when processing stock trades on its behalf through its omnibus account held with a U.S. broker, thus disguising the identity of the beneficial owner of the stock held in the omnibus account.

Enforcement actions

The case is still being investigated.

Margin Trading

137. One of the unique characteristics of the securities industry is that it can be used to both disguise the proceeds of criminal activity and to generate further profits. The use of margin account trading involves the investor borrowing funds to carry out trading. The securities themselves are used as collateral for the loan. By influencing the timing and value of trades (and leverage), a launderer can potentially use the proceeds of a scheme to generate more funds.

Case study 17: Margin accounts

Offence:	Money laundering
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	Malaysia
Subject:	Individual
Instruments, methods and techniques:	Multiple trading and margin accounts, offsetting trades

Case description

Mr. W opened five trading accounts and two margin accounts at five broker-dealers in various names. These accounts were opened under his name, his mother's name, Mrs. F, his girlfriend's name, Ms. V, and company XYZ, which was owned by Mr. W and Mrs. F. The scheme was carried out on four separate occasions, involving two cycles where the proceeds from the first cycle were used to facilitate the scheme carried out during the second cycle. During the first cycle, Mr. W placed odd lot buy orders using his trading account and Mrs. F's trading account and simultaneously placed odd lot sell orders through another broker-dealer to match the trades, but at exorbitant prices. Mr. W controlled both the selling and the buying parties.
Mr. W then took out the proceeds at the selling brokers and defaulted on the buying brokers' side. This allowed him to raise huge amount of sales proceeds that were used to increase his margin and facilitate his scheme during the second cycle. During the second cycle, the same scheme was used but involved different broker-dealers, where he had used trading accounts of Ms. V and company XYZ.

3.7 Determination of Value

138. Securities traded on exchanges tend to have a reasonable degree of price transparency. However, both on and off-market trades can be used to disguise value, especially where there are no traditional pricing mechanisms, and such trades can be used to transfer value in circumstances which are attractive to a money launderer. For example, a difficult to price instrument can be transferred at a pre-arranged, excessive price in order to transfer value from one person or entity to another.

Transfer Pricing

139. Large capitalisation stocks are subject to a high degree of transparency and, subject to general market forces, generally fluctuate within an established price band. It is noted, however, that the market price on small capitalisation stocks, which may be rarely traded, can be subject to more extreme price movements. In addition, the price of such an illiquid stock may be substantially affected by relatively

small transactions. This mechanism has been exploited for money laundering purposes where block trades of illiquid stocks are transacted at a pre-agreed price between two parties. In such transactions, parties agree to the initial purchase of an illiquid security at an artificially low price with the same security being bought back some time later by the original seller or an associate at a significantly higher price.

140. A variation on this occurs in the derivatives market where OTC derivatives can be structured to meet the requirements of a specific customer. Such transactions may be highly leveraged or arranged so that only a small movement in the value of the underlying securities can trigger disproportionately large payments. Furthermore, the pricing model on a bespoke or custom built derivative may be extremely difficult for anyone, other than a market expert, to understand. Such transactions have frequently been used to transfer profits from high-tax to low-tax jurisdictions and for the purposes of avoiding exchange control regulations.

Case study 18: Money laundering through transfer pricing

Offence:	Money Laundering/Tax evasion
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	U.K.
Subject:	Banking/securities corporation
Instruments, methods and techniques:	Off-market prices on derivative contracts
Indicators	• Unnatural diminution in profits; • Unnecessarily complex transaction structure; and • Subsidiary companies established for no viable economic purpose in a low-tax jurisdiction.

Suspicious transaction/activity report information

No reports were filed at the time but subsequent investigations were undertaken by revenue authorities.

Case description

The investment banking arm of a global investment bank had made substantial profits on its derivative trading book. In order to transfer profits to a low-tax jurisdiction, a special purpose subsidiary company was established in that jurisdiction. A number of complex over-the-counter derivative contracts were entered into between the investment bank and the subsidiary. During the course of the contracts, variation margin payments were made to the subsidiary on each "revaluation" of the contract and a substantial loss was realised on liquidation of the contract.

Enforcement actions

Investigations by revenue authorities proved inconclusive due to the complexity of the transactions.

Short selling

141. In the securities industry short selling generally involves the practice of selling securities that are not actually owned by the seller, or that will be borrowed for delivery. In a "naked" short sale, the seller does not borrow or arrange to borrow the securities in time to make delivery to the buyer within the standard settlement period. The investment strategy behind short selling is the hope that a profit will be made from the difference in price of the assets sold and those purchased (at a lower price) for return to the borrower.

142. Short selling is a trading vehicle that can be linked to market manipulation or insider trading, which are both predicate offences that could be the basis for ML/TF. One example cited involves "PIPES", or private investment in public equities. A financial institution may solicit indications of interest from potential purchasers before committing to the deal. While potential investors are forbidden from trading on the information about the transaction, some disregard the prohibition and sell the associated public equity short, anticipating a price decline.

3.8 Rogue Employees

143. While most AML/CFT regimes are designed to detect and report suspicion surrounding customer interactions, these programs are only as reliable as the people who implement them. To this extent, employees who assist customers in money laundering, terrorist finance may, and/or in predicate offences, pose a serious vulnerability to a financial institution.

Suspicious Indicators Associated with Rogue Employees

144. A number of jurisdictions identified the following as suspicious indicators that may be associated with employees vulnerable to assisting money launderers or terrorist financiers. These indicators are not necessarily unique to the securities industry or indicative of employee misconduct, but rather should be taken into account with other indicators:

- The employee appears to be enjoying a lavish lifestyle inconsistent with his or her salary or position;
- The employee is reluctant to take a holiday or vacation;
- The employee is subject to intense job-related demands, such as sales or production goals, that may make him more willing to engage in or overlook behaviour that poses ML/TF risks;
- The employee puts a high level of activity into one customer account even though the customer's account is relatively unimportant to the organisation;
- The employee is known to be experiencing a difficult personal situation, financial or other;
- The employee has the authority to arrange and process customer affairs without supervision or involvement of colleagues;
- The management/reporting structure of the financial institution allows an employee to have a large amount of autonomy without direct control over his activities;
- The employee is located in a different country than his direct line of management, and supervision is only carried out remotely;
- A management culture within the financial institution focuses on financial reward over compliance with regulatory requirements;
- The employee's supporting documentation for customers' accounts or orders is incomplete or missing; and
- Business is experiencing a period of high staff turnover or is going through significant structural changes.

Case study 19: Employee of a securities intermediary assisting a politically exposed person (PEP) launder money

Offence:	Drug Trafficking, Bribery
Securities Related Designated Offence (if any):	N/A
Jurisdiction:	United States
Subject:	Individuals
Instruments, methods and techniques:	Stock brokerage accounts, wire transfers, foreign shell companies
Indicators:	• PEP • Widespread news accounts regarding investigation of the PEP; • Foreign wire transfers; and • Shell companies.

Suspicious transaction/activity report information

None Indicated.

Case description

D, an investment representative at a large broker-dealer, helped a PEP from a foreign jurisdiction launder over US$10 million that the PEP received from drug traffickers. The PEP received these illicit assets as payment for allowing drug shipments to safely pass through his jurisdiction. D helped the PEP establish numerous brokerage accounts at her firm in the name of various foreign shell companies and then deposited the illicit assets into these accounts. Weeks before the PEP was to lose prosecution immunity, D assisted the PEP in wire transferring the illicit assets out of the brokerage account and into a foreign account. D then set up a fictitious account for the PEP and wire transferred all of the assets back to her firm.

Enforcement actions

D was criminally indicted.

Case study 20: Use of "friendly" broker to deposit funds and conduct stock market transactions

Offence:	Money laundering
Securities Related Predicate Offence (if any):	
Jurisdiction:	Brazil
Subject:	Individual
Instruments, methods and techniques:	Use of multiple accounts
Indicators:	N/A

Suspicious transaction/activity report information

None indicated.

Case description

A businessman, M, wishes to "pay" another businessman J for "rendered services" without any apparent business relationship between them. M is a friend of N and a broker with "Stocks & Co". M continuously deposits money of unknown origin into N's current account with the broker.
N keeps these deposits of money segregated from his own. These deposits are used in transactions carried out on the stock exchange without regard to profit or loss. In time, N made deposits of small amounts of money of unknown origin into several bank accounts belonging to J.
M, N, and J apparently believed that this procedure would minimise the possibility of detecting a link between the origin of the amounts "paid" by M to J. The jurisdiction observes that the securities account was being used to hide the origin of the money that was deposited in J´s bank accounts.

Enforcement actions

The two brokers involved were subject to an administrative penalty by the securities commission, as were the directors of the brokers, for failing to file STRs.

Case study 21: Employee of a securities intermediary assisting in market manipulation

Offence:	N/A
Securities Related Designated Offence (if any):	Market manipulation; securities fraud
Jurisdiction:	United States
Subject:	Individuals
Instruments, methods and techniques:	Stock brokerage accounts; penny stocks; wash trades, shell companies
Indicators:	• Accumulation of stock in small increments throughout trading day to increase price; • Marking the closing price; • Unauthorised buying of stock through customer accounts; • Account activity not consistent with customer profile; and • Trading between numerous accounts controlled by the same people.

Suspicious transaction/activity report information

No STRs were filed. Securities intermediary faced liability for ignoring red flags and suspicious indicators and for failing to supervise a problem employee despite warning from compliance officers.

Case description

RR1, a customer and RR2 from another firm participated in scheme to manipulate the stock of a thinly traded security. They artificially inflated and maintained the price for the stock, marked the closing price, engaged in matched and wash trades, attempted to artificially create "downbids" to suppress short sales, and engaged in unauthorised and unsuitable trading in customer accounts. Certain senior executives allowed RR to operate with greater freedom than other RRs. The securities intermediary that RR2 worked for was aware of numerous red flags and suspicious indicators regarding the market manipulation but did not file an STR.

Enforcement actions

A cease and desist order was filed against the firm and the firms was required to pay disgorgement.

3.9 Terrorist Financing

145. The replies to the questionnaire and the case studies gathered suggest that there is relatively little evidence of the securities industry being used to finance terrorism.

146. However, this lack of evidence specific to the securities industry does not rule out the potential for terrorist financing in this sector.

147. Following the 9/11 attacks in the United States, various agencies worldwide engaged in studies to ascertain which sectors of the financial services industry had been used to finance the attacks. No empirical evidence was revealed to suggest that securities had been used either to finance the attacks or to generate funding from them (for example, through short selling of airline or hotel stocks).

148. The lack of information on terrorist financing in this sector might, in part, be explained by the relative newness of the provisions on terrorist financing compared with those relating to money laundering. The 8 (now 9) FATF Special Recommendations came into effect in October 2001, and the effect of them in an industry which, in itself, is expanding quickly, may not have been fully felt.

149. The information provided in Section 3.6, above, dealing with clients and account types details some of the TF threats in this and other sectors.

150. Specific indicators relating to the securities industry were not cited, but more common ones which are potentially relevant to this industry are found in the FATF typology on Terrorist Financing. [26]

[26] http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf

CHAPTER 4:
PREDICATE OFFENCES FOR MONEY LAUNDERING LINKED TO SECURITIES

4.1 Introduction

151. As previously mentioned, the securities industry is not only a vehicle through which illicit assets can be laundered; it is also vehicle for generating illicit assets that would eventually have to be laundered. Indeed, the FATF's definition of the "designated offences" that lead to money laundering include three securities-specific offences: insider trading, market manipulation, and fraud.

152. This section addresses these three securities-specific designated offences because: (1) a significant number of jurisdictions included these designated offences in their questionnaire responses; (2) the relatively low level of securities related STRs may be the result of the non-reporting of these offences;[27] and (3) in identifying and reporting these types of offences, jurisdictions may be in a position to better prevent money laundering.

153. This chapter is organised into topical sections that address each of the three designated offences that implicate the securities industry. Suspicious indicators and case studies are also included.

4.2 Insider trading

154. Although insider trading is illegal conduct, this does not mean that company insiders, such as officers, directors and employees, can never trade shares of the company's securities. In some jurisdictions, certain circumstances require such transactions to be reported to regulators and the public. Insider trading, however, involves situations where the person who buys and sells securities, whether a company insider or not, does so in violation of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. In some jurisdictions, this includes situations where a person in possession of material, non-public information provides this information to someone else for trading where, depending on the circumstances, the recipient of the information can violate insider trading laws as well.

155. Insider trading is unique to the securities industry and generates illicit assets. As a predicate offence for money laundering, and an offence in its own right, this type of misconduct is reportable on STRs and has proven useful in assisting law enforcement and regulators prosecute such misconduct.

156. The illicit assets generated by insider trading can be laundered through the securities industry itself or through other parts of the financial sector. The most common example of laundering would be the simple transfer of illicit proceeds to a bank account.

Suspicious Indicators Associated with Insider Trading

157. The following were identified as suspicious indicators that could implicate insider trading:

- The customer makes a large purchase or sale of a security, or option on a security, shortly before news is issued that affects the price of the security;

[27] This may also result from a perception that these securities-specific designated offences are not money laundering per se.

- The customer is known to have friends or family who work at or for the securities issuer;
- The customer lives in the locality where the issuer is located;
- The customer's purchase does not correspond to his or her investment profile. For example, the customer may never have invested in equity securities, but does so at an opportune time;
- The customer's account is opened or significantly funded shortly before a purchase; and
- The customer sells his or her position in a security in conjunction with a significant announcement about the security.

Case study 22: Insider trading and money laundering

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Insider trading
Jurisdiction:	Belgium
Subject:	Individual, companies
Instruments, methods and techniques:	Shares, affiliated companies
Indicators:	• Unusual important transactions; • Suspicion of insider trading; and • Securities sold a few months later.

Suspicious transaction/activity report information

In 2004, a Belgian bank reported several unusual important purchases of shares of two Belgian quoted companies, belonging to the same group, by company Y represented by Mr. X and a third party also in relation with company Y. Mr. X was manager in the two Belgian quoted companies, but also managed company Y.

Case description

Mr. X, manager of an important group of companies, knew that a reorganisation of the group was going to be publicly announced. This could have a favourable effect on the share price of two companies of this group after the reorganisation was announced.
Mr. X used this knowledge to purchase securities of these two companies through another company he managed and through a third party before the reorganisation was announced.
Once the reorganisation was announced, the share price of these two companies rose sharply. The shares were sold at a high profit.
The profit made by Mr. X was then invested in other securities and part of the money was transferred to other bank accounts held by him. As such, the money obtained illegally (thanks to the insider trading) was laundered.

Enforcement actions

The case was disclosed in 2005 to the public prosecutor for ML for insider trading.

Case study 23: Insider trading and money laundering

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Insider trading
Jurisdiction:	Belgium
Subject:	Individuals
Instruments, methods and techniques:	Shares, use of a nominee
Indicators:	• Unusual transaction; and • Purchases do not correspond to the customer's investment profile.

Suspicious transaction/activity report information

A Belgian bank reported that a significant purchase of shares of company M was carried out through the bank account of Mr. Y's wife. The transaction was unusual.

Case description

Mr. Y had insider information on company M, quoted on the stock exchange. Through relatives, he knew that company M would soon be acquired.
To avoid attracting attention, he transferred his assets to his wife's account over which he had power of attorney, and purchased shares of company M prior to the announcement of the takeover. The bank knew that Mr. Y's spouse did not usually perform stock exchange transactions and was surprised to find out that funds were transferred from her husband's account. It is believed that Mr. Y's wife carried out the transactions on his behalf and tried to conceal the transactions by using her account.
After the takeover, his wife's account was credited with the proceeds of the securities sold.
Mr. Y then laundered the money by having the funds transferred to his personal account.

Enforcement actions

The case was disclosed in 2006 to the public prosecutor for ML for insider trading.

4.3 Market Manipulation

158. Market manipulation generally refers to conduct that is intended to deceive investors by controlling or artificially affecting the market for a security. In particular, the manipulator's purpose is to drive the price of a security up or down in order to profit from price differentials. There are a number of methods that manipulators use to achieve these results.

159. The most pervasive market manipulation method involves what is colloquially referred to as a "pump-and-dump" scheme. This scheme involves touting a company's stock with false or misleading statements, often in conjunction with securities trades that raise the price of the security or make it appear as if the securities trading volume is higher than it actually is. Therefore the security price is artificially raised ("pumped"); the security is then sold ("dumped") for a profit. Often the underlying security is low priced, illiquid, and trades with little volume.

Penny Stock Manipulations

160. Penny stocks may represent equity interests in companies that are about to become public or that are already public. The issuers of these shares often, but not always, have legitimate business operations and revenue streams. Shares in these issuers may take the form of physical securities that can be deposited with a securities intermediary. Penny stocks are not likely to be traded on traditional exchanges, but in OTC markets or on bulletin boards. Penny stocks typically have very low trading volumes but, unlike bearer securities, ownership of these shares will often be registered with the issuer or a transfer agent.

161. Illicit actors can acquire penny stocks in several ways. They can purchase already issued penny stocks in the OTC markets, acquire large blocks of shares as compensation for bringing a company public e.g. through a reverse merger into a private shell company, or issue the shares. These shares, which usually have little or no value, can then be deposited into brokerage accounts. Fraudulent promotion

methods and wash trades may then be used to inflate the price of the security. After the manipulators exit the market, investors are often left with worthless securities. Penny stock pump-and-dump schemes have increasingly been conducted through internet-based accounts and through trading accounts held in the name of private shell companies.

Suspicious Indicators for Market Manipulation

162. The following have been identified as suspicious indicators involving market manipulation in general and penny stock pump-and-dump schemes in particular:

- The customer engages in large or repeated trading in securities that are illiquid, low priced or difficult to price;
- The issuing company has no apparent business, revenues or products;
- The issuing company has experienced frequent or continuous changes in its business structure and/or undergoes frequent material changes in its business strategy or line of business;
- The officers or insiders of the issuing company are associated with other low priced, illiquid or low volume companies;
- The officers or insiders of the issuing company have a history of regulatory violations;
- The issuing company has failed to make required regulatory disclosures;
- The issuing company has been the subject of a prior trading suspension;
- A customer's transactions show a pattern of receiving physical securities or receiving incoming shares transfers that are then sold, with the proceeds wired out of the account;
- The customer deposits physical securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares;
- One party purchases securities at a high price and then sells them at a considerable loss to another party;
- A customer journals securities between unrelated accounts for no apparent business reason; and
- A customer engages in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low priced securities.

Case study 24: Stock price manipulation

Securities Related Predicate Offence (if any):	Embezzlement Market manipulation
Jurisdiction:	Korea
Subject:	Individuals
Instruments, methods and techniques:	Shares, funds transfers, multiple securities accounts
Indicators:	• Unusually large transactions; and • Repeated purchase and sale of shares.

Suspicious transaction/activity report information

According to an STR, person A had frequent large fund transactions with unspecified persons, including B and C, and securities accounts at three brokers. In light of repeated selling and buying of shares of U Co. Ltd in large volumes through a certain computer IP, it was suspected that A was manipulating the market price using embezzled money and a borrowed bank account using an assumed name.

Case description

Analysis revealed that B, a company director of U Co. Ltd, embezzled corporate funds deposited as payment for shares and was manipulating the market price using a securities account in the name of unspecified persons with the embezzled funds.
The executives, including the former representative director and the present representative director of U Co. Ltd and a former branch manager of the broker, conspired to manipulate the share price more than 10 times through false stock trading orders and wash sales with embezzled money and gained illegal proceeds worth 35 billion won. As a result, private investors were severely damaged. It is of significance that relevant crimes were detected and further damage was prevented because an STR was sent to law enforcement authorities.

Enforcement actions

B was prosecuted for violation of the Securities Exchange Act and bribery (sentenced to 2 years of imprisonment, stay of execution for 4 years at the first trial). C was prosecuted for violation of the Act on the Aggravated Punishment, Etc. of Specific Economic Crimes (Embezzlement and Breach of Trust) and the Act on External Audit of Stock Companies (sentenced to 5 years imprisonment and a fine of 2 billion won). Other related persons were also prosecuted.

Case study 25: Market manipulation involving the use of private shell companies

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Market manipulation
Jurisdiction:	United States
Subject:	Individuals
Instruments, methods and techniques:	Stock brokerage accounts; penny stocks; wash trades, false promotional methods; foreign accounts
Indicators:	• Individuals subject to previous securities related injunctions; • False and misleading disclosure documents; and • Brokerage accounts opened using private shell companies.

Suspicious transaction/activity report information

N/A

Case description

Individuals, some of whom were previously subject to securities misconduct injunctions, conspired to acquire controlling interests in a public company trading on the OTC markets. In perpetuating the conspiracy, the individuals acquired restricted stock of the companies and used fabricated and backdated corporate records that made it appear as if the restricted stock certificates had satisfied minimum holdings periods. The individuals then used false attorney opinion letters to get the transfer agents to issue freely tradable shares. Thereafter, the individuals prepared and distributed false and misleading disclosure documents for the companies and engaged in promotional campaigns to create demand. The individuals used brokerage accounts opened through private shell companies to sell shares of the companies in conjunction with the promotional campaigns.

Enforcement actions

N/A

Case study 26: Securities intermediary expelled for inadequate AML/CFT policies and procedures

Offence:	Regulatory violation
Securities Related Predicate Offence (if any):	N/A
Jurisdiction:	United States
Subject:	Broker-dealer
Instruments, methods and techniques:	Penny stocks; wire transfers; journaling
Indicators:	• Stock Promoters; • Penny Stocks; • Customers with money laundering convictions and regulatory actions against them; • Wire transfers to well known tax havens; and • Journaling of securities between accounts followed by immediate liquidation.

Suspicious transaction/activity report information

N/A

Case description

A broker-dealer agreed to an expulsion from SRO membership for systematic and repeated violations of AML/CFT rules and regulations, including failure to investigate and report numerous suspicious transactions.
The SRO found that, at various times from February 2004 to September 2006, the broker-dealer's customers included notorious stock promoters and others who had been barred by the SRO, disciplined by the country's primary securities regulator, or had criminal histories, including one customer who had been convicted for the sale of an illegal controlled substance and money laundering. The same individual had been previously convicted for his role in a "smurfing" scheme, a commonly-used money laundering technique involving the splitting of a large financial transaction into smaller transactions to avoid scrutiny by regulators and law enforcement.
The SRO further found that in at least a dozen instances, the broker-dealer's customers sold large blocks of penny stocks that were linked to allegedly fraudulent schemes. The country's securities regulator had filed at least two enforcement actions charging federal securities law violations involving penny stocks that were later sold through the broker-dealer and other firms. In one instance, an individual who had previously been barred by the SRO delivered over 1.8 billion shares of a penny stock issued by a company that was contemporaneously the subject of a pending, and publicly released, complaint by the securities regulator alleging manipulation and other securities laws violations. In the following 10-month period, this customer sold the shares for approximately US$8 million in 155 separate sales, wiring the proceeds out of his account after each sale.

Enforcement actions

The broker-dealer agreed to an expulsion from SRO membership.

4.4 Securities Fraud

163. Securities fraud broadly refers to deceptive practices in connection with the offer and sale of securities. In this regard, securities fraud encompasses insider trading and market manipulation.

164. For example, illicit actors can engage in confidence or boiler room schemes the structure of which would make the scheme a "security" for the purposes of a jurisdiction's securities laws. However, the actual sellers of these (mostly worthless) shares are often based in a separate country from the purchaser, making access to perpetrators of the fraud difficult.

165. In a Ponzi scheme, a fraudster lures investors with the promise of high returns that are to be generated through the investment or business efforts of the fraudster. Instead of generating actual profits, the fraudster creates the illusion of profits by paying investors returns from their original investment or paying returns from the money that new investors contribute to the fraud. This type of scheme tends to collapse when the number of new investments into the scheme do not satisfy the payment obligations for previous investors.

166. Although many Ponzi schemes do not necessarily involve the direct use of securities intermediaries or markets, the way these schemes are marketed often causes sales of interests in the scheme to be classified as securities, and thus subject to the jurisdiction of securities regulators.

Securities Offering Fraud Indicators

167. The following have been identified as suspicious indicators associated with a securities offering fraud:

- The customer opens numerous accounts for different legal entities that the customer controls;
- The customer receives many incoming cheques or wire transfers from unrelated third parties;
- The customer allocates incoming third-party deposits among numerous accounts;
- The customer makes numerous outgoing payments to third parties close in time to when the customer receives many incoming third-party cheques or wire transfers;
- The customer's profile does not suggest a legitimate business reason for receiving many third party deposits; and
- The cheques or wire transfers note that the funds are for an investment.

Case Study 27: Securities fraud

Offence:	Money laundering
Securities Related Predicate Offence (if any):	Securities fraud
Jurisdiction:	United States
Subject:	Individual
Instruments, methods and techniques:	Cheques, wire transfers, monetary transactions
Indicators:	• D established various businesses and bank accounts under his name; • Monetary transfers between various bank accounts controlled by D (or D's businesses); • Authorities had imposed cease and desist order against D and D's business; • D promised substantial guaranteed returns and secure principal investment; and • Deposited investment monies into bank account controlled by D.

Case description

The individual generated illicit assets within the securities industry by operating two Ponzi schemes. Under the first scheme, D told investors that their money would be used to purchase equipment that would be leased and resold. Under the second scheme, D sold promissory notes that were purportedly secured by stock in D's associated legal entity and by precious metal production contracts. Both schemes promised investors high rates of return and guaranteed the principal investment. In actuality, the defendant used investor funds for his personal expenses.
Investors would either wire, hand deliver or mail their investments (via cheques) to D or one of his businesses (legal entities) and the funds were deposited into bank accounts controlled by D. D would then transfer the funds among various bank accounts that he controlled in order to disguise the origin of the proceeds and to further perpetuate the fraud. After receiving the funds, D would use them to pay for personal expenses, promote another business, and to make periodic payments to investors. The periodic payments to investors were made to legitimise and disguise the underlying schemes and to avoid reporting to and detection by law enforcement.

Enforcement actions

A U.S. state investigated the investments offered by D under the first program, and issued an order against D and his related business to cease and refrain from further offer or sale of such investments in the state.
A federal action has been filed against D alleging violations of federal laws related to mail fraud, securities fraud, and money laundering.

CHAPTER 5: SUSPICIOUS TRANSACTION REPORTING AND ENFORCEMENT ACTIONS

5.1 Suspicious Transaction Reports

168. A review of the published STR reporting figures from some of the Third Round Mutual Evaluation Reports suggests that STR reporting in the securities industry is relatively low, compared with the banking industry. A selection of comparative statistics is set out below:

Country A

Financial Institution	2001	2002	2003	2004
Banks	911	1 128	1212	1 698
Money Exchange	21	28	199	330
Securities	**24**	**4**	**3**	**3**

Country B

Financial Institution	2002	2003	2004	2005
Banks	680	549	685	921
Money Exchange	102	106	39	20
Securities	**10**	**12**	**3**	**5**

Country C

Financial Institution	2002	2003	2004	2005
Banks	193	177	288	349
Money Exchange	0	0	0	0
Securities	**0**	**0**	**1**	**1**

Country D

Financial Institution	2002	2003	2004	2005
Banks	272 823	288 343	381 671	522 655
Money Exchange	5 723	209 512	269 284	383 567
Securities	**0**	**4 267**	**5 705**	**6 936**

169. The STR reporting disparity between the banking and securities industries is not surprising in light of the relative size of the banking industry in most countries compared to the securities industry. In addition, in some countries STR reporting in the securities industry is a newer legal requirement than that for submitting STRs in relation to banking activities. Nevertheless, the figures might be indicative of under-reporting in the industry, and it is suggested that the issue be examined further.

170. It is also worth nothing that some jurisdiction's reporting requirements are narrower than others', which results in the inconsistent capture of data for the same event or activity.

171. The securities typology questionnaire (see Annex D) requested information on the amount and nature of the STRs received in the securities sector. Of the 40 questionnaire responses received, 31 provided responsive data.

172. In contrast, a number of jurisdictions reported that their STR tracking and/or reporting mechanisms were not conducive to quantitative breakdowns regarding the number of securities related

STRs filed. This appears to be a reporting gap, in that data is simply not available in certain jurisdictions to enable an assessment of the potential risks in the sector.

173. One FIU reported that STRs were categorised based on the institution making the filing. Accordingly, figures for the securities business of larger banking groups are potentially being categorised as banking STRs.

Number of Securities Related STRs

174. Questionnaire responses represent the number of securities related STRs filed between 2005 and 2008 (see the summary at Annex C, Table 1). Of significance, most jurisdictions evidenced yearly increases in securities related STRs between 2005 and 2008, with a particular increase in 2007. It should be noted that most questionnaires were submitted in late 2008, making final 2008 figures unavailable for some respondents.

Breakdown of STRs Based on Type of Security

175. Fourteen of the forty questionnaire responses provided a breakdown of STRs filed by securities type. The most common type of securities product subject to an STR filing were equities, mutual funds, money market mutual funds, bonds and similar debt instruments, foreign exchange contracts, and certificates of deposit. It should be noted that not all jurisdictions consider certificates of deposit and foreign exchange contracts to be securities. Furthermore, with reference to the type of product referenced in an STR, some jurisdictions permit the designation of "any other." This may mean that the suspicious activity was related to the securities markets, even though the STR did not explicitly identify it as such.

STRs Filed By Type of Institution

176. The overall trend for STR reporting was upwards in all areas, with broker-dealers submitting the most. It is not clear if there is any incidence of double reporting amongst institutions.

Emerging Issues

177. Discussions with representatives of FIUs, law enforcement and the private sector suggest that there is a need for greater understanding of the expectations of all parties who file STRs. Reports of poor quality are often thought to hamper enforcement action. This phenomenon is not peculiar to the securities industry, and is one which greater dialogue between the competent authorities and the private sector might help to resolve. Guidance and feedback to those required to report suspicious transactions is part of the package of measures that competent authorities should provide under the FATF Recommendations.

178. Conversely, there is often a perception that the products and methodologies used in the securities industry are extremely complex. This, in turn requires specialist knowledge, which relatively few FIUs and law enforcement agencies currently have.

179. The complexity of the products and methodologies, coupled with the ability to move funds/value internationally also gives rise to practical considerations as to how best to bring actions to seize and freeze criminal assets. Again, mechanisms to share expertise between agencies and jurisdictions are to be encouraged.

180. In some jurisdictions a separate reporting regime exists for suspicions of money laundering and those of the predicate offences where the securities market can be used, such as insider trading and market manipulation. Under these circumstances, it is not always clear that the reporting institution is aware of the possibility that there might also be a requirement to report a suspicion of money laundering. This is a

potential gap in the system, and might partially explain the relatively low levels of ML/TF STR reporting in the securities sector. Again, greater awareness between competent authorities and amongst the industry is to be encouraged.

STR Referrals to Law Enforcement

181. The questionnaire responses did not give uniform results, and thus the trends, rather than the figures, are reported here.

182. The number of reported STR referrals to law enforcement, and subsequent criminal prosecutions remain relatively low. Due to the dual nature of STR reporting for ML/TF cases and predicate offences, such as insider trading and market manipulation in some jurisdictions, conclusion trends on numbers are difficult to determine.

5.2 Enforcement actions

Referrals from the FIU made to Law Enforcement

183. Out of 31 countries that reported receiving STRs involving securities, 18 reported referrals to law enforcement based on these STRs. The number of referrals in specific countries generally represents a small fraction of the number of STRs (less than 10%). Only 7 countries reported money laundering prosecutions in respect to these referrals and 3 reported convictions. It should be noted however, that a number of countries reported that statistics associating prosecutions and convictions to specific STRs or sectors were not available.

184. Eighteen countries reported no enforcement action from 2005 to 2008, either because none were taken in the securities sector or because data was unavailable.

185. Among the 21 countries that reported at least one action in that period, the large majority reported regulatory actions (i.e. actions against financial institutions or intermediaries that failed to comply with their AML obligations, including AML program requirements, CDD and reporting); five countries reported at least one criminal enforcement action (i.e. actions for criminal violations using the securities sector), and one reported joint regulatory/criminal enforcement actions.

186. Most countries noted that the enforcement actions provided no information on areas of high risk or vulnerability in the securities sector, since the action related to deficiencies in AML procedures. However, the following vulnerabilities were noted:

- Fictitious companies;
- Off market trading under conditions that were not “at arms length”;
- Trading in penny stocks;
- Trading in thinly-traded or illiquid shares; and
- Wire transfers.

CHAPTER 6:
CONCLUSION AND RECOMMENDATIONS FOR FURTHER WORK

6.1 General

187. The primary goal of this study was to consider and raise awareness of the vulnerability of the securities industry to money laundering and terrorist financing. With the help of the jurisdictions and international organisations that participated in the typology, a comprehensive set of red flags and indicators and relevant case studies have been gathered for the first time in a global study.

188. Such a study is, by its very nature, limited by the number of practical examples that have been experienced by the participants, and some threats remain theoretical rather than actual. However, in an industry which, by its very nature, facilitates the movement and investment of funds worldwide into an ever-changing array of products, often very rapidly, knowledge of the threats goes some way to raising awareness of the potential issues.

189. In a dynamic environment, the risks will evolve, and the project team hopes that this study will form the catalyst for further work on this topic by industry organisations, supervisory bodies and law enforcement. In particular, further cooperation in endeavouring to understand the risks and methodologies involved in a complex and fast-moving environment would enhance the effectiveness of the global effort to fight ML/TF.

190. In countries with less developed securities markets, some of the typologies and indicators might not currently be readily recognisable. However, given the rapid expansion of the securities industry globally in the past 25 years, it is hoped that the information provided will be of use as markets in developing economies expand.

6.2 Terrorist Financing

191. Although the literature review and the responses to the questionnaire do not readily suggest that the securities industry lends itself to terrorist financing, it remains a serious risk. In particular, the possibility that the use of opaque corporate structures and/or charities, combined with the transfer of value via securities and transactions at securities firms is a potential vulnerability. In addition, the FATF Special Recommendations relating to terrorist financing are newer than those for money laundering, and thus further trends may become apparent as suspicious transaction reporting regimes mature.

6.3 Money Laundering

192. Case studies and other intelligence gathered for this report show that the use of the securities industry to launder money constitutes an actual threat. The industry itself can be uniquely used to generate illicit proceeds from proceeds which might have had a legitimate origin. These illicit proceeds lead to almost "automatic" laundering when they are realised. This phenomenon can be contrasted with the more traditional use of the securities sector to disguise the origin of illicit funds derived from outside the sector.

193. As defences in areas more traditionally associated with ML/TF, such as banking, are tightened, the use of the securities industry may become a greater temptation to those seeking to disguise illicit proceeds, or indeed to generate them.

194. The use of cash in the securities industry does not appear to be widespread, and funds are very often introduced via other regulated sectors. Whilst reliance on other parts of the financial sector to

conduct certain aspects of CDD can be a perfectly acceptable way to facilitate transactions in the global financial system, it is important that the industry and its regulators take appropriate steps to ensure that reliance is only placed on third parties with adequate AML/CFT systems and controls. CDD itself is more than just customer identification, and ascertaining the purpose and intended nature of a transaction with funds from another part of the financial sector remains an important consideration.

6.4 STRs, Law Enforcement and Co-operation

195. The recorded figures for STRs in the securities industry suggest that reporting in this area remains relatively low. Comparisons with the banking sector do not provide much in the way of conclusive findings, given the difference in size between the relative sectors in most countries.

196. There is no one factor behind the relatively low figures for STR reporting, but the following appear to play a part:

- The reporting requirement for securities has only been relatively recently introduced in some jurisdictions;
- The separate reporting requirements for insider trading, market manipulation and securities fraud in some jurisdictions might mean that ML STRs are not being submitted to the FIU;
- Most securities intermediaries do not accept cash;
- The definition of "security" is not consistent;
- Securities in some jurisdictions can be sold by participants in other industries, such as banking and insurance companies;
- Because the securities markets are fast paced and transaction times are of critical importance, intermediaries are required to act quickly on a client's behalf, thus potentially affecting an intermediary's ability (and perhaps inclination) to scrutinise and submit STRs;
- Some in the industry may not understand STR requirements; and
- There may be a perception that the securities industry is not attractive to those wanting to launder money/finance terrorism.

197. The relative lack of referrals of STRs to law enforcement and the corresponding figures for securities-related criminal money laundering cases globally raises several issues.

198. Law enforcement in some jurisdictions report that STRs received from the securities sector do not contain a sufficient level of detail to enable them to take further action. Conversely, the products and schemes used within the industry are often complex and require specialist expertise to understand the full nature of the flows of funds. In addition, the global nature of the securities industry makes the ability to trace and seize assets more complex than more tangible domestically based assets.

199. Several of the case studies presented in this report suggest that the indicators of predicate offences such as securities fraud or market manipulations are similar to those for money laundering and that the transactions involved in both categories are closely linked, if not the same.

200. Liaison between law enforcement, regulators, FIUs, and the industry is to be encouraged, as each has relevant experience which can increase awareness of the vulnerabilities in this sector. In particular, obtaining direct private sector input and feedback in developing case studies is essential to ensure they are useful tools to the industry.

6.5 Definitions

201. This study has not attempted to produce a global standard definition of "security". It is, however, clear from the questionnaire responses that a variety of terms are used worldwide to match the financial activities specified in the FATF glossary. This might give rise to some overlap or even gaps where different regulatory authorities have responsibility for traditional activities thought to fall within the banking or securities sectors.

202. In addition, several jurisdictions note that securities products are traded by participants in other markets, such as banking, and products traditionally seen as insurance-related are in turn traded by those in the banking or securities markets, because they contain an investment element. Co-operation between the competent authorities responsible for each core sector is to be encouraged to address any potential vulnerabilities.

6.6 Issues for consideration

Securities and the "financial institution" category

203. The definition of the financial institutions in the FATF standards is broad and encompasses a variety of financial sectors, including banks, credit unions, insurance, and securities broker-dealers. Given the overlap among these sectors, it may be impractical to effectively establish mutually exclusive categories applicable to each sector in the 40+9 Recommendations and the Methodology. Nonetheless, representatives of the securities industry consulted during the development of this report have noted that they do not fully recognised themselves in the term "financial institution", which they tend to associate with the banking sector. In the future, consideration could therefore be given, when practical, to producing securities-specific material or sections in FATF documents (e.g., best practices paper or interpretative notes).

Scope of "financial institution" definition

204. This report refers to a broad range of products and intermediaries that may not be fully captured under the FATF standards. The recent financial crisis has brought the world's attention to certain products and areas where a lack of regulation has been cited as one of the causes of the turmoil. It is suggested that the FATF keep the definition of "financial institution" under review, to ensure that all products and intermediaries are captured.

RBA Guidance

205. Unlike DNFBPs, MSBs and life insurers, the securities sector has not been the object of a risk-based approach (RBA) guidance document by the FATF. Given the particular complexity of securities products, and continuing difficulties for the sector in identifying money laundering, they may be merit for the FATF in producing such guidance.

CDD/reliance

206. There are a number of synergies between the securities industry and other parts of the financial services industry. In particular, this report notes a trend to rely on customer due diligence information

gathered from the banking sector which is then relied upon to fulfilling the CDD/KYC obligations of the securities industry. This is an area which would benefit from further investigation, possibly in the context of more general work being undertaken in relation to FATF Recommendation 9.

Sector/product specific vulnerabilities

207. Whilst foreign exchange trading is an activity covered by the FATF definition of activities conducted by a "financial institution", it remains somewhat unclear what the ML/TF risks are, and there appears to be scope for some cross-over between the securities and banking sectors. Further work to clarify the risks and identify any potential gaps in supervisory responsibility would be beneficial.

208. Similarly, some securities products, most notably those with insurance elements, involve synergies within the insurance industry. It is recommended that further work (possibly work looking at the insurance industry) be undertaken to look at any potential specific risks in this sector.

209. Whilst several ML/TF vulnerabilities associated with derivatives were identified in this report, further work, perhaps involving the private sector, could address this issue in greater depth.

Suspicious transaction reporting

210. The categorisation of suspicious transaction reports by some FIUs means that some STRs relating to the securities industry are being categorised in a way that may not fully capture the full picture of the risks in this area. It is recommended that thought be given to further work to improve the categorisation of STRs, where this is necessary.

REFERENCES AND BIBLIOGRAHY

Typologies

- FATF (2003), *Report on Money Laundering Typologies 2002-2003*, www.fatf-gafi.org/dataoecd/19/11/33624379.pdf.
- MONEYVAL(2008), *Typology Research, Use of Securities in Money Laundering Schemes*, www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2008)24Reptyp_securities.pdf.
- APG (2009), *Yearly Typologies Report 2009*, www.apgml.org/documents/docs/6/APG%20Typologies%20Report%202009.pdf.

International Guidance and Best Practices

- BCBS, IAIS and IOSCO (2005), *Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism*, www.bis.org/publ/joint05.htm.
- IOSCO (2005), *Anti-Money Laundering Guidance for Collective Investment Schemes, Final Report*, www.iosco.org/library/pubdocs/pdf/IOSCOPD205.pdf.
- IOSCO (2004), *Principles on Client Identification and Beneficial Ownership for the Securities Industry*, www.iosco.org/library/pubdocs/pdf/IOSCOPD167.pdf.
- IOSCO (1995), *Report on Money Laundering, Working Party No. 4*, IOSCO, Madrid, Spain.

Domestic Material

- Australian Transaction Reports and Analysis Centre (AUSTRAC) (2007), *Guideline No. 4, Areas of Suspect Activity, Securities Offences*, www.austrac.gov.au/g4e4.html.
- Australian Transaction Reports and Analysis Centre (AUSTRAC) (2008), *Securities & Derivatives: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, www.austrac.gov.au/files/securities_derivatives_presentation_2008.pdf.
- Australian Transaction Reports and Analysis Centre (AUSTRAC) (2007), *Typologies and Case Studies Report 2007*, www.austrac.gov.au/files/typologies_report.pdf.
- Financial Crimes Enforcement Network (FinCEN) (2009), *The SAR Activity Review: Trends, Tips and Issues, Issue 15*, http://fincen.gov/news_room/rp/files/sar_tti_15.pdf.
- Financial Crimes Enforcement Network (FinCEN) (2008), *The SAR Activity Review: Trends, Tips and Issues, Issue 13*, http://fincen.gov/news_room/rp/files/sar_tti_13.pdf.
- Financial Crimes Enforcement Network (FinCEN) (2005), *The SAR Activity Review: Trends, Tips and Issues, Issue 9*, http://fincen.gov/news_room/rp/files/sar_tti_09.pdf.
- Financial Crimes Enforcement Network (FinCEN) (2003), *The SAR Activity Review: Trends, Tips and Issues, Issue 5*, http://fincen.gov/news_room/rp/files/sar_tti_05.pdf.

- Financial Industry Regulatory Authority (FINRA) (2004), *Small Firm Template-Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures*, www.finra.org/Industry/Issues/AML/p006340.

- Financial Industry Regulatory Authority (FINRA) (2004), *Small Firm Template-Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures*, www.finra.org/Industry/Issues/AML/p006340.

- Financial Industry Regulatory Authority (FINRA) (2002), *Notice to Members Anti-Money Laundering-NASD Provides Guidance to Member Firms Concerning Anti-Money*, www.finra.org/Industry/Regulation/Notices/2002/P003703.

- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), *Information for Securities Dealer*, www.fintrac-canafe.gc.ca/re-ed/sec-eng.asp and www.canafe-fintrac.gc.ca/re-ed/sec-fra.asp.

- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) (2004), *Money Laundering in Canada: an Analysis of RCMP Cases*, FINTRAC, Ottawa, Canada.

- Belgian Financial Processing Unit CTIF-CFI (2006, 2007), *Annual Reports for 2006 and 2007*, www.ctif-cfi.be/menu.php?lang=en&page=ann_rep.

- Securities Industry and Financial Markets Association (SIFMA) (2008), *Guidance for deterring money laundering and terrorist finance activity*, www.sifma.org/regulatory/anti-money/pdf/AMLguidance.pdf.

- Securities Industry and Financial Markets Association (SIFMA) (2006, 2008), *Anti-Money Laundering and Financial Crimes Committee-Suggested Practices for Customer Identification Programs*, www.sifma.org/regulatory/anti-money/pdf/CIP-suggested.pdf.

Other

- Boyer, Allan D. and Susan Light (2008), *Dirty Money & Bad Luck: Money Laundering in the Brokerage Context*, 3 Virginia Law and Business Review 82, http://www.virginialawbusrev.org/VLBR3-1pdfs/Boyer.pdf.

- Marco Arnone & Pier Padoan (2008), *Anti-money laundering by international institutions: a preliminary assessment*, European Journal of Law and Economics, Vol. 26, No. 3, pp. 361-386, Netherlands.

ANNEX A:

GLOSSARY OF TERMS[28]

Annuities: Form of contract sold by life insurance companies that guarantees a fixed or variable payment to the annuitant at some future time, usually retirement.

Bearer form: Securities that are not registered with the issuer and payable to the person who is in possession. Bearer bonds have coupon attachments that the holder can present on the interest date for payment. Bearer securities are negotiable without endorsement, can be transferred by delivery and can pay dividends upon presentation of a coupon.

Bearer bonds: Bond issued with detachable coupons that must be presented to a paying agent or the issuer for interest payment.

Bearer securities: Securities that are completely negotiable and entitle the holder to the rights under the security (e.g. to payment if it is a debt security, and voting if it is an equity security). They are transferred by delivering the instrument from person to person. In some cases, transfer is by endorsement, or signing the back of the instrument, and delivery.

Beneficial owner: the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Bills of exchange: An unconditional order in writing, addressed by one person (the drawer) to another person (the drawee) and signed by the person giving it, requiring the drawee to pay, on demand or at a fixed or determinable future time, a specified sum or money to, or to the order of a specified person (the payee) or to the bearer.

Boiler rooms: Refers to dishonest broker-dealers who set up a group of high-pressure salespeople who use banks of telephones to make cold calls to as many potential investors as possible. These salespeople urge investors to buy "house stocks"; stocks that the firm buys or sells as a market maker or has in its inventory. Boiler room operators typically sell penny stocks.

Bonds: An IOU issued by a borrower to a lender. Bonds often take the form of fixed interested securities issued by governments, municipalities, or companies. A bond typically obligates the issuer to pay the bondholder a specified sum of money, usually at specific intervals, and to re-pay the principal amount at maturity.

Broker: A person who acts as an intermediary between a buyer and seller of securities, usually for a commission.

[28] To reflect their common usage, the terms in this glossary were derived, in part, from: (1) Barron's Dictionary of Finance and Investment Terms (6th Ed. 2003); (2) Oxford's Dictionary of Finance and Banking (3rd Ed. 2005); and from the FATF Glossary.

Block trade: Refers to a large trade that is usually at least 10,000 shares of a stock or $200,000 of bonds. It can also refer specifically to large trades that occur between institutional parties at a fixed or pre-determined price.

Bulletin boards: Electronic inter-dealer quotation system that displays real-time quotes, last-sale prices, and volume information for many over-the-counter securities that are not listed on a national securities exchange.

Call options: Call options give the buyer the right, but not the obligation, to buy the underlying currency or a security at a particular price by a particular date.

Cashier's cheque: A cheque that draws directly on a customer's account, making the bank the primary obligor. Customers requiring a cashier's check must pay the amount of the cheque to the bank. The bank will then issue a cheque to a third party named by the customer.

Certificates of participation: Certificates showing the level of participation in a business.

Certificate of deposit (CDs): A negotiable certificate that usually pays interests and is issued by a bank in return for a term deposit (ranging from months to years).

Cheques: A bill of exchange, or draft on a bank drawn against deposited funds to pay a specified sum of money to a specified person on demand.

Closed-end companies (Units in Collective Investment Schemes (UCIS)): A fund set up by an investment trust that issues a fixed number of shares to its investors.

Commercial paper: Short-term debt obligations with maturities ranging from 2 to 270 days issued by banks, corporations and other borrowers to investors with temporarily idle cash.

Contracts for difference (CFD): A type of derivative where an agreement is made to exchange the difference in value of a particular security (or other financial instrument) between the time at which a contract is opened and the time at which it is closed. The CFD allows a trader to buy and sell in any market and make profit from rising and falling prices, and to establish a deposit or margin to gain exposure to markets without tying up capital.

Correspondent account: An account whereby one financial institution regularly performs services for another financial institution in markets that may be inaccessible to the latter. Many correspondent relationships involve the wire transfer of money.

Credit-default swaps (CDS): Financial contract whose value is based on underlying debt obligations. A CDS can be tied to the performance of the debt obligations of a single entity or security, or, with more complex CDS, an index of several such entities or securities.

Dealer: A person who acts as a principal in a financial transaction rather than as a broker or agent.

Debenture: General debt obligation backed only by the integrity of the borrower and documented by an agreement called an indenture (e.g. an unsecured bond).

Dematerialisation of securities: The transfer of physical, hard-copy security certificates to book entry credits of a security holder's interest.

Depository institutions: Financial institutions that take deposits and extend loans. This definition includes banks and credit unions.

Derivatives: A financial instrument whose price is related to an underlying commodity, currency, economic variable, financial instrument or security. The different types of derivatives include futures contracts, forwards, swaps, and options. They can be traded on exchanges or over-the-counter (OTC). Market traded derivatives are standard, while OTC trades are specific and customised.

Downbid: Generally refers to a current bid less than a previous bid.

Electronic communications networks (ECN): Electronic trading systems that automatically match buy and sell orders at specified prices. Subscribers, which are typically institutional investors, broker-dealers, and market-makers; they can place trades directly with an ECN.

Equities: Ownership interest possessed by shareholders in a corporation. Often called stocks.

Exchanges: Any organisation, association, or group of persons, whether incorporated or unincorporated, which constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood, and includes the market place and the market facilities maintained by such an exchange.

Foreign exchange contracts: Futures and options contracts based on foreign currencies. The buyer of a currency futures contract acquires the right to buy a particular amount of that currency by a specific date at a fixed rate of exchange and the seller agrees to sell that currency at the same fixed price.

Forward rate agreements: Purchase or sale of a specific quantity of a commodity, government security, foreign currency, or other financial instrument at the current or spot price, with delivery and settlement at a specified future date.

Fraud: Intentional misrepresentation, concealment, or omission of the truth for the purpose of deception or manipulation to the detriment of a person or organisation.

Free look period: A contractual provision that provides the contract owner the right to return the contract within a specified period for a refund.

Futures contract: An agreement to buy or sell a fixed quantity of a particular commodity, currency, or security for delivery at a fixed date in the future at a fixed price. Unlike an option, a futures contract involves a definite purchase or sale and not an option to buy or sell.

Hedge funds: Hedge funds pool investors' money and invest those funds in financial instruments in an effort to make a positive return. Many hedge funds seek to profit in all kinds of markets by pursuing leveraging and other speculative investment practices that may increase the risk of investment loss. Hedge funds typically issue securities in "private offerings" that are usually not required to be registered with a securities or financial regulator.

Insider trading: Buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non public information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information.

Investment adviser: Any person who, for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who, for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities.

Investment trusts: Refers to firms that, for a management fee, invest the pooled funds of small investors in securities appropriate for its stated investment objectives. See also **Unit Trusts**.

Journaling: A book entry system where assets are debited from one account and credited to another.

Margin: Arrangement whereby an investor pays for part of a securities purchase and borrow the rest from a securities intermediary. For example, an investor may buy $5,000 worth of stock in a margin account by paying for $2,500 and borrowing $2,500 from the securities intermediary.

Money manager: See **Portfolio manager**.

Market manipulation: A deliberate attempt to interfere with the free and fair operation of the market and create artificial, false or misleading appearances with respect to the price of, or market for, a security, commodity or currency.

Money orders: A financial instrument that can be easily converted into cash by the payee named on the money order. The money order lists both the payee and the person who bought the instrument, known as the payor. Money orders are issued by a variety of entities to people presenting cash or other forms of payment.

Mortgage bonds: Bond issue secured by a mortgage on the issuer's property, such as the lien on which is conveyed to the bondholders by a deed of trust.

Mutual funds (Open-end investment company): See definition of **unit investment trust.**

Nominee accounts: An account under which a person, a nominee named by another, acts on his or her behalf often to conceal the identity of the nominator.

Nostro: Account established by a domestic banking institution to receive deposits from, make payments on behalf of, or handle other financial transactions for a foreign financial institution, usually in the foreign financial institution's currency. See also **correspondent account**.

Note: A written promise to pay a specified amount to a certain entity on demand or on a specified date.

Omnibus accounts: Account opened in the name of one financial institution at another financial institution comprised of multiple individual accounts whose names are not disclosed to the former.

Options: The right to buy or sell a fixed quantity of a commodity, currency, or security at a particular date at a particular price (the exercise price). Unlike futures, the purchaser of an option is not obligated to buy or sell at the exercise price. If the option lapses, the purchaser only loses the initial purchase price of the option.

Over-the-counter (OTC) markets: A market in which securities are bought and sold outside of established securities markets.

Penny stocks: Securities with very low market price, volume and/or liquidity that are traded on a securities exchange or on the OTC markets. These shares are usually issued by companies with a short or erratic history of revenues and earnings, and therefore such stocks are more volatile than those of well established companies trading on major securities exchanges.

Pink sheets: an electronic quotation system that displays quotes of many securities traded over the counter.

Politically exposed person (PEP): Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Ponzi scheme: A type of fraud names after Charles Ponzi, who operated such a scheme in the U.S. in the 1920s. Under the scheme, investors are offered unsustainably high rates of interest and are initially paid their interest from a fund consisting of new deposits. When the deposits dry up, the scheme collapses. Also referred to as **pyramid schemes**.

Portfolio manager: A professional responsible for the securities portfolio of an individual or institutional investor. In return for a fee, the manager has the responsibility of choosing and managing assets.

Pump-and-dump: "Pump and dump" schemes, also known as "hype and dump manipulation," involve the touting of a company's stock (typically **penny stocks**) through false and misleading statements to the marketplace. After pumping the stock, fraudsters profit by selling their cheap stock into the market.

Put options: Put options give the buyer the right to sell underlying currencies or securities at a specific price and date.

Reverse merger: A method through which a private company can go public without an initial public offering (IPO). This occurs when a private company acquires or merges with a public shell company that is listed on a stock exchange or traded on the OTC markets.

Shell bank: a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

Shell companies: Company that often has no physical presence and generates little or no independent economic value. These companies are commonly organised in a way that makes ownership and transactions information of the company easier to conceal, particularly when the shell company is private.

Short sale: Generally, the sale of a stock that an investor does not own. Investors who sell short believe the price of the stock will fall. If the price drops, the investor can buy the stock at the lower price and make a profit. If the price of the stock rises and the investor buys it back later at the higher price, he or she will incur a loss. When an investor sells short, a securities intermediary loans the investor the stock. The stock the investor borrows comes from either the intermediary's own inventory, the margin account of another of the intermediary's clients, or another securities intermediary.

Subscription rights: A privilege granted to existing shareholders of a corporation to subscribe to shares of a new issue of common stock before it is offered to the public; better known simply as a right. Such a right normally lasts two or three weeks, are freely transferable and entitles the holder to buy the new public stock below the public offering price.

Transfer agents: Companies that have publicly traded securities typically use transfer agents to keep track of the individuals and entities that own their stocks and bonds. Many transfer agents are banks or trust companies, but sometimes a company acts as its own transfer agent. Transfer agents perform three main functions: issue and cancel certificates to reflect changes in ownership; act as an intermediary for the company; and handle lost, destroyed, or stolen certificates.

Traveller's cheques: A preprinted, fixed-amount cheque designed to allow the person signing it to make an unconditional payment to someone else as a result of having paid the issuer for that privilege.

Trust accounts: An arrangement enabling property to be held by a person or persons (the trustees) for the benefit of some other person or persons (the beneficiaries). The trustee is the legal owner of the property but the beneficiary has an equitable interest in it.

Underwriting: The process of agreeing to purchase a new issue of securities from an issuer and distribute it to investors. The underwriter makes a profit between the price paid to the issuer and the public offering price.

Unit investment trusts or unit trusts: An investment trust formed to manage a portfolio, in which investors can buy units. Open-end investment companies are often organised as unit investment trusts.

Variable annuity: A contract issued by an insurance company under which an investor provides the insurer with a lump-sum payment or series of payments. In return, the insurer agrees to make periodic payments to the investor beginning immediately or at some future date. The investor is usually permitted to invest the purchase payments in a range of investment options. The value of the account in a variable annuity will vary depending on the performance of the investment options that have been chosen.

Warrants: A security that offers the owner the rights to subscribe for ordinary shares of a company at a fixed date, usually at a fixed price. Warrants can themselves be bought and sold on stock exchanges and are equivalent to stock options.

Wealth managers: See **Investment adviser** and **Portfolio manager**.

ANNEX B:

SUSPICIOUS INDICATORS

Introduction

211. This annex is divided into two sections. Section I lists suspicious indicators that have been identified in the questionnaire responses as indicating possible ML/TF in the securities industry. Section II lists suspicious indicators and red flags that are pertinent for evaluating whether a customer may be engaged in activities that would come under the FATF's list of "designated categories of offences" that are: (i) predicate offences to money laundering and (ii) offences that are unique to the securities industry, namely insider trading, market manipulation, and other forms of securities fraud.

1. The suspicious indicators listed in these two sections are being provided here to give law enforcement, regulators and the private sector an overview of the types of activities that can be suspicious. We caution however, that this list is non-exhaustive and that some of these ML/TF suspicious indicators and red flags may be not be applicable in all jurisdictions. Furthermore, some of the suspicious indicators and red flags with respect to the designated offences may be more useful for banks in identifying securities specific illicit activities that may not necessarily require the use of a securities intermediary or markets per se (i.e. securities offering fraud).

2. We also note that the occurrence of one or more of these indicators/red flags may be a warning sign of unusual activity that may be indicative of ML/TF and/or the occurrence of a securities specific designated offence. However, this does not necessarily mean that money laundering, terrorist financing or any other illicit activity is occurring. Further investigation should be conducted if any of these indicators/red flags are present during the course of a transaction or customer interaction.

Section I:
Suspicious Indicators for Money Laundering and Terrorist Financing in the Securities Industry

Customer Due Diligence

- The customer provides the securities firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. This indicator may apply to account openings and to interaction subsequent to account opening, such as wire transfers.

- During the account opening process, the customer refuses to provide information to complete CDD/KYC (e.g. occupation, prior financial relationships, etc.).

- The customer, whether a person or entity, is reluctant to provide the securities firm with complete information about the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, the entity's officers and directors or business location.

- The customer, whether a person or entity, is located in a jurisdiction that is known as a bank secrecy haven, a tax shelter, or high-risk geographic locations (e.g. narcotics producing jurisdiction).

- The customer is reluctant to meet personnel from the securities firm in person, is very secretive and/or evasive or becomes defensive when asked to provide more information.

- The customer refuses to identify a legitimate source for funds or provides the securities firm with information that is false, misleading, or substantially incorrect.

- The customer engages in frequent transactions with money services businesses.

- The customer's background, whether a person or entity, is questionable or does not meet expectations based on business activities.

- The customer has no discernable reason for using the firm's service or the firm's location (e.g. customer lacks roots to the local community or has come out of his or her way to use the firm).

- The customer refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, misleading or substantially incorrect.

- The customer's address is associated with multiple other accounts that do not appear to be related.

- The customer has a history of changing financial advisors and/or using multiple firms or banks. This indicator is heightened when the customer uses firms located in numerous jurisdictions.

- The customer is known to be experiencing extreme financial difficulties.

- The customer is, or is associated with, a PEP or senior political figure.

- The customer refuses to invest in more appropriate securities when those securities would require a more enhanced CDD/KYC procedure.

- The customer with a significant history with the securities firm abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction.

- The customer appears to be acting as a fiduciary for someone else but is reluctant to provide more information regarding for whom he or she may be acting.

- The customer is publicly known to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds or is known to associate with such persons. Sources for this information include news items or Internet searches.

- The customer inquires as to how quickly he or she can liquidate accounts or earnings without explaining why or provides suspicious reasons for doing so.

- The customer opens an account or purchases a product without any regard to loss, commissions or other costs associated with that account or product.

- The customer has commercial or other types of relationships with risky persons or institutions.

- The customer acts through intermediaries, such as money managers or advisers, in order not to have his or her identity registered.

- The customer exhibits unusual concern with the securities firm's compliance with government reporting requirements and/or the firm's AML/CFT policies.

- The customer is reluctant to provide the securities firm with information needed to file reports or fails to proceed with a transaction once asked for documentation or learns of any recordkeeping requirements.

- The customer is interested in paying higher charges to the securities firm in order to keep some of his or her information secret.

- The customer tries to persuade an employee of the securities firm not to file a required report or not to maintain required records.

- The customer funds deposits, withdraws or purchases financial or monetary instruments below a threshold amount in order to avoid any reporting or recordkeeping requirements imposed by the jurisdiction.

- The customer requests that account openings and closings in his or her name or in the name of family members be done without producing a paper trail.

- Law enforcement has issued subpoenas regarding a customer and/or account at the securities firm.

Fund Transfers and/or Deposits

- Wire transfers are sent to, or originate from, financial secrecy havens, tax shelters or high-risk geographic locations (e.g. jurisdictions known to produce narcotics/psychotropic drugs or to be related to terrorism) without an apparent business reason or connection to a securities transaction.

- Wire transfers or payments to or from unrelated third parties (foreign or domestic) or where the name or account number of the beneficiary or remitter has not been supplied.

- Many small, incoming wire transfers or deposits are made, either by the customer or third parties, using cheques, money orders or cash that are almost immediately withdrawn or wired out in a manner inconsistent with customer's business or history.

- Incoming payments made by third-party cheques or cheques with multiple endorsements.

- Deposit of large amount of small-denomination currency to fund account or exchanges of small notes for bigger notes.

- Wire transfer activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

- The securities account is used for payments or outgoing wire transfers with little or no securities activities (e.g. account appears to be used as a depository account or a conduit for transfers).

- The controlling owner or officer of a public company transfers funds into his personal account or into the account of a private company that he or she owns or that is listed as an authorised signatory.

- Quick withdrawal of funds after a very short period in the account.

- Transfer of funds to financial or banking institutions other than those from where the funds were initially directed, specifically when different countries are involved.

- Transfers/journals between different accounts owned by the customer with no apparent business purpose.

- Customer requests that certain payments be routed through nostro or correspondent accounts held by the financial intermediary or sundry accounts instead of its own account.

Bearer Securities

- The customer requests cashing bearer securities without first depositing them into an account or frequently deposits bearer securities into an account.

- The customer's explanation regarding the method of acquiring the bearer securities does not make sense or changes.

- The customer deposits bearer securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

Unusual Securities Transactions and Account Activity

- Transaction where one party purchases securities at a high price and then sells them at a considerable loss to another party. This may be indicative of transferring value from one party to another.

- A customer's transactions include a pattern of sustained losses. This may be indicative of transferring value from one party to another.

- The purchase and sale of non-listed securities with a large price differential within a short period of time. This may be indicative of transferring value from one party to another.

- Payments effected by administrators and asset managers in cash, bearer cheques or other transferable instruments without indentifying who they are for or providing very little information regarding the underlying account holder or beneficiary.

- A company uses cash to pay dividends to investors.

- Use of shell companies to purchase public company shares, in particular if the public company is involved in a cash intensive business.

- Transfer of assets without a corresponding movement of funds, such as through journaling or effecting a change in beneficial ownership.

- A dormant account that suddenly becomes active without a plausible explanation (e.g. large cash deposits that are suddenly wired out).

- A customer's transactions have no apparent economic purpose.

- A customer who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless.
- Transactions that show the customer is acting on behalf of third parties.
- The purchase of long term investments followed by a liquidation of the accounts shortly thereafter, regardless of fees or penalties.
- Transactions involving an unknown counterparty.
- Large sum cash purchases of financial instruments and mutual funds holdings followed by instant redemption.

Insurance Products (applicable to jurisdictions where some insurance products can be considered securities)

- The customer cancels an insurance contract and directs that the funds be sent to a third party.
- The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of the funds.
- The customer cancels an annuity product within the free-look period. Although this could be legitimate, it could also signal a method of laundering funds if accompanied with other suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders and/or having a history of cancelling annuity products during the free look period.
- The customer opens and closes accounts with an insurance company only to reopen a new account shortly thereafter with the same insurance company, but with new ownership information.
- The customer purchases an insurance product with no concern for investment objective or performance.
- The customer purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official cheques or sequentially numbered money orders.
- Securing a policy loan against the cash value soon after the policy is issued and repaying the loan with various monetary instruments or cash.

Activity that is Inconsistent with the Customer's Business Objective or Profile

- The customer's transaction patterns suddenly change in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.
- There are unusual transfers of funds or journaling (i.e. book entries) among accounts without any apparent business purpose or among apparently unrelated accounts.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- The customer's account is not used for its intended purpose (i.e. used as a depository account).

- The customer enters into a financial commitment that appears beyond his or her means.
- The customer begins to use cash extensively.
- The customer engaged in extremely complex transactions where his or her profile would indicate otherwise.
- Customer's credit usage is in extreme amounts that do not correspond to his or her financial status or collateral, which is provided by an unrelated third-party.
- The time zone in customer's location is not consistent with the times that the trades were executed, with no apparent business or other purpose, or there is a sudden change inconsistent with the customer's typical business activity.
- A foreign based customer that uses domestic accounts to trade on foreign exchanges.
- The customer exhibits a lack of concern about higher than normal transaction costs.

Rogue Employees

- The employee appears to be enjoying a lavish lifestyle that inconsistent with his or her salary or position.
- The employee is reluctant to take annual leave.
- The employee is subject to intense job-related demands, such as sales or production goals that may make him more willing to engage in or overlook behaviour that poses ML/TF risks.
- The employee inputs a high level of activity into one customer account even though the customer's account is relatively unimportant to the organisation.
- The employee is known to be experiencing a difficult personal situation, financial or other.
- The employee has the authority to arrange and process customer affairs without supervision or involvement of colleagues.
- The management/reporting structure of the financial institution allow an employee to have a large amount of autonomy without direct control over his activities.
- The employee is located in a different country to his direct line of management, and supervision is only carried out remotely.
- A management culture within the financial institution focuses on financial reward over compliance with regulatory requirements.
- The employee's supporting documentation for customers' accounts or orders is incomplete or missing.
- Business is experiencing a period of high staff turnover or is going through significant structural changes.

Section II:
Suspicious Indicators for Predicate Offences To Money Laundering Linked to Securities

Insider Trading

- The customer makes a large purchase or sale of a security, or option on a security, shortly before news is issued that affects the price of the security.
- The customer is known to have friends or family who work for the securities issuer.
- A customer's trading patterns suggest that he or she may have inside information.

Market Manipulation, including Penny Stocks

- A customer engages in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low priced securities.
- Securities or funds transfers between parties without an apparent relationship.
- Securities transactions occur across many jurisdictions, and in particular high risk jurisdictions.
- Two or more unrelated accounts at the securities firm trade an illiquid or low priced security suddenly and simultaneously.
- A customer journals securities between unrelated accounts for no apparent business reason.
- A customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Transactions between the same or related parties structured solely so that one side incurs a loss while the other incurs a gain.
- Transaction where one party purchases securities at a high price and then sells them at a considerable loss to another party.
- The customer deposits a large number of physical securities at the securities firm.
- The physical securities are titled differently to the name on the account.
- The physical security does not bear a restrictive legend even though the history of the stock and/or the volume of shares being traded suggest that it should have such a legend.
- The customer's explanation regarding the method of acquiring the physical securities does not make sense or changes.
- The customer deposits physical securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
- Large or repeated trading in securities that are illiquid, low priced or difficult to price.

- The company at issue has no apparent business, revenues or products.
- The company at issue has experienced frequent or continuous changes in its business structure and/or undergoes frequent material changes in business strategy or its line of business.
- The officers or insiders of the company at issue are associated with other low priced, illiquid or low volume companies.
- The officers or insiders of the low priced, illiquid or low volume company have a history of regulatory violations.
- The low priced, illiquid or low volume company at issue has failed to make required regulatory disclosures.
- The low priced, illiquid or low volume company at issue has been the subject of a prior trading suspension.
- A customer's transactions include a pattern of receiving physical securities or receiving incoming shares transfers that are sold with the proceeds wire transferred out of the account.
- The purchase and sale of non-listed securities with a large price differential within a short period of time.

Securities Offering Fraud

- The customer opens numerous accounts for different legal entities that the customer controls.
- The customer receives many incoming cheques or wire transfers from unrelated third parties.
- The customer allocates incoming third party deposits among numerous accounts.
- The customer makes numerous outgoing payments to third parties close in time to when the customer receives many incoming third party cheques or wire transfers.
- The customer's profile does not suggest a legitimate business reason for receiving many third party deposits.
- The cheques or wire transfers note that the funds are for an investment.

ANNEX C:
SUSPICIOUS TRANSACTION REPORTS

Table 1: Securities Related STRs – 2005-2008[29]

2005	2006	2007	2008 (to extent available)	Total
10,852	13 241	20 350	13 357	**57 800**

Table 2: STR Breakdown Based on Type of Security

Type of securities activity/product	2005	2006	2007	2008 (to extent available)	Totals
Transferable Securities					
Equities	1 255	1 549	3 021	1 818	**7 643**
Bonds and Similar Instruments	194	252	334	271	**1 051**
Certificates of Deposit	48	105	88	114	**355**
Commercial Paper	11	23	42	17	**93**
Other	19	22	27	30	**98**
Units in Collective Investment Trusts					
Mutual Funds	366	392	754	441	**1 953**
Money Market Mutual Funds	196	257	373	231	**1 057**
Derivatives					
Options		1		1	**2**
Securities Futures Products	13	23	8	11	**55**
Commodity Derivatives Contracts (including futures)	14	17	40	12	**83**
Foreign Exchange Contracts	30	59	163	100	**352**
OTC Derivatives	16	15	35	14	**80**
Others	10	26	39	14	**178**
Other					
Warrants	7	10	21	6	**44**
Other securities	84	78	104	83	**349**
Any other	1 818	1 834	2 272	1 281	**7 205**

[29] Two jurisdictions provided figures that appear large with respect to their securities markets. Jurisdiction one indicated that 303,054 STRs were filed between 2005 and 2008. In particular, jurisdiction one indicated that 70,405 STRs were filed in 2005, 78,705 in 2006, 86,607 in 2007 and 67,337 in 2008. It is unclear whether this figure is representative of all STRs filed in the jurisdiction or only those related to securities. Jurisdiction two indicated that 34,700 STRs were filed in 2007, but did not provide yearly figures or specify whether figures were inclusive of all STRs filed. Because of this ambiguity, Table 2 adjusts the securities related STRs figures by deducting the figures provided by jurisdictions one and two. Inclusion of these figures would bring the total numbers of securities related to 81,257 for 2005, 91,946 for 2006, 141,657 for 2007, 80,964 for 2008 for a total of 395,824 securities related STRs filed for that period.

Table 3: STR Breakdown by type of institution

Type of Institution	2005	2006	2007	2008 (to extent available)	Total
Securities Broker or Dealer[30]	8 284	8 486	13 224	7 765	**37 759**
Commodities Futures Merchant, Broker, Dealer, Pool Operator[31]	196	258	446	206	**1 106**
Fund Manager	54	15	892	351	**1 312**
Bank or Affiliate[32]	947	1 395	1 231	1 044	**4 617**
Financial Adviser	262	698	1 299	918	**3 177**
Collective Investment Scheme[33]	623	646	1 404	423	**3 096**
Other, Foreign FIU, Self-Regulatory Organisation[34]	1 170	1 933	3 550	1 973	**8 626**

30 This figure includes market makers, municipal or local government securities dealers, introducing and clearing brokers, securities dealers, securities floor traders, securities options brokers and dealers, specialists, and federal or national government broker-dealers.

31 This figure includes agricultural trade option merchants, commodity pool operators, commodity trading advisors, futures commission's merchants, and futures floor brokers and dealers.

32 This figure includes banks, bank holding companies and bank subsidiaries.

33 This figure includes mutual funds.

34 This figure includes STRs filed by direct participation programs, FIUs and self-regulatory organisations, and those did not indicate what type of institution was filing, if any.

ANNEX D: QUESTIONNAIRE AND RESPONDING JURISDICTIONS AND ORGANISATIONS

The following jurisdictions submitted a response to the questionnaire that is re-produced below.

Andorra	Argentina	Australia	Austria
Belgium	Brazil	British Virgin Islands	Canada
Cayman Islands	China	Denmark	European Commission
France	Hong Kong	Israel	Japan
Jordan	Lithuania	Luxembourg	Malta
Mauritius	Mexico	Moldova	Monaco
Norway	Panama	Poland	Portugal
Qatar	Romania	Singapore	Slovakia
Spain	Sweden	Switzerland	The Netherlands
Turkey	Ukraine	United Kingdom	United States

2008 FATF Securities Typology Questionnaire

I. BACKGROUND

1. The objectives of the FATF Securities Typology Questionnaire are to collect information about: (i) the range of products classified as "securities" in various jurisdictions; (ii) how jurisdictions supervise compliance with anti-money laundering/combating terrorist financing ("AML/CTF") requirements for these products; (iii) potential areas of AML/CTF vulnerabilities in the securities industry; (iv) suspicious transaction reports (STRs) in the securities industry; and (v) enforcement actions in the securities industry.

2. The results of this survey will be used to develop a securities typology report to provide insight into the how money laundering and terrorist financing ("ML/TF") may operate in the securities industry. The securities typology project team will use the responses along with information from other sources to prepare the securities typologies report.

II. INSTRUCTIONS FOR COMPLETING THE SURVEY

3. All FATF members and FSRBs are invited to submit completed questionnaires to support the securities typologies report initiative. Contributions should be submitted to the FATF Secretariat (secretariat@fatf-gafi.org) **by 19 December 2008**. All questionnaire participants are encouraged to seek input from private sector representatives operating within their respective jurisdictions, as appropriate, in developing responses to the questions contained in this questionnaire. Responses should be complete yet concise and clearly address the questions asked. Any additional information which may be relevant for the securities typologies report may be submitted along with the questionnaire response. The typology is looking at the use of the securities industry/securities products for money laundering and terrorist financing, and questionnaire responses should concentrate on this, rather than examining the predicate offence (e.g. fraud).

1. Jurisdiction/Organisation

Name of Jurisdiction or Organisation completing questionnaire

2. Contact details

Contact details for any queries arising from this response

3. Range of products classified as "securities"

Using the definition of "financial institution" in the FATF glossary as a point of reference, please use the following chart to identify: (1) products that are traded as "securities" in your country; (2) the type of financial institutions involved in selling, recommending or distributing securities (e.g. broker-dealers, banks, etc.); and (3) the supervisory authority(ies) responsible for AML/CFT supervision of that product/financial institution.

Product	**FATF definition of activity (see Glossary - below)**	**Is this treated as a security in your jurisdiction? (YES or NO)**	**If product is a security, type(s) of institutions involved in sale, advice, or distribution** (e.g. broker-dealer/fund manager/bank)	**Name of supervisory authority(ies) responsible for regulating AML/CFT compliance of applicable institution**
1. Transferable Securities				
Equities	7(a), 9, 10, 11			
Bonds and similar debt instruments	7(a), 9, 10, 11			
Certificates of deposit	7(a), 9, 10, 11			
Bills of exchange	7(a), 9, 10, 11			
Other (please specify)				
2. Units in collective investment schemes				
Unit trusts	7(d), 9, 10, 11			
Investment trusts	7(d), 9, 10, 11			
Mutual funds	7(d), 9, 10, 11			
OEICs (open-ended investment companies)	7(d), 9, 10, 11			
SICAV/Fs (an open-ended collective	7(d), 9, 10, 11			

investment scheme)				
Closed-end company	7(d), 9, 10, 11			
3. Derivatives				
Options	7(a), 7(b), 7(c), 7(e), 9, 10, 11.			
Future	7(a), 7(b), 7(c), 7(e), 9, 10, 11.			
Swaps	7(a), 7(b), 7(c), 7(e), 9, 10, 11.			
Forward rate agreements	7(a), 7(b), 7(c), 7(e), 9, 10, 11.			
Commodity derivatives contracts	7(a), 7(e), 9, 10, 11.			
Foreign exchange contracts	7(a), 7(b), 7(c), 9, 10, 11.			
Other				
4. Other				
Please detail any other product which is classified as a "security" in your jurisdiction (e.g., insurance products such as variable annuities).				

4. AML/CTF vulnerabilities in the securities industry

4.1 Please describe the types of transactions, products and/or activities in the securities industry that are considered to present high risk factors for ML/TF, if any.

4.1.2. Are any of the above designated as high risk by law/regulation/other measures in the jurisdiction?

4.2 Please describe the payment methods in the jurisdiction (e.g., cash, wire transfer, cheque, online systems, mobile phone systems, etc.) associated with higher risks for ML/TF, if any.

4.3 Please describe the delivery methods used in the jurisdiction (e.g. physical securities, book-entry, etc.) associated with higher risks for ML/TF, if any.

4.4 Please provide examples of any specific suspicious transaction triggers/indicators/red flags for the securities industry.

5. Typologies/methods/trends

Please attach or provide hyperlinks to any ML/TF typologies for the securities industry developed within your jurisdiction (such as documents that detail high risk securities products or method of distribution, as well as what caused initial suspicions in the securities industry, how assets were traced, and the outcome of investigations/prosecutions). Where relevant, please indicate at which stage of the transaction(s) you consider that money laundering/terrorist financing took place.

6. Enforcement actions for violations of AML/CFT requirements

6.1 How many criminal/regulatory enforcement actions concerning AML/CFT requirements applicable to the securities firms have been brought in the past 3 years?

Year	Number – regulatory only	Number – criminal only	Number – joint regulatory/criminal
2005			
2006			
2007			
2008 (if available)			

6.2 Do any of these enforcement actions reveal areas of high risk or vulnerability in the securities industry? If so, provide brief summaries of key enforcement actions.

7. Suspicious transaction reports

7.1 How many STRs relating to securities transactions has the FIU received in the past 3 years?

Year	Number
2005	
2006	
2007	
2008 (if available)	

7.2 Please specify the number of STRs filed in the past 3 years relating to securities transactions for each type of securities activity/product and/or relating to the each type of filing institution (if this information is maintained by the FIU).

For example, possible types of products and institutions are given below.

Type of securities activity/product	2005	2006	2007	2008 (if available)
A. Transferable Securities				
Equities				
Bonds and similar debt instruments				
Certificates of deposit				
Bills of exchange				
Other (please specify)				
Other (please specify)				
B. Units in collective investment schemes				
Unit trusts				
Investment trusts				
Mutual funds				
OEICs				
SICAV/Fs				
Other (please specify)				
Other (please specify)				
C. Derivatives				
Options				
Futures				
Swaps				
Forward rate agreements				
Commodity derivatives contracts				
Foreign exchange contracts				
Other (please specify)				
Other (please specify)				
D. Other				

Please detail any other product which is classified as a "security" in your jurisdiction.				

Type of filing institution	2005	2006	2007	2008 (if available)
Broker/dealer				
Fund manager				
Bank				
Financial advisor				
Collective Investment Scheme provider				
Other (please specify)				

7.3 Do any of these STRs reveal areas of high risk or vulnerability in the securities industry? If so, please discuss any tends or areas of risk/vulnerabilities demonstrated by STRs.

7.4 Based on STRs related to the securities industry or as a result of other information concerning the securities industry: how many referrals has the FIU made to law enforcement, how many ML/TF prosecutions have been commenced, and how many convictions have resulted?

Year	Number of Referrals	Number of Prosecutions	Number of Convictions
2005			
2006			
2007			
2008 (if available)			

8. Other proceedings

Please give details of any ancillary proceedings/tracing/freezing of assets/regulatory proceedings/criminal proceedings that revealed the use of securities.

FATF/OECD
October 2009

www.fatf-gafi.org

Appendix GG:

FATF, *Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement* (Paris: FATF, 2015)

GUIDANCE FOR A RISK-BASED APPROACH

EFFECTIVE SUPERVISION AND ENFORCEMENT BY AML/CFT SUPERVISORS OF THE FINANCIAL SECTOR AND LAW ENFORCEMENT

OCTOBER 2015

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2015), *Emerging Terrorist Financing Risks,* FATF, Paris
www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

TABLE OF CONTENTS

ACRONYMS

ACPR	*Autorité de contrôle prudentiel et de résolution*
AML/CFT	anti-money laundering and countering financing of terrorism
CDD	customer due diligence
CNBV	National Banking and Securities Commission
DNFBP	designated non-financial businesses and professions
FCA	Financial Conduct Authority
FCA	Financial Conduct Authority
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial intelligence unit
FRFI	federally regulated financial institutions
FSA	Financial Services Authority
HMRC	HM Revenue and Customs
IAIS	International Association of Insurance Supervisors
IOSCO	International Organisation of Securities Commission
ML	money laundering
MSB	money service business
OFAC	Office of Foreign Assets Control
OSFI	Office of the Superintendent of Financial Institutions
RBA	risk-based approach
SAR	suspicious activity report
STR	suspicious transaction report
TF	terrorist financing
TFS	targeted financial sanctions

I. OBJECTIVES AND SCOPE

1. The objective of this non-binding guidance paper is to describe the features of an effective supervisory system, with an aim to enhance countries'[1] understanding of the relevant FATF requirements by describing good practices and providing illustrative case examples. Effective supervision and enforcement is an important component of an effective anti-money laundering and countering financing of terrorism (AML/CFT) regime. For the purposes of this paper, an effective supervisory and enforcement system comprises a wide range of financial supervisory measures that include preventive measures and related sanctions[2] and other remedial actions[3] that AML/CFT supervisors[4] (including regulators) can apply, as well as separate yet complementary measures and actions by law enforcement and/or other relevant competent authorities. The overall effectiveness of a country's AML/CFT regime requires recognition of the important synergies that exist between AML/CFT, prudential and business conduct supervision and between those supervisors and judicial/law enforcement authorities. The recognition of this complementarity, as well as the willingness and ability to promote and encourage its application, can only further improve efforts to prevent and combat money laundering (ML)/terrorist financing (TF) in countries.

2. The practices described in this document are intended to serve as examples of the measures and means that relevant supervisors in countries may use to meet the requirement of the FATF Recommendations regarding a supervisory approach. This guidance does not pre-judge the institutional measures and other means that countries may use to achieve risk-based supervision and enforcement in their country, which vary according to each country's context, such as the size and complexity of the financial services sector and the degree of ML/TF risks (including threats and vulnerabilities) to which it is exposed[5]. As Recommendation 1 recognises that not all financial

---

1 All references in this paper to *country* or *countries* apply equally to territories or jurisdictions.

2 Examples of types of sanctions include: written warnings; orders to comply with specific instructions (possibly accompanied with daily fines for non-compliance); ordering regular reports from the institution on the measures it is taking; fines for non-compliance; barring individuals from employment within that sector; removing, replacing or restricting the powers of managers, directors, and controlling owners; imposing conservatorship or suspension or withdrawal of the license; or criminal penalties where permitted.

3 Examples of remedial actions are corrective actions such as written agreements, board resolutions/letters, supervisory letters,action plans, timelines, reprimands and fines.

4 Throughout this paper, the terms *supervisor* and *AML/CFT supervisor* refer to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing. This includes:

- Core Principles supervisors who carry out supervisory functions that are related to the implementation of the *FATF Recommendations*, and
- non-public bodies, including certain types of *self-regulatory bodies* (as defined in the *Glossary to the FATF Recommendations*) that have the power to supervise and sanction financial institutions in relation to AML/CFT requirements are empowered by law to exercise the functions they perform, and are supervised by a competent authority in relation to such functions.

5 This guidance is not a standard and is therefore not intended to designate specific actions or arrangements necessary to meet obligations under Recommendations 26, 27, 35 and their respective Interpretative Notes, nor does this guidance pre-empt the technical assessment of these Recommendations or the

institutions face the same ML/TF risks, there may be different approaches to supervision for different financial sectors (e.g., money or value transfer services, securities brokers and depository institutions). An actual assessment of effectiveness of the AML/CFT supervisory system in each country is part of the FATF's mutual evaluation process, where assessors evaluate whether the particular measures, controls, and actions taken by each country produce the desired effective outcomes.[6]

3. This guidance paper is intended to address AML/CFT supervision and enforcement of preventive measures for financial institutions[7] as defined by the FATF and should be read in conjunction with the relevant FATF Guidance Papers on the Risk Based Approach (RBA), such as the 2014 *RBA Guidance for the Banking Sector*[8]. Other documents that may assist countries are:

- *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* (Basel Committee, January 2014);
- *Core Principles for Effective Banking Supervision* (Basel Committee, September 2012)
- *Core Principles of Securities Regulation* (IOSCO, 2015a)
- Guidance on *Credible Deterrence in the Enforcement of Securities Regulation* (IOSCO, 2015b); and
- *Insurance Core Principles* (IAIS, nd)

4. **Section II** sets out some examples of supervisory models, **Section III** sets out the features of an effective supervisory system, and **Section IV** sets out complementary processes and actions available to law enforcement. **Section V** shows a graphic representation of effective supervision and enforcement.

5. For the purpose of this guidance paper, the terms *Core Principles*, *financial group*, *financial institutions*, *money or value transfer service* (MVTS), and *targeted financial sanctions* have the same meaning as set out in the General Glossary to the FATF Recommendations.

assessment of Immediate Outcome 3. Criteria for assessing technical compliance and effectiveness can be found in the FATF Methodology.

6 Throughout this paper, use of the term *should* is not meant to infer that measures or actions described in this paper are the only way to achieve effective supervision and enforcement.

7 This paper does not address the supervision and monitoring of designated non-financial businesses and professions (DNFBP).

8 *RBA Guidance for the Banking Sector* (FATF, 2014). The FATF will also issue the *RBA Guidance for Money or Value Transfer Services (MVTS)* towards 2016 which updates the 2009 *RBA Guidance for Money Service Businesses (MSBs)*.

II. FINANCIAL SUPERVISION MODELS

6. There are many different supervisory approaches and while the FATF does not prescribe a particular supervisory model, whichever supervisory system is chosen, it should effectively address and mitigate the money laundering and terrorist financing risks in the financial sector. The basic requirements that countries should comply with are in

- Recommendation 1 (assessing risks and applying risk-based approach),
- Recommendations 26 (regulation and supervision of financial institutions),
- Recommendation 27 (powers of supervisors),
- Recommendation 34 (guidance and feedback),
- Recommendation 35 (sanctions), and
- Recommendation 40 (other forms of international cooperation), as well as
- Recommendation 2 (National cooperation and coordination).

7. Whatever the approach countries take to financial supervision, they should strive to have effective communication and coordination between AML/CFT supervisors and other supervisory agencies, central banks, finance ministries and any other relevant authorities. AML/CFT supervision can form part of the broader supervision (e.g., safety and soundness or business conduct), or it can be entirely separate. However, AML/CFT supervision must be included in whichever model a country chooses and cannot be undervalued.

8. The AML/CFT supervisory model is a national decision that should be adopted taking into consideration the structure and risk of the financial sector in each country. The FATF acknowledges that different institutional arrangements are capable of meeting the FATF Standards. The arrangements in place should meet the technical requirements noted in Paragraph 6, and be capable of being effectively implemented. Box 1 below sets out the principal models used by many countries, but is not an exhaustive set of options.

9. The integration of AML/CFT supervision into the broader framework of prudential and/or business conduct supervision can leverage synergies, expertise, and resources to enhance the effectiveness of both overall supervision of financial institutions and AML/CFT supervision. Likewise, the integration of AML/CFT supervision with the financial intelligence functions may provide strong synergies, allowing a more targeted supervision based on identified ML/TF risks.

10. The role of supervision in the AML/CFT framework is to supervise and monitor financial institutions to ensure their effective assessment and management of ML/TF risk and compliance with AML/CFT preventive measures. Sometimes these measures need to be prescriptive, for example, for foreign politically exposed persons, while at other times they need to be risk-based, for example, customer due diligence measures on other types of customers. AML/CFT supervisors assess institution's policies, procedures and controls for identifying and managing ML/TF risk, and take remedial action where appropriate. It is not a "tick the box" approach; it requires judgement in

understanding the characteristics and situation of every financial institution. In the event that weaknesses in risk management programmes or breaches of laws or regulations are identified, AML/CFT supervisors should apply a proportionate range of remedial actions to address the identified weaknesses including appropriate sanctions that may include financial penalties for more severe breaches of AML/CFT legal or regulatory requirements.

11. Additionally, the mutual evaluations conducted by the FATF from 2014 to date suggest that supervisors need to pay more attention to the implementation of targeted financial sanctions (TFS), as outlined in Recommendations 6 and 7, in the financial sector. Generally, supervisors paid a low level of attention to compliance with TFS. The FATF Standards require that supervision be applied to TFS implementation but leave it to countries to determine how to implement the requirement. A range of options is available, depending on the national institutional arrangements: for example, responsibility could be assigned to sector financial regulators, the AML/CFT supervisor or enforcement unit or law enforcement. Countries that assign TFS to their external affairs or finance ministries could assign enforcement to such agencies.

Box 1. **Examples of financial supervision models**

Integrated Approach	Single universal supervisor performs both safety and soundness supervision function and conduct-of-business regulation for all the sectors of financial services business.
Twin Peaks Approach	Separation of regulatory functions between two or more supervisors: for example, one that performs the safety and soundness supervision function and the other that focuses on conduct-of-business regulation.
Functional Approach	Supervisory oversight is determined by the business that is being transacted by the financial institution, without regard to legal status. Each type of business may have its own functional supervisor.
Institutional Approach	Financial institution's legal status determines which supervisor is tasked with overseeing its activity.

Source: *Adapted from* The Structure of Financial Supervision: Approaches and Challenges in a Global Marketplace *(Group of Thirty, 2008)*

12. For example, when AML/CFT supervision is an integrated part of the broader supervisory process, AML/CFT supervisors may have broader and more direct access to relevant information on each financial institution (such as on quality of the management, quality of the internal control systems, quality of the risk management systems, level of the compliance culture, etc.), which may allow for an advantage of resource, expertise and cost efficiencies in conducting their AML/CFT supervision. Under the scope of an integrated approach, it is also possible to have a separate team/unit within the single supervisory agency that specializes on the AML/CFT supervision. Such an approach may facilitate ongoing interaction between the prudential and AML/CFT supervision while allowing better specialization and capacity building in AML/CFT supervision.

13. Where AML/CFT supervisors are not the competent authority for prudential or business conduct supervision, countries remain responsible for ensuring that AML/CFT supervision meeting

the Core Principles standards set out in Recommendation 26 is applied effectively. Cooperation between the AML/CFT supervisor and the prudential supervisors[9] can be an effective way of applying Core Principles supervision in the AML/CFT space, avoiding the necessity for the AML/CFT supervisor to duplicate work already being done in the prudential sector.

14. Equally, prudential supervisors who are not the designated competent authority for AML/CFT supervision should be aware of the consequences and implications of their supervised institutions' failures to adequately identify and manage ML/TF risks. Conversely, AML/CFT supervisors should understand how AML/CFT deficiencies may impact prudential supervision (e.g., impact on safety and soundness). This is particularly important in cases involving global, systemically important financial institutions where prudential supervisors can advise on any unintended consequences on confidence in, and the stability of, the institution and global financial system.

[9] Throughout this paper, the terms *prudential supervisor* refers to Core Principles supervisors who may or may not have responsibilities for carrying out supervisory functions that are related to the implementation of the FATF Recommendations and requirements to combat money laundering and terrorist financing.

III. BASIS OF AN EFFECTIVE SUPERVISORY SYSTEM

15. The effectiveness of a country's supervisory regime is based on a number of factors, as set out in the Immediate Outcome 3 of the FATF Methodology, including, but not limited to:

a. How well does licensing, registration or other controls implemented by supervisors or other authorities prevent criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions? How well are breaches of such licensing or registration requirements detected?

b. How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions?

c. With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions are complying with their AML/CFT requirements?

d. To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?

e. To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions?

f. How well do the supervisors promote a clear understanding by financial institutions of their AML/CFT obligations and ML/TF risks?

16. These are explored in greater detail below.

A. MARKET ENTRY

17. Market entry controls (e.g., licensing or registration) are meant to prevent criminals or their associates from owning, controlling, holding a significant or controlling interest, or holding a management function in a financial institution.[10] Such controls should be applied at the time of initial licencing or registration of the financial institutions, and also to the directors or members of senior management when new persons are appointed to these positions.

18. While supervisory arrangements vary across countries, all financial institutions should be created and/or licenced/registered in accordance with laws or enforceable means, and policies and procedures that include AML/CFT laws and regulations, in addition to any other requirements. Examples of practices that have proven to be effective include conducting fit and proper tests and/or background checks prior to granting market entry, including, when needed, beneficial

[10] See the FATF Methodology criteria for Recommendation 26: "26.2 Core Principles financial institutions should be required to be licensed. Other financial institutions, including those providing a money or value transfer service or a money or currency changing service, should be licensed or registered. Countries should not approve the establishment, or continued operation, of shell banks."

ownership determination. This is an instance where supervisors may seek information from law enforcement or share with the relevant authority's information discovered by the supervisor or any third party conducting a fit and proper test and/or background check.[11] This may lead to rejecting applications for reasons of criminality, fitness or propriety, as well as taking appropriate action when applicants make misrepresentations that allow them to obtain a charter or license.

Examples illustrating various approaches to market entry

Example 1. **"Fit and proper tests" (United States)**

All banking institution applicants are subjected to "fit and proper tests" that include background checks. Should applicants have a criminal history, they are either denied participation or undergo a thorough review to determine if their past criminal history would negatively impact their ability to operate a financial institution. In cases where applicants omit information that would expose their criminal record, federal and/or laws and regulations allow for civil or criminal recourse. For example, the *Background Investigations* (2009)[12] booklet of the Comptroller's Licensing Manual incorporates policies and procedures used by the OCC to review the background of persons and certain companies (filers) interested in entering the national banking system, acquiring control of a national bank, and/or influencing its operations; *Changes in Directors and Senior Executive Officers* (2009) booklet which incorporates policies and procedures used by the OCC to review and evaluate changes in directors and senior executive officers.

Example 2. **Registration of MSBs (Canada)**

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is the responsible authority in Canada for the registration of MSBs under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). In order to register with FINTRAC, MSBs have to provide identifying information and other business information in a registration form. FINTRAC's MSB registration program provides telephone assistance to potential MSB registrants, and throughout pre-registration, registration, renewal, denial, cessation and expiration process.

FINTRAC MSB registration process involves a criminal records check. Individuals convicted of the following offences are ineligible to own or control an MSB:

- money laundering or terrorist financing,
- an offence under certain sections under the PCMLTFA,
- an offence under most sections of the Controlled Drugs and Substances Act, and
- an offence under certain sections of the Canadian Criminal Code.

Should it be determined that an individual or entity that owns or controls the applying entity is ineligible, the application for registration is denied. It may also happen that, when FINTRAC

[11] Alternatively, supervisors may require regulated entities to obtain the relevant information themselves and certify their compliance to the supervisor.

[12] Office of the Comptroller of the Currency (2009a).

performs the criminal records check, the individuals have been charged with offence that makes them ineligible, but they are not yet convicted. In these instances, FINTRAC performs a regular follow-up on the criminal record check to ensure that the MSB registration is revoked upon conviction. FINTRAC also monitors open source information to be aware of charges laid against previously eligible MSB owners.

In addition, FINTRAC scrutinizes MSBs and potential MSBs on an on-going basis. FINTRAC requires MSBs to submit updated information on owning or controlling individuals or entities when changes occur and again when the MSB applies for renewal of its registration every two years. This information is verified again. FINTRAC also has a process of searching for unregistered MSBs through open source and by visiting them.

When an MSB registration is denied, revoked, expired or pending, FINTRAC conducts a "reporting entity validation" which is a brief off-site review or on-site visit to the MSBs' last known address to establish if the MSB is still in operation. This ensures that the entity is not operating illegally. FINTRAC may also impose administrative monetary penalties (AMPs) on MSBs for failure to register, failure to submit an application in prescribed form and manner, and failure to submit notification of changes.

Example 3. **Prudential supervisor of federally regulated financial institutions (FRFIs) (Canada)**

Under the Bank Act, the Office of the Superintendent of Financial Institutions (OSFI) arranges for criminal and other background checks on the planned owners and operators of financial institutions. In addition, OSFI has prudential guidance in place that requires banks and other financial institutions to conduct background checks on directors and senior managers of federally regulated entities when these persons change. OSFI refers to such persons as "Responsible Persons". When conducting an AML/CFT onsite assessment, OSFI reviews the FRFI's compliance with this guidance and tests the application by reviewing the conduct and results of background checks. These reviews are particularly useful for assessing the processes around obtaining background information for individuals who have not resided in Canada.

For new applicants for banking or other financial institution licences, OSFI also reviews the planned AML/CFT risk assessment and compliance programs as part of the application process with an emphasis on the Applicant's business plan and model, prior to the issue of Letters Patent by the Minister of Finance. If a potential financial institution does not seem to understand the risks, or address the AML/CFT requirements satisfactorily, the application is delayed from proceeding to Ministerial approval until issues are closed.

For applicants who already operate businesses which will be transferred to a financial institution status, the evaluation also includes an abbreviated on-site assessment as part of OSFI's general pre-commencement exercise designed to determine operational readiness.

Example 4. **Technical report before registration (Mexico)**

Derived from the Financial Reform, specifically with the modifications made to The General Law of Organizations and Auxiliary Credit Activities (LGOAAC), the obligation of Money Exchange Centers

(MSBs) and Money Transmitters to obtain the Technical Report on the prevention of Money Laundering and Terrorist Financing (ML/TF) was implemented.

Technical Report is a tool that contributes to generate confidence in the financial sector and users of Money Exchange Centers and Money Transmitters. While it does not replace the function of supervision, which is in charge of the National Banking and Securities Commission (CNBV), Technical Report evaluates and verifies the implementation of measures and recommends implementation of best practices. The report is valid for three years from their issuance.

On 8 September, 2014, the deadline for the Money Exchange Centers and Money Transmitters to process their application for renewing their registration with the CNBV expired, for which, they must had obtained in advance a Technical Report on the ML/TF prevention.

The CNBV expects that compliance with the regulations of the Financial Reform, through obtaining the Technical Report will contribute to build trust among the sectors under the supervision of the CNBV. It is important to note that the Technical Report is a requirement to apply for or renew the registration for Money Exchange Centers or Money Transmitters with the CNBV. However, obtaining Technical Report does not involve the granting or renewal of the entity's registration; it only shows the general compliance regarding the AML/CFT measures: it does not prejudge proper registration application of the entity.

Example 5. **Visit to newly authorised institutins (Mexico)**

The supervisor performs visits to newly authorised FIs, prior to its start of operations. These visits are comprehensive reviews of all aspects of compliance with AML/CFT regulations, including: fit and proper test of the corporative structure (background of the legal person members), effective customer identification programs, know-your-customer policies, AML manual (document containing all relevant AML policies, procedures and internal structure (corporate governance) schemes according to the applicable legal framework), AML risk matrix, reporting obligations and an automated system to detect and make STRs and CTRs in a timely manner.

B. UNDERSTANDING THE ML/TF RISKS

19. As stated in Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment,[13] countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This risk-based approach should be an essential foundation to efficient allocation of resources across the AML/CFT

[13] The types of information that might form the basis of the supervisor's risk assessment include, but are not limited to: national risk assessments, information collected from reporting entities either off-site or on-site, the results of examinations and supervisory processes, and information from the FIU, including typologies and feedback on suspicious transaction reports.

regime and the implementation of measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks

20. The 2014 *RBA Guidance for the Banking Sector*, particularly Section II – Guidance to Supervisors, contains relevant guidance explaining how to develop an understanding of the ML/TF risks which should then inform the supervisor's inspection plans and approach. It should be noted that the broad principles contained in this guidance may also be directly relevant to the supervision and monitoring of other sectors. As it notes: "When assessing ML/TF risk[14], countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identified affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures[15]. The RBA is not intended to be a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate ML/TF risks, but it is still used for ML or TF purposes."[16] Additionally, when financial institutions do not effectively mitigate the risks due to a failure to understand risks, implement an appropriate risk-based approach, or failure of a risk-based programme that was not adequate in its design, the competent authorities should take action to ensure financial institutions correct any deficiencies in risk management and improve future compliance with AML/CFT requirements, as set out below. [17]

C. SUPERVISION AND MONITORING TO MITIGATE ML/TF RISKS

21. Ongoing AML/CFT supervision comprises assessing the quality of controls designed to detect and deter ML and TF based on the assessed risks, including controls that are required by law or regulation. Such supervision is applied through off-site and on-site examinations, which can include questionnaires and dedicated meetings. The three global standard setting bodies have established the Core Principles: the standards for effective supervision and regulation by competent authorities, which are also relevant for AML/CFT supervision as required under Recommendation 26. Under these Core Principles, effective supervision should:

1) be risk-based, focusing on both major prudential and conduct of business risks, as well as a wide range of other risks, such as compliance risk, reputational risk, legal risk and ML/TF risks;

2) be the result of a combination of off-site and on-site supervision;

3) be based on having appropriate access to all the books and records of each supervised financial institution sufficient to collect the widest range of information that a supervisor needs; and

---

[14] *FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment*, Paragraph 10, (FATF, 2010).

[15] *Ibid.* See also Section III.B for further detail on identifying and assessing ML/TF risk.

[16] FATF (2014), Paragraph 10.

[17] See the previous *FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures* (FATF, 2007), at par. 1.13;

4) include the international element of financial institutions or groups operating across borders by allowing for international cooperation (including arrangements for the sharing of confidential information with foreign counterparts).[18]

22. In a risk-based regime, financial institutions will adopt controls relevant to their business model and assessed risks, and thus not all financial institutions will adopt identical AML/CFT controls. Furthermore, isolated incidents of AML/CFT deficiencies that do not rise to a systemic risk level may not necessarily invalidate the integrity of a financial institution's AML/CFT controls. At the same time, financial institutions should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

FEATURES OF EFFECTIVE CONTROL/MONITORING PROCESSES

23. The supervisor should take adequate measures to identify and understand the ML/TF risks faced by financial institutions and sectors in its country, and internationally. These risks include, at minimum, the ML/TF risks associated with financial institutions' customers, products, geographical reach and delivery channels. The risk profiles of supervised entities should be reviewed periodically, including where there has been a change in circumstances, such as changes in management or business activities. Additionally, when determining the approach to supervision in a particular sector, in line with the RBA, supervisors should consider the capacity and AML/CFT experience of the sector being supervised. Supervisors may have greater expectations of sectors with greater AML/CFT capacity and which, in turn, should inform the supervisor's approach[19]. In other words, what constitutes an effective supervisory approach for the banking sector may not be a suitable approach for other types of financial institutions (i.e., those not subject to Core Principles or prudential regulation).

Example 6. **On-going monitoring tool (France)**

Each financial institution under AML-CFT supervision of the ACPR resets, each year, its answers to a questionnaire in the field of AML-CFT compliance.

This questionnaire is composed of ten parts and includes in particular questions related to:

- the organization and governance of the AML-CTF system;
- the implementation of the customer due diligence measures and of the reporting obligations to the FIU, including collection of statistical data ;
- the internal process and the institution's tools of the targeted financial sanctions related to terrorism and terrorism financing.

It is accompanied by an annual report of internal control which completes the given answers.

[18] The Core Principles are in line with Recommendation 26.

[19] Paragraph 1, Interpretive Note to Recommendation 1.

24. Financial institutions that are assessed as higher ML/TF risk by supervisors should be subject to closer supervision, such as more frequent and/or more comprehensive AML/CFT examinations/inspections (e.g., where there are indications that a ML/TF risk may have crystalised). There should be an analysis and decision process underpinning this risk-based AML/CFT supervision. The FATF's *Guidance for a Risk-Based Approach for the Banking Sector* has more detail on this.[20]

25. Supervisory examination processes should include:

a. The supervisor should have clear and adequate methodologies and procedures for off-site supervision and on-site inspections. Off-site monitoring tools could include (self-assessment) questionnaires on the policies, procedures and controls in place in financial institutions. On-site assessment tools could include assessing the adequacy of AML/CFT controls, such as management reporting and oversight. In the Core Principles sector it is normal to include in the assessment a review of the financial institution's internal or external audits. Supervisors should consider interviewing members of the Board of Directors, staff of various levels of seniority and with different functions (e.g. senior management; compliance; internal audit/control functions; and customer-facing staff), assess procedures and policies in place and/or conduct testing (e.g., review of customer files, testing effectiveness of a transaction monitoring system, suspicious activity reporting, training and integrity of staff) to assess effective implementation of the financial institution's policies and controls. Sample testing is a particularly important tool when examining for compliance, both for risk- based and rules-based requirements.(e.g., the implementation of targeted financial sanctions).

b. The supervisor should ensure that officers carrying out AML/CFT inspections are adequately trained and have up-to-date knowledge of AML/CFT issues.

c. In addition to supervision at individual financial institutions, the supervisor should, where appropriate, conduct risk-based assessments across all or part of a financial sector where the supervisor considers the risks warrant this approach: for example, where a group of financial institutions face the same threats and vulnerabilities.

d. Where appropriate, the supervisor should conduct consolidated AML/CFT supervision of the overseas branches and subsidiaries of financial institutions headquartered in its country via off-site supervision and on-site inspections.

e. The supervisor should also consider taking risk-sensitive measures to inspect or review financial institution's governance and controls over third party service providers where AML/CFT measures are outsourced to others as agents of the financial institution, in order to determine whether the inspected financial institution's arrangements comply with its AML/CFT obligations.

[20] See footnote 3.

SUPERVISORY COORDINATION AND COOPERATION

26. Where more than one competent authority is responsible for supervising and enforcing the AML/CFT compliance of a financial institution, supervisory action should be coordinated, where appropriate, with other relevant competent authorities. Where more than one competent authority is responsible for supervising a financial institution at the domestic level (e.g., where the financial institution has both an AML/CFT supervisor and a separate prudential supervisor), such coordination and cooperation should occur among all relevant domestic supervisory authorities. Where the financial institution operates in multiple jurisdictions and is subject to supervision by competent authorities from different countries, such coordination and cooperation should occur internationally. This is particularly relevant where the institution involved is systemically important and/or operates in more than one country. Coordination can include coordination on supervisory approaches, coordination of supervisory expectations and coordination of supervisory actions (control actions, remedial actions and enforcement actions), and information exchange. Coordination with other supervisors, central banks and finance ministries, and, where relevant, law enforcement is also important.

FEATURES OF EFFECTIVE SUPERVISORY COORDINATION AND COOPERATION

27. Coordination, cooperation and information exchange with other national and international authorities on AML/CFT issues and financial sanctions may be ensured through mechanisms (either AML/CFT specific or broader) such as: legislation authorising sharing of supervisory and/or compliance information, information exchange agreements (e.g., Memoranda of Understanding), established committees, working groups or other bilateral or multi-agency meetings. The applicable confidentiality provisions should be respected and applied to these mechanisms. These arrangements should ensure the timely exchange of information to facilitate the discharge by each authority of its responsibilities.

28. National authorities with which the AML/CFT supervisor may coordinate and cooperate may include:

a. Financial Intelligence Unit (e.g., exchange of information including information on the quality of reports and information on entities; individuals and their transactions where permitted; joint policy actions);

b. Ministry of Finance and other relevant ministries (e.g., to collaborate on policy issues, preparation of laws, regulations and guidance, not exclusively directed at financial institutions);

c. Intelligence Services;

d. Other supervisory authorities relevant for AML/CFT or financial sanctions (e.g., other prudential supervisory authorities, business conduct or financial market supervisory authorities, self-regulatory bodies/organisations where relevant, or those responsible for administering data protection legislation);

e. Public prosecutor's office; and

f. Law enforcement agencies.

29. International coordination and cooperation may include:

a. Regular or ad-hoc cooperation and/or exchange of information in a timely manner, pursuant to specific requests from competent supervisory authorities in other countries;

b. Examination of foreign establishments of financial institutions with the assistance of the supervisory authorities of the host country;

c. Indirect cooperation with non-counterparts, in line with Recommendation 40;

d. Memoranda of understanding, consolidated supervision agreements between home and host supervisors of foreign-owned financial institutions, or other form of agreement which address cooperation and information exchange between authorities in different countries; and

e. Participation in the relevant international meetings (e.g., the Basel Committee, the FATF, the Financial Stability Board, International Organisation of Securities Commission (IOSCO), International Association of Insurance Supervisors (IAIS), EU meetings or other international fora).

Examples of cooperation/coordination with relevant authorities

Example 7. **Special coordinating body (Sweden)**

In Sweden there is a special coordinating body for the supervision of measures against money laundering and terrorist financing. The body comprises representatives from supervisory authorities (FI and the authorities that supervise designated non-financial businesses and professions (DNFBP's)) and the financial intelligence unit (FIU). The body has the overall coordinating responsibility for the operations of the supervisory authorities relating to methods and the issuing of rules, together with the evaluation and follow-up of the supervision performed. The body also provides the supervisory authorities with support on matters relating to training and work to promote efficient collaboration between the supervisory authorities and the FIU.

According to the Swedish AML Act, a supervisory authority shall, without delay, notify the National Police Board (FIU) if the authority upon inspecting a natural or legal person or in any other way discovers a circumstance that may be assumed to be related to or constitute money laundering or terrorist financing.

Example 8. **Regular meetings (Netherlands)**

The Dutch National Bank and the Netherlands Authority for Financial Markets cooperate with criminal justice authorities and other relevant authorities through different cooperative efforts such as the monthly Tripartite meeting (TPO) between financial supervisors, the Fiscal Intelligence and Investigation Service (FIOD) and the Public Prosecutor's Office (OM) or through the Financial Expertise Center (FEC) which is a cooperative effort between various supervisory, investigative and enforcement agencies, working together on a policy as well as operational level. In addition, bilateral cooperation and information exchange with other supervisory authorities and criminal

justice authorities takes place.

The FEC comprises all the organisations that carry out duties related to the financial sector: supervisory authorities; control, intelligence, and investigative agencies; and prosecution authorities. The FEC was founded to strengthen the integrity of the financial sector. It does this by taking preventive action to identify and combat threats to this integrity. The FEC also plays an important role in providing and disseminating information.

Within the TPO, which takes place every month, cases are discussed which might be of interest to either the supervisory authorities or criminal justice authorities. The basic principle of enforcement is that a person is not punished twice for the same offence (*ne bis in idem*). If an administrative punitive sanction has been issued, authorities are not allowed to take criminal action for that same offense (*una via*). If supervisory actions reveal criminal/economic offences (and vice versa), within the TPO the most effective means of enforcement is discussed. Depending on several factors, such as the severity of the offence, criminal intent, recidivism, complexity, damages etc., a choice is made to transfer the case to the criminal justice authorities. It is then however, still possible to also handle this case with administrative powers which are not punitive but corrective.

Example 9. **AML/CFT Steering Committee (Singapore)**

Singapore has a high-level AML/CFT Steering Committee that leads the national effort to develop and implement its AML/CFT regime. The Committee comprises the Permanent Secretary of the Ministry of Home Affairs (MHA), Permanent Secretary of the Ministry of Finance (MOF) and Managing Director of the Monetary Authority of Singapore (MAS), heads of the respective agencies.

The Committee's mandate is to coordinate the whole of government approach to prevent and combat ML/TF by overseeing the effective implementation of AML/CFT measures by the respective agencies; and identifying and mitigating emerging ML/TF risks (e.g., through the National Risk Assessment exercise). The Committee meets 3 to 4 times a year, or more often if necessary. The AML/CFT Steering Committee is supported by an Inter-Agency Committee (IAC) made up of the key agencies in Singapore's AML/CFT regime.

Example 10. **Cooperation/ coordination with relevant authorities (United Kingdom)**

The UK's Financial Crime Network (FIN-NET) facilitates the sharing of financial crime related information between members - comprising of regulators, law enforcement and government departments. Established in 1992, in response to the collapse of the Bank of Credit and Commerce International (BCCI), the network helps to ensure the right people are communicating to the right people at the right time across an array of financial crime issues, including money laundering and terrorist financing.

FIN-NET has approximately 110 members from public sector organisations from both UK and overseas authorities. It relies on each member having a single point of contact that specialises in financial crime matters. Where members have a shared interest in a case then a meeting may be held to ensure that all parties are aware of the full intelligence picture; to help avoid duplication of effort; and to assist members in collaborating on a joint investigation. Typically around 180 requests

for information are made by members each year which can lead to positive results.

FIN-NET is an independent body - it is accountable to a Steering Group which is chaired by the UK Government's Home Office. The UK's Financial Conduct Authority provides the secretarial function of FIN-NET as well as being a member of the network itself.

D. REMEDIAL ACTIONS AND SANCTIONS

SUPERVISORY REMEDIAL ACTIONS

30. As the FATF Recommendations require, supervisors should have a sufficient range of sanctions available that can be applied proportionately to greater or lesser breaches of supervisory requirements. This range should extend from taking informal remedial actions to taking formal supervisory actions. Sanctions applied in practice should address the specific deficiencies identified, effective at ensuring future compliance by the sanctioned institution, and dissuasive of non-compliance by others.

31. Remedial actions should seek not only to correct weaknesses in processes, procedures, systems or controls within financial institutions, but also to influence and foster a corporate culture that contributes to effective risk management and compliance with national laws.

32. Remedial measures imposed by supervisors should be proportionate to the severity of the deficiency identified. They may include action plans and timelines, and supervisory follow-up to ensure that the required measures are effectively implemented. These plans, timelines and follow-up may include sufficient detail in terms of required action, deadlines and the nature of supervisory follow-up.

FEATURES OF EFFECTIVE REMEDIAL ACTIONS

33. **Communication to financial institutions:** Supervisors should communicate clearly with financial institutions when issues arise, so that the financial institutions understand what their failings and shortcomings are, what supervisors expect (including the remedial action required), and the timeframe within which possible remedial work/actions must be completed. Supervisors should appropriately escalate issues to senior management and/or the Board of Directors in instances where required remedial actions respond to major issues, are of high impact or where previous supervisory intervention has not been effective. Supervisors should determine whether their finding is an isolated incident caused by a specific factor/issue or a systemic risk at the financial institution, or across the sector, and communicate their views to the relevant financial institutions.

RANGE OF TOOLS USED, COMPREHENSIVENESS AND ESCALATION PROCESS

34. The supervisor should be able to apply a wide range of supervisory measures, such as warnings, action letters, limitations and conditions for activities of the financial institution, which may be progressive in severity, requiring financial institutions to remedy AML/CFT control deficiencies and any breach of AML/CFT obligations or failure to mitigate ML/TF risks in a timely

manner. Home supervisors receiving such warnings or signals should aim at addressing the issues, and should seek to apply the necessary supervisory tools to prevent an institution from lowering the AML standards in host country. The supervisor may require the financial institution to obtain an independent audit/test of their policies, procedures and controls in place to ensure compliance with applicable rules, regulations and guidance.

35. In the case of financial institutions under the consolidated supervision of foreign regulatory authorities (home supervisor), the host supervisor may send findings to the home supervisor and head/parent office of the financial institution so that they are aware of the weaknesses identified and to seek their co-operation to ensure that the financial institution rectifies the weaknesses noted during the inspection.

36. The supervisor may follow up with external/internal auditors of the financial institution and request them to follow up on the correction of weaknesses and the adequacy of the remedial measures taken by the financial institution.

CONSISTENCY

37. The supervisor should work closely with financial institutions in order to be satisfied that the targets and deadlines of the remedial actions are well understood and capable of remediating the identified issues within acceptable timeframes. Follow-up of implementation of remedial actions should be systematic and there should be an appropriate response where financial institutions fail to fix the identified problems in a timely manner. Follow-up actions include utilizing inspection/examination information to track progress in supervised entities over time.

38. The supervisor should apply consistent policies with respect to remedial actions, while taking into account the specific characteristics of the financial institution. The supervisor should apply comparable, proportionate solutions to similar issues/cases.

39. Where more than one competent authority is responsible for supervising the same financial institution, those supervisors should coordinate to ensure that a consistent and coordinated approach is being taken to AML/CFT supervisory and compliance issues.

40. If the AML/CFT supervision and prudential supervision are being conducted by separate specialized teams or units within the same agency, these two units should coordinate to ensure that a consistent and coordinated approach is being taken to AML/CFT supervisory and compliance issues.

41. **Outcomes:** Supervisory measures should lead to adequate changes in behaviour of financial institutions (e.g., strengthening of AML/CFT controls, hiring experienced AML/CFT compliance officers, enhancing AML/CFT training of officers in the financial institutions).

Examples of sanctions and other remedial actions from various countries

Example 11. **Range of measures (Netherlands)**

When deciding on an intervention strategy a choice will be made from three different strategies for influencing the supervised institution: educational (explaining and/or supporting), normative (persuading and/or guiding) and deterrent (punishing and/or rewarding). In some cases, explaining the background to a standard or norm suffices, while in others it will be necessary to impose a sanction. A choice can also be made between a group and individual approach; formal measures will always be targeted at an individual institution. Interventions are geared to the specific situation, cause and severity. In extreme cases, a solution will have to be found on the same day. In other cases, relatively light interventions will suffice and the use of formal enforcement instruments will not be necessary. Choices made are subject to peer review by colleagues, and the choice of enforcement instruments to be used is based on the enforcement policy of the Dutch National Bank and the Netherlands Authority for Financial Markets

Example 12. **Range of measures from advice to criminal prosecution (United Kingdom)**

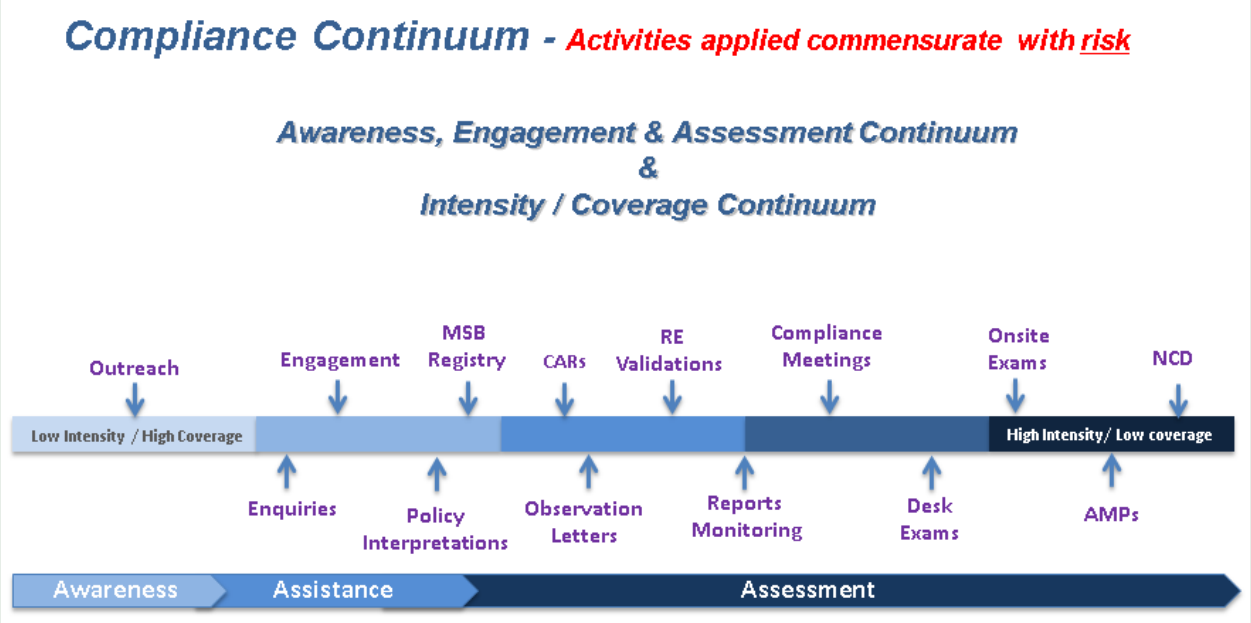
HM Revenue and Customs (HMRC) deals with AML/CFT breaches in a range of ways, depending on the seriousness and potential impact of the breach and the behaviours evidenced by the business concerned.

- Advice – where a business wants to comply but is uncertain it may be appropriate to simply issue advice and guidance to support them in understanding their obligations and ensure compliance.
- Warning letters - these may be appropriate for less serious breaches if there is no previous history of non-compliance. They will set out the improvements that the business must make within a specified timescale to avoid more serious sanctions and will be followed up by further checks to establish whether the business has taken all necessary action.
- Financial Penalties – these are intended to be effective, proportionate and dissuasive and will be applied where there is evidence of regulatory failures and HMRC is satisfied that the business has not taken reasonable steps to comply with their AML obligations.
- Refusal of Fit and Proper person status – This prevents any individual who is considered to pose a risk in relation to money laundering or terrorist financing from holding any management role or controlling an MSB, either directly or indirectly.
- Removal from the register – a business may be removed from the register because a relevant person in the business has had their fit and proper status withdrawn or because the business has failed to provide HMRC with information it has requested by notice.
- Criminal prosecution – The most serious AML regulatory breaches may be referred to law enforcement for potential criminal investigation and prosecution, leading to a sanction imposed by the courts, which could include a fine, non-custodial or prison sentence.

Example 13**. Range of measures on the compliance continuum (Canada)**

FINTRAC possesses a suite of compliance activities that are applied commensurate with various risks and to each sector. These activities range from "low intensity, high coverage" activities to "high intensity, low coverage" activities.

The initial stage of the "compliance continuum" generally refers to "awareness and assistance" as FINTRAC will obtain or provide information to the reporting entities via the following activities: compliance assessment reports (i.e. questionnaires that reporting entities are required to respond to and which help FINTRAC maintain a good knowledge of reporting entities and better assess the risks), outreach, compliance support and engagement. The second stage identifies potential compliance issues (via reports monitoring function that assesses any reporting deficiencies) and advise the reporting entities of these identified compliance deficiencies (through for example an observation letter which outlines to reporting entities their current deficiencies). The third stage comprises of the examination strategy where reporting entities are selected on a risk-based approach for either a desk or onsite exam. This stage also includes the imposition of Administrative Monetary Penalties (AMPs) and Non-Compliance Disclosures (NCD) to law enforcement for potential investigation. This "compliance continuum" is illustrated in the image below.



OSFI's administrative powers of enforcement are derived from its mandate under governing legislation as a prudential regulator. OSFI applies these powers to its AML/CFT supervisory program in the same way as for all other areas of financial institution supervision. The specifics of actions taken in exercising these powers are found in OSFI's Supervisory Framework (available at www.osfi-bsif.gc.ca/Eng/Docs/sframew.pdf) which explains how the level of supervisory intervention is determined. Intervention ratings higher than zero (normal) trigger staging of the FRFI with increased supervisory attention (frequency, depth, breadth) on the issues which caused the staging, including AML/CFT issues. In addition, the potential for staging acts as a dissuasive factor because it triggers increases in Canada Deposit Insurance Corporation premiums (for deposit taking

institutions) and Assuris policy protection (life insurance companies) - it should be noted that all financial institutions subject to AML/CFT supervision by OSFI are required by law to be members of these organizations. Finally, OSFI's findings and any lack of action by a financial institution to resolve the issues identified by OSFI could ultimately lead to the revocation of the financial institutions' licence to operate in Canada, if the issues seriously threaten the safety and soundness of the FRFI.

Example 14. **Banking: Remedial Measures to remedy AML/CFT issues (Canada)**

An AML/CFT assessment of a bank was conducted by the office of the Superintendent of Financial Institutions (OSCI) in March 2010. The bank has a significant retail banking operation in neighbouring and other foreign countries. The OSFI assessment found the bank's AML/CFT programme to be in a basic or rudimentary state. The OSFI assessment identified 27 findings, major deficiencies ranging from non-compliance to weak risk management processes and policies. A severe message was delivered by OSFI to the bank's senior management and Board of Directors.

In November 2011, a follow-up assessment was conducted by OSFI to assess implementation of the bank's plan to address the 2010 findings. There had been little progress made despite changes to governance structure and more senior management engagement.

Concurrently with the 2011 work, OSFI was aware that the regulator of the bank in the neighbouring country had identified similar concerns in respect of the bank's subsidiary operations in that country. In 2012, the supervisor initiated AML discussions with the regulator of the neighbouring country to coordinate the discussions with the bank.

In the summer 2012, OSFI called a meeting with the bank's senior management, including the CEO and the foreign regulator, to discuss concerns on execution risk. In response to the meeting, the Board of Directors and senior management directed that interim controls be developed to improve short-term risk management processes. The bank also struck a senior management committee, chaired by the CEO, to monitor development and appropriate implementation of these controls.

OSFI implemented enhanced monitoring: it typically monitors progress at major banks on a quarterly basis, however, monitoring meetings with this bank were increased to monthly.

A second follow-up on-site assessment was conducted by OSFI in 2013, which found 24 of 28 previous findings had been addressed.

OSFI's enhanced strategies with the bank resulted in a vastly improved AML/CFT programme with increased and constant focus on the implementation of controls appropriate for the size, complexity and risk of the bank.

Example 15. **Targeted Financial Sanctions: Range of measures from no action to criminal referral (United States)**

The Office of Foreign Assets Control (OFAC) administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. On November 9, 2009, OFAC published its enforcement guidance for persons subject to the

requirements of U.S. sanctions statutes, which is outlined below.

Types of Responses to Apparent Violations: Depending on the facts and circumstances of a particular case, an OFAC investigation may lead to one or more of the following actions:

A. *No Action*: If OFAC concludes that the conduct does not rise to a level warranting an administrative response, then no action will be taken.

B. *Request Additional Information*: If OFAC determines that additional information regarding the apparent violation is needed, it may request further information from the Subject Person or third parties, including through an administrative subpoena.

C. *Cautionary Letter*: If OFAC determines that there is insufficient evidence to conclude that a violation has occurred or that a Finding of Violation or a civil monetary penalty is not warranted under the circumstances, but believes that the underlying conduct could lead to a violation in other circumstances and/or that a Subject Person does not appear to be exercising due diligence in assuring compliance with the statutes, Executive orders, and regulations that OFAC enforces, OFAC may issue a cautionary letter, which may convey OFAC's concerns about the underlying conduct and/ or the Subject Person's OFAC compliance policies, practices and/or procedures.

D. *Finding of Violation*: If OFAC determines that a violation has occurred and considers it important to document the occurrence of a violation and, based on an analysis of the General Factors outlined in Section III of its Guidelines, concludes that the Subject Person's conduct warrants an administrative response but that a civil monetary penalty is not the most appropriate response, OFAC may issue a Finding of Violation that identifies the violation.

E. *Civil Monetary Penalty*: If OFAC determines that a violation has occurred and, based on an analysis of the General Factors outlined in Section III of these Guidelines, concludes that the Subject Person's conduct warrants the imposition of a monetary penalty, OFAC may impose a civil monetary penalty.

F. *Criminal Referral*: In appropriate circumstances, OFAC may refer the matter to appropriate law enforcement agencies for criminal investigation and/or prosecution. Apparent sanctions violations that OFAC has referred for criminal investigation and/or prosecution also may be subject to OFAC civil penalty or other administrative action.

G. *Other Administrative Actions*: In addition to or in lieu of other administrative actions, OFAC may also take the following administrative actions in response to an apparent violation:

   1. *License Denial, Suspension, Modification, or Revocation*: OFAC authorizations to engage in a transaction (including the release of blocked funds) pursuant to a general or specific license may be withheld, denied, suspended, modified, or revoked in response to an apparent violation.

   2. *Cease and Desist Order*: OFAC may order the Subject Person to cease and desist from conduct that is prohibited by any of the sanctions programs enforced by OFAC when OFAC has reason to believe that a Subject Person has engaged in such conduct and/or that such conduct is ongoing or may recur.

General Factors Affecting Administrative Action: As a general matter, OFAC will consider some or all of the following General Factors in determining the appropriate administrative action in response to an apparent violation of U.S. sanctions by a Subject Person, and, where a civil monetary penalty is imposed, in determining the appropriate amount of any such penalty:

A. Wilful or Reckless Violation of Law	G. Cooperation with OFAC
B. Awareness of Conduct at Issue	H. Timing of apparent violation in relation to imposition of sanctions
C. Harm to Sanctions Program Objectives	I. Other enforcement action
D. Individual Characteristics	J. Future Compliance/Deterrence Effect
E. Compliance Program	K. Other relevant factors on a case-by-case basis.
F. Remedial Response	

Civil Penalties for Failure To Comply With a Requirement To Furnish Information or Keep Records: In those cases in which a civil monetary penalty is deemed appropriate, OFAC will make a determination as to whether a case is deemed "egregious'" for purposes of the base penalty calculation. This determination will be based on an analysis of the applicable General Factors.

See www.treasury.gov/resource-center/sanctions/Documents/fr74_57593.pdf.

Example 16. **Remedial action from various jurisdictions (United Kingdom)**

Seeking the best supervisory response to change behaviours (UK Financial Conduct Authority (FCA))

In addition to the its formal enforcement powers, the UK's Financial Conduct Authority has a wide range of supervisory responses to improve compliance in firms. It targets resources strategically to achieve 'credible deterrence' in areas of greatest concern. By this the FCA seeks the best means to change the behaviour of those who are the subject of its actions and deter non-compliance by others.

Where firms have deficient AML systems and controls, it will work with them to put appropriate remedial plans in place. Over the last year, the FCA has achieved positive results in firms, particularly around increasing senior management engagement on AML issues, by making use of its 'early intervention toolkit' where it identifies weaknesses. These are a range of measures including, for example, restricting certain types of higher risk business until deficiencies in the firm are fixed. On some occasions, the FCA requires attestations from senior management that weaknesses have been remediated. For example, the FCA recently obtained a voluntary undertaking from a small bank with serious AML weaknesses that the bank would not establish new high risk or PEP relationships until it had corrected the weaknesses the FCA identified. The bank's Chief Executive subsequently gave an attestation that remedial action had been carried out.

The FCA can also appoint a consultant (also referred to as 'Skilled Person') to test a firm's systems and controls, identify weaknesses, and in some cases, remediate the weaknesses identified. It will

also undertake regular follow-up reviews with banks to assure itself that financial crime weaknesses have been rectified and overall compliance standards have improved. Where they have not, the FCA may consider further enforcement action.

Example 17. **Range of measures (France)**

The ACPR is an independent administrative Authority chaired by the Governor of the French central bank, which is in charge of the supervision of the banking sector and insurance sector, including as regards AML-CFT. It uses a range of remedial actions depending on the breaches:

- Follow-up letter: In the context of off-site controls, financial institution must provide explanations and documentation as a case maybe within a time limit.
- Action letter: Following the on-site inspections, a letter is systematically transmitted to the financial institution detailing the authority's findings and to address recommendations within specified timetable.

The ACPR has also administrative enforcement powers which are distinct from sanctions as an escalate means when the nature of the deficiencies is more serious and the financial institution has the ability to correct these deficiencies by themselves.

In the case of enforcing AML-CFT compliance, the ACPR uses its powers of cease-and-desist orders. In this case, the ACPR requires the correction within a specific time limit. At the end of the time limit, a new on-site inspection will be undertaken to make sure that the remedial measures have taken place and, if not, the ACPR has the power to escalate to sanctions measures.

Such administrative enforcement measure may be brought to the attention of the parent undertakings on a consolidated basis.

The ACPR can take sanction measures like a blame or revocation of licence to contraventions and pecuniary sanctions (until 100 thousands euros) in case of serious lack of vigilance or a deficiency in the organization of its internal control procedures and forwards the case to an enforcement authority for criminal prosecution.

SUPERVISORY ENFORCEMENT ACTIONS (SANCTIONS)

42. Serious failures to comply with AML/CFT requirements or failures to address remedial supervisory actions to comply with AML/CFT requirements identified during supervisory examinations or through other means may lead to more severe measures, defined as supervisory enforcement actions (sanctions). The FATF Standards require that supervisory sanctions be effective, proportionate and dissuasive, and be applicable to both natural and legal persons (including the directors and senior management of financial institutions). Effective sanctions seek to change the behaviour of those who are the subject of supervisory actions, deter non-compliance by others and eliminate financial gain or benefit from non-compliance. This is one tool amongst a range of supervisory responses that might be used. Depending on the applicable legal and institutional

framework, supervisors may engage judicial or law enforcement authorities to assist in correcting deficiencies.

43. Supervisory enforcement actions may be public or non-public in nature, and supervisors may take either action, or combine them as needed. Jurisdictions should consider how to strike a balance when deciding to take either public or non-public enforcement action, and deciding on what form of enforcement action should be appropriate. In some cases, non-public supervisory enforcement actions can be highly effective. Additionally, supervisory intervention, particularly when publicised, can lead to focus on the particular area of risk at which the intervention was directed, while other areas could get neglected.

44. When making decisions on the proportionality of a sanction and whether it should be made public, supervisors should consider various factors, including the nature and severity of the identified non-compliance, the financial institution's commitment, the results of previous supervisory interventions to correct the deficiencies, and the possibility of destabilising confidence in the financial sector. Making supervisory sanctions public when appropriate, may contribute to greater transparency of enforcement and deter financial institutions from engaging in similar behaviour in the future, as well as deterring other financial institutions from acting in a similar manner. However, while there can be a deterrent effect in publicizing supervisory actions taken against a financial institution, public action may not always be appropriate, or proportionate, or achieve the intended outcome.

45. Supervisors should be able to take either public or non-public action, or both, in achieving their supervisory objectives, and as such, the absence of public action or the frequent application of non-public action should not be considered indicators of a lack of effectiveness of a country's supervisory system. The use of either public or non-public action, or both, should be recognized as part of the supervisory strategy to ensure the soundness of a country's financial system.

FEATURES OF EFFECTIVE SUPERVISORY ENFORCEMENT ACTIONS

46. There should be a broad range of enforcement measures available to the supervisor. Sanctions should be effective, dissuasive and proportionate, and be applied by different supervisors in a consistent manner, providing legal certainty to the supervised entities. The supervisor may escalate the action if remedial measures are not taken adequately and/or within reasonable timeframes as agreed with the financial institution.

47. Supervisory enforcement action can:

a. range from administrative sanctions, withdrawal of the capacity to be a fit and proper manager, imposition of a temporary limitation to business activities, imposition of a restriction or cancelation of business licences for the most egregious misconduct, to referral to law enforcement or judicial authorities for suspected criminal violation of AML/CFT preventive measures, including with respect to TFS.

b. be both punitive to penalise past behaviour as well as remedial and preventive, to compel financial institutions to take action to prevent future compliance failures and to promote future compliant behaviours;

c. be applied to legal as well as natural persons (i.e. the persons in charge of the administration or the management of the financial institution); and

d. be published, whenever appropriate, as a consolidated report or as rulings of individual cases to promote transparency as well as guidance.

48. **Proportionality of measures:** The supervisor should proportionately sanction financial institutions for AML/CFT breaches in a fair and consistent manner. While the sanction applied to each case would be determined, taking into account a range of factors, including the seriousness of the breach and the extent to which the behaviour was deliberate or reckless, the supervisor should have and inform an enforcement/penalty framework to the respective sectors.

49. **Referral to other authorities:** Where there are severe AML/CFT weaknesses, poor management oversight and/or significant breaches of AML/CFT laws and regulations, and where the supervisor does not have authority to take appropriate enforcement measures against the financial institution, the supervisor should forward the case to the appropriate competent authority. Where the supervisor finds or assumes criminal offences in activities of financial institutions, it should notify the relevant law enforcement agencies and/or prosecutor's office. Section III describes in more detail the relationship between supervisors and law enforcement, and the importance of their cooperation and coordination.

Examples of sanctions (supervisory enforcement actions) from various countries

Example 18. **Banking: Sanctions against management (Italy)**

In 2008, in connection with investigations by the judiciary on some individuals involved in organised crime, the Bank of Italy conducted an on-site inspection on the country's subsidiary of a foreign banking group. The on-site visit revealed serious breaches of AML legislation and serious deficiencies in the internal control system. The subsidiary systematically and wittingly ignored the country's customer due diligence (CDD) provisions in order to facilitate customers' transactions with off-shore entities.

The central bank decided to activate the special administration (SA) tool, which temporarily dissolves (normally up to one year) governing bodies of the bank and replaces them with special administrators appointed by the central bank, and imposed sanctions on old management. The central bank transmitted the findings to the judiciary and FIU. Information was also provided to the bank's parent country's home authorities, which conducted an overall review of the group activities. In 2010, the SA procedure ended and the bank returned to shareholders' hands. It was the first time for the central bank to test the SA for AML purposes. Cooperation with domestic and foreign authorities was also tested.

Example 19. **Currency exchange business: Face-to-face interventions uncovering disqualified person exercising control (United Kingdom)**

The supervisor of money service businesses, HM Revenue and Customs, strengthened its fit and proper person test since October 2012 and it delivered early results in February 2013. The

supervisor carried out a compliance visit to a currency exchange business. The business had previously been deregistered when the owner was convicted of fraud offences and had his fit and proper status removed, but had subsequently re-registered under new ownership. The new owner passed the fit and proper person test and provided information from accountants to evidence the transfer of ownership of the company.

The visiting officer was broadly satisfied with the business' AML procedures but discovered that the previous owner of the business was being employed by the business, which suggested that he continued to exercise control. The officer carried out a detailed investigation into the circumstances surrounding the sale of the company which eventually revealed that behind a complex set of artificial loan arrangements, share purchases and transfers, the new owner had not paid anything for the business.

The officer concluded that the new owner was simply a 'puppet' director and the previous owner was still the beneficial owner and was effectively directing the business. The supervisor withdrew the fit and proper status from the new director on the grounds that he had knowingly allowed a disqualified person to exercise control over the business and deregistered the business immediately. The situation came to light because a compliance visit was carried out at the business' premises, and this illustrates the effectiveness of face-to-face interventions when dealing with high-risk business.

Example 20. **Credit Card Issue: Limiting financial activities (Italy)**

In 2009, the central bank conducted an in-depth off-site review of a credit card issuer, following a report by the Board of Directors concerning deficiencies in the registration procedure. Subsequent on-site inspection confirmed weak AML practices over a long period. The central bank requested the firm to develop an action plan to address the deficiencies and prohibited issuance of new credit cards and imposed a specific capital add-on for operational risks, until completion of the action plan. The central bank informed the judiciary and FIU of these initiatives.

The limitation on business activity and the additional capital ratio were revoked in 2011, after a follow-up on-site visit verified that all deficiencies had been addressed and fixed.

Example 21. **Sanction against a life insurance firm (France)**

The on-site investigation team of the ACPR performed an on-site AML-CFT control at a life insurance firm. This on-site control noted serious failures in the AML-CFT system and policy of this institution, in particular in:

- the business-wide risk assessment established by the institution which did not take into account all of the ML-TF risks it could be confronted with, especially those related to the customers and the activities (those gaps are translated to vigilance defects regards to the business relationships);
- the on-going monitoring system which was insufficient for detecting efficiently all the atypical and suspicious transactions ;
- the customer due diligence measures and in particular, cases of absence of verification of

the identity of the beneficial owner and of insufficient knowledge of the business relationships ;

- the detection process of politically exposed persons which was inefficient ;
- the reporting of suspicious transactions, with identification of several suspicious transactions of high amounts for which no STR has be performed.

A disciplinary procedure has been opened against this French life insurance firm and it resulted to a censure and a financial penalty of an amount of EUR 5 000 000.

E. EFFECT OF SUPERVISORY ACTIONS ON COMPLIANCE

50. The ML/TF risks may evolve and change over time. Consequently, it is important for supervisors to understand what impact their actions are having on the compliance of supervised entities with a view to ensuring that supervision is adequate to mitigate current ML/TF risks. A number of elements can be used to achieve this: the results of follow-up actions, the evolution of a sector or a particular entity's risk profile over time and following supervisory action (e.g., taking into account the adequacy of a financial institution's AML/CFT measures which may change as a result of supervisory action), and the extent to which business moves into the formal financial system or remains in the underground/informal system.

51. In regards to TFS compliance, past recent criminal prosecutions involving large global banks have revealed that some banks engage in deceptive practices to, for example, remove originator and beneficiary information from wire transfers in order to evade sanctions—a process called "stripping." In line with the risk-based approach, given the increasing terrorist threat and this past experience, appropriate implementation of targeted financial sanctions continues to be an area warranting attention from supervisors with a view to determining whether those criminal prosecutions have had a positive impact on the behaviour of those banks.

FEATURES OF EFFECTIVE IMPACT OF SUPERVISION ON COMPLIANCE

52. Ideally, the results of follow-up actions will demonstrate that supervisory actions are having a positive impact on the compliance of supervised entities. In other words, follow-up actions should show that the supervised entity has responded to supervisory concerns in a timely manner (e.g., by correcting deficiencies, or implementing more robust AML/CFT controls) and is mitigating its ML/TF risks better.

53. Follow-up actions include using inspection/examination information and review of the supervised entities' audit reports to track progress over time.

a. **Optimal usage of findings:** The supervisor should facilitate sharing of the findings of AML/CFT inspections among its officers to ensure consistency of supervisory actions/measures. Where the AML/CFT supervision is carried out by different authorities, they should discuss and share the relevant AML/CFT information, exchange

expert guidance/opinions on AML/CFT supervision and ensure consistency in applying AML/CFT standards.

b. **Periodic review:** The supervisor should also take the results of follow-up actions into account when reviewing a sector or particular entity's risk profile, and use this information for the purposes of fine tuning and recalibrating its inspection plans and supervisory approach, as needed, in order to mitigate current ML/TF risks.

54. Entities conducting financial activity underground (i.e., without proper authorisation) are identified, moved into the formal financial system (i.e., registered or licensed), and/or sanctioned, as appropriate.

F. PROMOTING A CLEAR UNDERSTANDING OF AML/CFT OBLIGATIONS AND ML/TF RISKS

55. Effective information processes should ensure that clear, relevant, meaningful and up-to-date AML/CFT-related information is made available to financial institutions. Information provided by supervisors can take any form, be communicated in various ways, and may include changes to the AML/CFT-related legal framework, explanation of the AML/CFT regulatory requirements, relevant typologies, updates on ML/TF vulnerabilities, risks and threats, and regulatory expectations. For example, if a detected risk is new, such risks should be assessed and relevant information should be shared with financial institutions, and supervisors should determine whether additional guidance or other action is necessary. Inconsistent interpretation of AML/CFT obligations can impact the effectiveness of the supervisory regime. Information should be targeted for the audience, and may include guidance (international and domestic), updates, formal and informal meetings.

FEATURES OF EFFECTIVE INFORMATION PROCESSES

56. Disclosed information to financial institutions should:

a. be based on a clear understanding of ML/TF risks (including vulnerabilities and threats) present at both national and international level, specifically within the financial sector as a whole and within each of its subsectors;

b. be targeted, practical, up-to-date, easy to understand and apply;

c. outline supervisory expectations and explain rule-making: for example, it is based on supervisory work (e.g., best practices, bad practices, high risk areas) and on relevant documentation issued by standard setters;

d. help financial institutions to identify ML/TF risks associated with customers, products and services, geographic areas of operations, or their distribution channels, by providing risk indicators and/or typologies for identifying and monitoring risk;

e. clarify that financial institutions should not open accounts, commence business relations or perform transactions, or to terminate business relationships for customers when they are unable to apply appropriate CDD measures (pursuant to the FATF Recommendations); and

f. highlight new requirements, emerging ML/TF risks, and examples of recent supervisory actions, where appropriate.

57. The disclosed information should be easily accessible:

a. The supervisor should use as many different delivery channels as appropriate (e.g., web-based, written exchanges with individual financial institutions, bilateral meetings, seminars, conferences, outreach with representative associations, annual reports, advisory circulars) to communicate with financial institutions, and to enable the information to reach a wider audience.

b. The supervisor's website should be easy to navigate and may include a dedicated page or site for AML/CFT preventive measures, including TFS issues.

58. The supervisor should engage in an on-going dialogue with the its supervised financial institutions. The supervisor should provide a framework for open communications with financial institutions. There should be clear and effective lines of communication between financial institutions and supervisors. Where it is appropriate to give feedback, the supervisor's responses should be clear, useful, and delivered in a timely fashion. Guidance or expectations can be communicated industry-wide through written materials, such as case studies or poor/better practices, or industry-wide training/seminars, so that all financial institutions are informed of good practices.

59. Messages and guidance from the supervisor should be consistent. The supervisor should review its regulations and guidelines on AML/CFT to ensure that they are relevant and up-to-date.

60. The supervisor should consult the industry when proposing to make new regulations or regulatory amendments, and respond to and clarify issues raised by the industry.

Examples of dialogue with the sector

Example 22. **Thematic review to facilitate a root cause analysis (Netherlands)**

Thematic examinations are used to effectively influence the level of compliance of FIs. The examination was on ongoing due diligence measures of banks, life insurers and trust offices. The project focused on the measures regarding periodic review of clients, transaction monitoring, STR reporting, and screening and filtering against the sanctions lists. Thirty FIs, 10 from each sector, were selected based on several factors, such as size, client base and results of previous AML/CFT examinations. The selected FIs received a questionnaire with qualitative and quantitative questions.

The project team analysed all answers using a scoring system, 1 (compliant) to 4 (non-compliant). Based on the scores, several FIs were selected for a further in-depth on-site examination. The in-depth on-site AML/CFT examinations result in a report to the FIs and further enforcement actions in some cases. The sectors are kept informed of the thematic examinations through an annual publication on the themes and regular updates through newsletters.

The project team also made a root cause analysis in each sector: e.g., why a certain sector reports relatively few STRs, is the reason for non-compliance not being able to comply, or not

understanding the requirements? Based on the root cause analysis, additional supervisory approaches are used. For example, round table discussions or seminars in cooperation with the FIU and associations with representatives of FIs, or dialogue sessions with individual institutions to develop good and bad practices. Round table discussions or dialogue sessions result in further guidance.

Example 23. **Thematic review helps illustrate potential vulnerabilities with targeted financial sanctions compliance (Jersey)**

The supervisor is running a thematic review of AML/CFT compliance, covering systems and controls around client screening and sanctions. A self-assessment questionnaire has been completed by all deposit-takers, which was followed by a series of on-site examinations. Deposit-takers were provided with a list of names to pass through screening filters used at the FI. The list aims to test matching capacity of the system, and the exercise has proved very useful in illustrating potential vulnerabilities and demonstrating to what extent management of FIs understand the scope and calibration of their screening arrangements.

Example 24. **Thematic review helps to assess current or emerging risks (United Kingdom)**

The supervisor, the Financial Conduct Authority (FCA), uses thematic reviews to assess a current or emerging risk relating to an issue or product across a number of firms within a sector or market. In 2014, it published its report *How small banks manage money laundering and sanctions risk*. The report was a follow-up to an FSA (the FCA's predecessor) review in 2011 and paid particular attention to mid to smaller sized banks' management of higher risk money-laundering situations. As a result of these reviews, and following consultation with industry, the FCA has since updated its Financial Crime: a guide for firms. This guide provides practical guidance to firms on the steps they can take to reduce their financial crime risk. It is well utilised by industry; it does not contain rules but sets out good and poor practice on the management of higher risk situations so firms can adopt a more effective, risk-based and outcomes-focused approach to mitigating financial crime risk. To further expand its dialogue with industry on its 2014 report, the FCA broadcast its first ever AML thematic review webinar which attracted a large audience from across industry. The FCA is currently exploring similar innovative and effective methods of communicating with industry across other areas of its AML work.

Example 25. **Thematic review to have full knowledge of the sector (Mexico)**

In order to have full knowledge of financial institutions under its supervision, the National Banking and Securities Commission (CNBV) launched in May 2014 the "Know Your Entity Program", which covers in detail FIs' business model, types of their customers, products and services offered, monetary instruments, geographical areas they operate, among other key areas of topics.

Derived from the AML/CFT data analysis from each of the participating entities, recommendations to strengthen its processes and measures to manage and mitigate ML/TF risks are made.[21] This

[21] In accordance with paragraph 22 of the "Guide for Risk-Based Approach for the Banking Sector".

program represents a direct communication channel with the supervised sectors and an effective forum for sharing experiences and concerns between FIs and the authority.

Example 26. **Publication of common findings (Jersey)**

Summary findings reports, based on common findings from on-site examinations, are regularly published, so that licence-holders which did not undergo an examination can learn from issues emerging in the relevant sector. Occasional guidance notes are also published, informed by examination findings. Work is ongoing to produce a guidance note highlighting examples of effective and less effective compliance monitoring arrangements.

Example 27. **Regular meeting with the sector (South Africa)**

Quarterly meetings are held with the association for savings and investment in the country. All issues affecting the industry would be discussed. The regular meetings develop a good relationship between the supervisor and the industry and ensure industry's compliance with the regulatory frameworks, including AML/CFT measures. All issues of non-compliance are referred to the enforcement unit, and its decisions are published.

FIs complete an annual compliance report and submit it to the supervisor. The questionnaire in the compliance report guides FIs. In addition to compliance inspections to the premises of FIs, the supervisor provides guidance and training to FIs by hosting seminars and facilitating workshops on AML/CFT laws and regulations. These supervisory actions have proved effective on the part of FIs to improve overall compliance with AML/CFT legislation and the way to manage AML/CFT risks.

Example 28. **Cross section working groups (Isle of Man)**

The Isle of Man has identified that it is useful to discuss any potential issues with AML/CFT legislation with the industry and not just amongst the regulators. Therefore, if further information on a matter is needed, the FSC is able to send out electronic surveys to licence holders to gather comments / data on the matter. Also, the Isle of Man has established a working group entitled the Joint Anti-Money Laundering Advisory Group ("JAMLAG") which is made up of representatives from the industry, supervisors and professional bodies and is used as a forum to discuss any issues / areas for further development.

Considering a particular case study, the FSC recently undertook a visit to an Isle of Man-based group entity of a global financial services group. The supervisory visit uncovered some issues with AML/CFT compliance. These issues were raised firstly to the local entity and then escalated to the parent company and the supervisor in that country. It became apparent that the business had tried to use one set of procedures / processes across the business and this had not been suitable for that business.

Example 29. The French CCLCB (France)

Each instruction, guideline or position of the ACPR in the field of anti-money laundering and counter financing terrorism (AML-CFT) should, prior to its adoption by the board of the ACPR and its publication, receive an opinion of an advisory committee called the Consultative Commission Anti-

Money Laundering (CCLCB) which has been set up by the board of the ACPR. The CCLCB meets on average every two months. This commission is chaired by two members of the board of the ACPR.

It is composed of :

- all the professional associations of the French banking and insurance sectors (6 for the insurance sector; 4 for the banking sector);
- several representative persons of financial institutions designated by the ACPR.

The French Treasury Department as well as TRACFIN (French Financial Intelligence Unit) participate to meetings of the CCLCB. Other concerned authorities (for example: the Financial Market Authority or CNIL which is the competent authority on the protection of personal data) can as well be invited depending on the studied subjects.

This consultation work, including the development of guidelines, is done during meetings and can also be done by written procedure.

IV. COMPLEMENTARY PROCESSES AND ACTIONS AVAILABLE TO LAW ENFORCEMENT

61. In establishing an effective supervision and enforcement regime, prohibiting and criminalising a particular activity by law or international convention alone is insufficient: laws and regulations also need to rely on enforcement agencies and mechanisms that investigate and prosecute money laundering, financing of terrorism and predicate offences. Law enforcement should seek to prevent, deter and disrupt ML, associated predicate offences, the financing of proliferation of weapons of mass destruction and TF activity. Also, law enforcement should be aiming to deprive criminals of their illicit proceeds and terrorists of the resources needed to finance their activities.[22] While supervisors focus on the process of implementing prevention and detection measures in the financial sector, law enforcement covers investigations, prosecution, and more public punishments for criminal violations that also serve as industry-wide deterrence. Actions taken by law enforcement, where appropriate, may complement effective compliance and supervision – in other words, they take over where supervisors' mandates end.

62. Law enforcement actions are based on criminal and/or civil authority that, in some countries, is contained in the same legislation governing financial supervision. Law enforcement processes and actions are covered in the FATF Recommendations in Recommendation 30 (responsibilities of law enforcement and investigative authorities) and Recommendation 31 (powers of law enforcement and investigative authorities) and are linked to effective supervision and enforcement issues through the criminal sanctions provisions in Recommendation 35 (sanctions), as well as Recommendation 2 (national cooperation and coordination).

A. LAW ENFORCEMENT MECHANISMS

63. The law enforcement mechanism can vary, depending on what makes sense for the country. Some countries may have a dedicated or specialised unit(s) within the police force, FIU, prosecutor's office, and/or court that is able to investigate and prosecute criminal violations of AML/CFT preventive measures. Other countries may allow any law enforcement agency to bring forth criminal charges for ML/TF based on the predicate activity or criminal conduct. For further information on investigatory practices see the *FATF Financial Investigations Guidance*[23].

64. A financial institution may be administratively sanctioned by a supervisor for failure in effective management of ML/TF risks in the institution. To the extent that the failures in the institution result in violations of law or regulation, it may also be subject to criminal sanctions.

[22] See FATF (2012), paragraph 4.

[23] FATF (2010).

Box 2. **Examples of law enforcement mechanisms**

Supervisors with both regulatory and criminal power	Supervisors have the authority to take a range of supervisory actions, and the authority to take criminal actions.
Enforcement referral from supervisor	Law enforcement agency receives referral from supervisor and proceeds with investigation.
Parallel actions / investigations	Supervisor either refers an issue, or independent investigations by supervisor and/or law enforcement reveal an issue and both the supervisor(s) and law enforcement take an appropriate enforcement action.
Direct action by law enforcement agency	Action that is not prompted by supervisory action or an action undertaken independently from ongoing supervisory action.

65. Law enforcement authorities can be involved in a number of ways, and a country should determine which mechanism works best for its regime.

SUPERVISORS WITH BOTH REGULATORY AND CRIMINAL POWER

66. In some cases, supervisors have the authority to take a range of supervisory actions, and the authority to take criminal actions other arrangements.

Example of supervisors with both regulatory and criminal power

Example 30. **Supervisors with both regulatory and criminal power (United Kingdom)**

The UK's Financial Conduct Authority (FCA) takes regulatory action and imposes substantial fines against firms and individuals for AML systems and controls failures. The FCA does not have statutory powers of investigation allowing it to investigate stand-alone offences of substantive money laundering (as opposed to systems failures) but has prosecuted allegations of substantive money laundering in the context of criminal prosecutions (for offences such as insider dealing) brought in furtherance of its statutory objectives. The FCA also liaises closely with other law enforcement agencies to which it refers stand-alone investigations of substantive money laundering.

ENFORCEMENT REFERRAL FROM SUPERVISOR

67. In other arrangements, an AML/CFT supervisor may not have the legal authority to investigate potential criminal activity/conduct by the financial institution and is required by law or by common practice to communicate or make a formal referral to law enforcement. Law enforcement proceeds with the investigation, and based on their policies and procedures, determines whether or not to pursue an enforcement action.

Examples of enforcement referral from supervisor

Example 31**. Enforcement referral from supervisor (BVI)**

It is usually the case that administrative AML/CFT breaches are handled either by the Financial Services Commission (FSC) or the Financial Intelligence Agency (FIA). If during this time it is found that there is some criminal element to the breach, it is then turned over to the police. Conversely, if the police encounter cases that may reveal a breach in the AML/CFT framework, this information is passed on to the police financial investigation unit for further investigation.

The police FIU can, through established memoranda of understanding share information with the BVI FIA and BVI FSC.

Example 32. **Enforcement referral from supervisor (Denmark)**

If *Finanstilsynets* (FSA) inspection/examination reveals breaches, the FSA reports its findings to the State Prosecutor for Serious Economic and International Crime. The Prosecutor will then decide on the merits of the case after due investigation of whether to initiate criminal proceedings. The FSA will issue administrative orders and continue its investigations until all administrative orders have been complied with.

PARALLEL ACTIONS/INVESTIGATIONS

68. In other situations, the supervisor may refer an issue to law enforcement, or an independent investigation by supervisor and/or law enforcement may reveal a breach. Characteristics of parallel actions/investigations include both supervisors and law enforcement using their resources to address the issue and take the appropriate action. Effective coordination between agencies, including announcements of any enforcement decisions, is particularly important where more than one agency is conducting an investigation into the same financial institution at the same time.

Examples of parallel actions/investigations

Example 33. **Parallel investigations (United States)**

Prosecutors and the FIU have complementary authorities to investigate and sanction financial institutions that do not comply with the US AML law. In addition to separate financial supervisors' corrective actions and enforcement action, in the United States, Department of Justice (DOJ), pursuant to 31 U.S.C. § 5322, has authority to bring criminal actions against financial institutions that wilfully fail to comply with the statutory and regulatory obligations under its principal AML law (Title 31 of the BSA). For example, under this authority, DOJ may pursue criminal charges against a financial institution that wilfully fails to comply with its statutory and regulatory requirements for maintaining an AML or customer identification program, reporting suspicious activity or other relevant provisions of the AML law. DOJ does not have any supervisory authority under the BSA.

DOJ has criminal authority for money laundering violations and the ability to prosecute unlicensed

money transmitting businesses.

FinCEN is also authorized to assess civil money penalties against a financial institution, non-financial trade or business, or a partner, director, officer, or employee of a financial institution or non-financial trade or business for wilful or negligent violations of the AML law. These violations can include record keeping, reporting, or failure to maintain and an adequate anti-money laundering program.

- Further, FinCEN may assess a penalty against a person who owns or controls a money services business and does not register with FinCEN.
- For a person who violates the structuring provisions of the AML law, FinCEN may assess a civil money penalty not to exceed the amount of the coins or currency involved in the transactions.
- FinCEN may assess a civil money penalty of not less than two times the amount of the transaction up to USD 1 000 000 against a financial institution that violates the AML requirements of due diligence on correspondent and private banking or the prohibition on correspondent shell banks.
- In addition to the ability to assess civil money penalties, FinCEN is authorised to seek injunctions, enact 311 special measures regulations, and issue geographic targeting orders. FinCEN may bring a civil action to enjoin a person who has violated, is violating, or will violate the AML law.

311 Special Measure regulations are enacted when a country outside of the United States, a financial institution operating outside of the United States, a class of transactions within or involving a country outside of the United States or a type of account is determined to be of primary money laundering concern.

DIRECT ACTION BY LAW ENFORCEMENT

69. An action that is not prompted by supervisory action and undertaken independently from ongoing supervisory action is a direct standalone action. In this mechanism, law enforcement authorities that uncover possible involvement in criminal activity by financial institutions open a criminal investigation to determine if the financial institution is wittingly or unwittingly involved in the activity, and if the financial institution is complying with AML/CFT laws and regulations that are designed to prevent criminal abuse. Law enforcement action may extend to investigate criminal activity by those that abuse the financial institution. Effective coordination should be encouraged between law enforcement and supervisors as an action may have a de-stabilising impact for globally systemically important banks.

Examples of direct action by law enforcement agency

Example 34. **Direct action by law enforcement agency (Denmark)**

According to the Danish AML/CTF Act, the FSA is obligated to complete a summary of all AML/CTF investigation reports, which should include, inter alia, a summary of administrative orders. The summary shall be published by the institution in question on its website and by the FSA on its website as well. On the basis hereof the State Prosecutor for Serious Economic and International Crime may decide to initiate prosecutions *ex officio*, i.e. without a formal request from the FSA.

Example 35. **Slovak Republic (FIU as part of National Police Force)**

FIU serves as central national unit for the area of the prevention and detection of legalization and terrorist financing. FIU disseminates information to law enforcement authoritie (LEAs) obtained according to AML/CFT Law, if the facts indicate that a criminal offence has been committed. FIU within cooperation with LEAs ensures postponement of performing of unusual transaction pursuant to Section 18 of AML/CFT Law related to disseminated cases. On the basis of this act, LEAs have an appropriate time (72 hours) to make a decision about further steps (e.g. seizure of funds on the customer's bank account). In serious cases, FIU acquires information and documents from financial institutions for LEA's further utilization. FIU may also mediate direct contact between LEAs and compliance officer of obliged entity.

FIU is incorporated in the National Criminal Agency, within the organization structure of the Slovak Police Force. The most serious cases and information related to subject under special-interest of other Units of the National Criminal Agency are disseminating to LEAs within the National Criminal Agency. The National Criminal Agency has subject-matter jurisdiction for those crimes for which the Specialized Criminal Court is authorized. In other cases FIU disseminates information to LEAs pursuant to Regulation of Minister of Interior of the Slovak Republic No. 175/2010 on the definition of jurisdiction of police departments of Presidium of Police Force and departments of the Ministry of Interior of the Slovak Republic in detecting criminal offences, identifying their perpetrators and on the procedure in criminal proceedings.

LEAs are independent within process, they are authorised to request cooperation from FIU, other units of Police Force or state bodies.

B. COOPERATION AND COORDINATION

70. Even under the most thorough supervisory framework, there is a risk of a financial institution breaching AML/CFT laws or regulations. In some circumstances, these breaches can result in actions taken by the jurisdiction's judicial or law enforcement authorities, in addition to, or as an alternative to, a supervisory action. For example, a financial institution may be sanctioned by a financial supervisor for failing to effectively manage the institution's ML/TF risks and, to the extent that such failures result in violations of law or regulation, it may also be subject to appropriate criminal sanctions provided by law where appropriate and proportionate, and where it is considered that such action will be effective in improving future compliance.

71. While in some countries, cooperation and coordination may not be mandated by law or regulation, in practice, law enforcement should engage with the supervisor(s) of the investigated financial institution as supervisors can share useful information that may impact the action. For example, where appropriate, supervisors may provide the relevant supervisory information (e.g., examination findings corrective plans) that may be useful to law enforcement during the course of their investigation, as well as information about the systemic importance of the financial institution in the sector. This is also applicable to broader prudential supervisors since they review risks beyond AML/CFT that could have impact on the safety and soundness of financial institutions.

72. Additionally, a parallel investigation by both law enforcement and supervisors, direct action or referral by either authority, and law enforcement and supervisors cooperation can maximize efficiency in resources, and a coordinated approach by both may send separate yet complementary messages to the broader financial community about AML/CFT priorities.

73. On the other hand, the failure of supervisors and law enforcement authorities to cooperate and coordinate in appropriate circumstances may have serious unintended consequences which may, in the worst case, jeopardise an ongoing criminal investigation (e.g., by inadvertently tipping off a suspect).

74. Further, where a financial institution operates in a number of countries and must comply with the laws of those countries, it is essential that law enforcement authorities and supervisors collaborate and coordinate their actions with those in the other relevant countries at both state and national level. Collaboration is particularly important in cases involving global, systemically important financial institutions where enforcement action can have unintended consequences on confidence in and the stability of the institution and global financial system.

FEATURES OF EFFECTIVE LAW ENFORCEMENT COORDINATION (DOMESTIC AND CROSS BORDER)

75. Law enforcement authorities should coordinate their actions with supervisors and other law enforcement bodies. Coordination allows competent authorities to take action under their authorities and promote information sharing between them.

76. The level of coordination may also depend on information sharing practices (e.g., law enforcement authority's or other supervisor's access to STR information for the purpose of supervising implementation of the STR reporting requirements and quality of STRs, transparency of legal persons and arrangements, assessing risk, etc.) and the particular circumstances of the action (e.g., the types of action, whether criminal or civil, or whether other supervisors are also investigating the same conduct). Dialogues should be encouraged among the relevant authorities before public enforcement actions. When violations of AML/CFT regulatory requirements by financial institutions are investigated and prosecuted by law enforcement, coordination between supervisors and law enforcement should be strongly encouraged.

77. The broad objectives of maintaining financial market stability and preserving the rights of consumers may require a supervisor to carefully consider what kind of actions to take and whether they should be publicised or not. Actions by supervisors and law enforcement authorities represent separate but complementary components of a country's overall regulation of its financial

institutions and markets, focusing on different areas of potential weaknesses and deficiencies that require tailored responses.

Examples of cooperation and coordination

Example 36. **Coordination and referrals (United States)**

General Coordination: Law enforcement, the FIU and supervisory agencies coordinate or consult with each other in connection with (i) the sharing of routine BSA/AML information pursuant to Memoranda of Understanding (MOUs); (ii) enforcement actions involving areas of mutual interest, and (iii) policy matters involving BSA/AML. With respect to item (i) the agencies generally have MOUs in place with FinCEN and OFAC for sharing routine examination information and significant problems. Generally, with respect to (ii), the agencies routinely work closely with FinCEN and OFAC and coordinate enforcement actions. The level of enforcement coordination depends on the particular circumstances of the action (e.g., the type of action, whether criminal or civil, or whether other supervisors are investigating the same conduct). In certain cases, the agencies will work closely with FinCEN and law enforcement in identifying and reporting suspicious activity. The agencies will also provide expertise and support to law enforcement in complex cases. The recent high-profile interagency public enforcement actions taken against a major bank involved the efforts of multiple USG agencies (OCC, FRB, FinCEN, DOJ, OFAC and the Office of the New York District Attorney (DANY). In fact, virtually all high profile BSA/AML public enforcement actions have involved coordinated interagency efforts to ensure BSA/AML compliance.

With respect to (iii) FinCEN, the agencies and DOJ coordinate closely on BSA/AML policy matters including rulemaking and the issuance of guidance. Interagency working groups, such as the Bank Secrecy Act Advisory Group (BSAAG) and the FFIEC BSA/AML Working Group, bring together staff from, the various agencies on a regular basis to share information on threats, vulnerabilities and risks and discuss upcoming rulemakings, guidance issuances and other issues related to strengthening BSA compliance and enforcement.

Referrals Generally: Most agencies generally make and receive referrals on an ad-hoc, case-by-case basis. The process for referring matters to criminal authorities, however, can be more formalized at certain agencies because of legal issues that arise in connection with parallel criminal and civil enforcement actions. For example, the SEC has formal procedures for referring matters to the DOJ or criminal investigative authorities. The FDIC refers criminal matters through its Office of Inspector General-Office of Investigations, which acts as a primary point of contact for other criminal authorities. The OCC's Law Department acts as a primary point of contact for law enforcement and routinely coordinates on grand jury procedures and other information sharing processes. Similarly, the FRB's Legal Division acts as a primary point of contact for law enforcement matters.

Example 37. **Cayman Islands**

In 2005, a person of the Cayman Islands was sentenced to three years in prison for his role in an international money-laundering scheme. The person was convicted of assisting Mr. A and Mr. B,

both of the United States, with engaging and benefiting from criminal conduct using a "Ponzi" scheme known as Cash4Titles.

Two companies subjected to fraudulent activity were regulated by the Cayman Islands Monetary Authority (CIMA) pursuant to the Companies Management Law. Through effective exchange of information between the U.S. Securities and Exchange Commission and the Financial Reporting Authority, CIMA conducted onsite inspections of the respective entities to garner further information. This resulted in an application being filed in the Cayman Islands Grand Court with recommendations to have Controllers appointed to both entities in the interest of investors, creditors and public at large; the companies were subsequently placed into liquidation.

Following this case, CIMA implemented an onsite inspection program for trust and corporate services providers.

C. LAW ENFORCEMENT SANCTIONS

78. The role of law enforcement authorities (who operate in the criminal context) is separate from the role of supervisory authorities (who operate in the regulatory context), as are the sanctions available to them.

FEATURES OF EFFECTIVE LAW ENFORCEMENT SANCTIONS

79. Criminal sanctions are available to address instances of egregious conduct (e.g., wilful and deliberate violations of sanctions or AML/CFT measures and/or behaviour which in itself constitutes money laundering or terrorist financing).

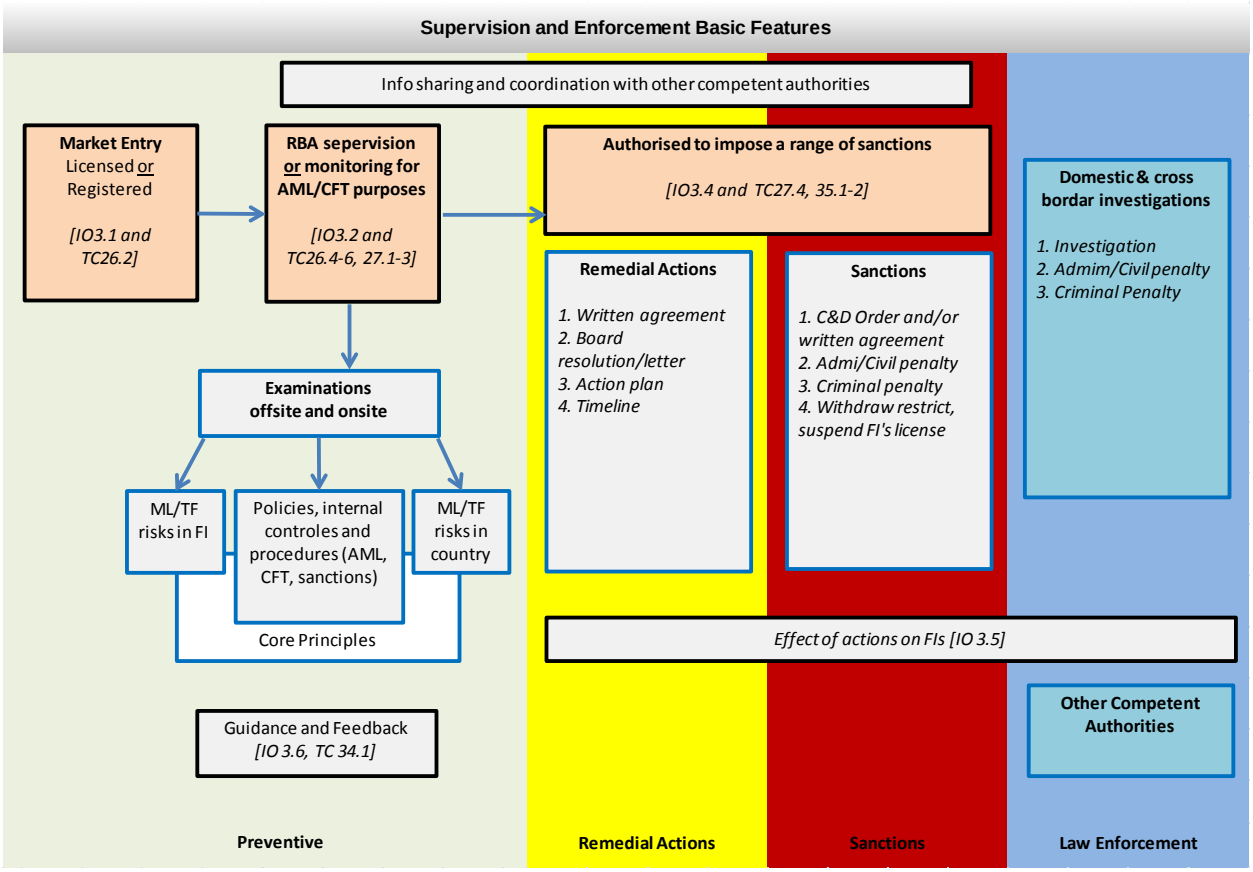
80. The sanctions available to law enforcement authorities include imprisonment, criminal fines and confiscation.

81. Criminal sanctions apply to natural persons and legal persons, unless the latter is not permitted by fundamental principles of domestic law.

V. GRAPHIC OVERVIEW OF THESE ELEMENTS

82. For the purposes of achieving effective compliance with the FATF Recommendations, countries can be guided by the comprehensive graphic overview for effective supervision and enforcement as below.

Graphic Overview of Basic Features of Supervision and Enforcement



BIBLIOGRAPHIE AND REFERENCES

Basel Committee (2012), *Core Principles for Effective Banking Supervision*, Basel Committee, Basel, Switzerland, September 2012, www.bis.org/publ/bcbs230.pdf

FATF (2014), *Risk-Based Approach for the Banking Sector*, FATF, Paris, France, www.fatf-gafi.org/documents/documents/risk-based-approach-banking-sector.html

FATF (2012), *Operational Issues - Financial investigations Guidance*, FATF, Paris, France, www.fatf-gafi.org/documents/documents/operationalissues-financialinvestigationsguidance.html

FATF (2010), *National Money Laundering and Terrorist Financing Risk Assessment*, FATF Guidance, FATF, Paris, France, www.fatf-gafi.org/documents/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

FATF (2007), *FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures*, FATF, Paris, France, www.fatf-gafi.org/publications/documents/documents/fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html

Group of Thirty (2008), *The Structure of Financial Supervision: Approaches and Challenges in a Global Marketplace*, Special Report, Working Group on Financial Supervision, Group of Thirty, Washington, United States, www.group30.org/rpt_06.shtml

IAIS (2013), *Insurance Core Principles*, IAIS, Basel, Switzerland http://iaisweb.org/index.cfm?event=getPage&nodeId=25224

IOSCO (2015a), *Core Principles of Securities Regulation*, IOSCO, Madrid, Spain

IOSCO (2015b), *Credible Deterrence in the Enforcement of Securities Regulation*, IOSCO, Madrid, Spain, June 2015, www.iosco.org/library/pubdocs/pdf/IOSCOPD490.pdf

Office of the Comptroller of the Currency (2009a), *Comptrollers' Licensing Manual*, OCC, Washington DC, United States, www.occ.gov/publications/publications-by-type/licensing-manuals/charters.pdf

Office of the Comptroller of the Currency (2009b), *Changes in Directors and Senior Executive Officers*, OCC, Washington DC, United States, www.occ.treas.gov/publications/publications-by-type/licensing-manuals/ChangesinDirectorSEO.pdf

GLOSSARY

Glossary definitions from the FATF Recommendations, adopted February 2012.

Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[24] 2. Lending.[25] 3. Financial leasing.[26] 4. Money or value transfer services.[27] 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);

[24] This also captures private banking.

[25] This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

[26] This does not extend to financial leasing arrangements in relation to consumer products.

[27] It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

	(b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading. 8. Participation in securities issues and the provision of financial services related to such issues. 9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[28]. 13. Money and currency changing.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala, hundi*, and *fei-chen.*
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities

[28] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Appendix HH:

FATF, *Guidance for a Risk-Based Approach: Money or Value Transfer Services* (Paris: FATF, 2016)

FATF

GUIDANCE FOR A RISK-BASED APPROACH

MONEY OR VALUE TRANSFER SERVICES

FEBRUARY 2016

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2016), *Guidance for a Risk-Based Approach for Money or Value Transfer Services,* FATF, Paris
www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-money laundering / countering the financing of terrorism
CDD	Customer due diligence
DNFBPs	Designated non-financial businesses and professions
FIU	financial intelligence unit
HOSSP	Hawala and other similar service providers
INR.	Interpretive Note to Recommendation
ML	money laundering
MSB	money service business
MVTS	money or value transfer services
NPPS	new payment products and services
R.	Recommendation
RBA	risk-based approach
STR	suspicious transaction report
TCSP	trust and company service providers
TF	terrorist financing

GUIDANCE FOR A RISK-BASED APPROACH FOR MONEY OR VALUE TRANSFER SERVICES

This Guidance should be read in conjunction with:

- the FATF Recommendations, especially Recommendations 1, 10, 14, 16 and 26 (R. 1, R. 14, R.16 and R. 26), their Interpretive Notes (INR) and the Glossary
- the *FATF RBA Guidance for the banking sector*

other relevant FATF Guidance documents, such as:

- the *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*
- the *FATF Guidance on Politically Exposed Persons*
- the *FATF Guidance on AML/CFT and Financial Inclusion*
- the *FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services*
- the *FATF Guidance on the Risk-Based Approach for Effective Supervision and Enforcement*

relevant FATF typology reports, such as:

- *the FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers*
- *the FATF Report: The role of Hawala and other similar service providers in money laundering and terrorist financing*

INTRODUCTION AND KEY CONCEPTS

A. BACKGROUND AND CONTEXT

1. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which were adopted in 2012[1]. The FATF has reviewed its 2009 RBA Guidance for money service businesses (MSBs), in order to bring it in line with the new FATF requirements[2] and to reflect the experience gained by public authorities and the private sector over the years in

1 FATF (2012).

2 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

applying the RBA. This revised version applies to the money or value transfer services (MVTS)[3] sector. The FATF will also review and update its other RBA Guidance papers[4] (based on the 2003 Recommendations), to be consistent with the 2012 FATF Recommendations.

2. The first draft of the RBA Guidance for the MVTS sector was drafted by the MVTS Project group, co-led by the UK and Mexico.[5] Representatives of the private sector were associated with the work and consulted on the draft document.[6]

3. The FATF adopted this updated RBA Guidance for MVTS providers at its February 2016 Plenary.

B. PURPOSE OF THIS GUIDANCE

4. The purpose of this Guidance is to:

- Support the development of a common understanding of what the RBA to AML/CFT entails for MVTS providers, banks and other financial institutions that maintain relationship with MVTS providers and competent authorities responsible for monitoring MVTS provider's compliance with their AML/CFT obligations;
- Outline the key elements involved in applying a RBA to AML/CFT associated to MVTS;
- Highlight that financial institutions that have MVTS as customers should identify, assess and manage the ML/TF risk associated with individual MVTS, rather than avoid this category of customers;
- Assist countries, competent authorities and MVTS providers in the design and implementation of a RBA to AML/CFT by providing general guidelines and examples of current practice;

---

3 These services are included in the FATF Glossary under "Financial institutions: Money or Value Transfer Services (MVTS) at point 4.

4 Between June 2007 and October 2009, the FATF adopted a set of guidance papers on the application of the RBA for different business sectors: financial sector, real estate agents, accountants, trust and company service providers (TCSPs), dealers in precious metals and stones, casinos, legal professionals, money services businesses (MSBs) and the life insurance sector: www.fatf-gafi.org/documents/riskbasedapproach/.

5 The project group was composed of FATF-members (Spain, Switzerland, South-Africa, Singapore, Japan, Norway, European Commission, New Zealand, United Kingdom, United States and Italy), Associate members (GIABA-Secretariat, Moneyval -through Albania, APG- through Sri Lanka, GIFCS-through Guernsey) and Observers (World Bank, UNODC), co-led by the UK and Mexico.

6 Comments were received from Bank of Tokyo-Mitsubishi UFJ, Russian Electronic Money Association, MoneyGram International Inc., Mizuho Bank Ltd, Asociación de Bancos de México, Actors Federal Credit Union, Association of UK Payment Institutions, Banking Association of South Africa, European Payments Institutions Federation (EPIF), Australian Bankers' Association, Union of Arab Banks, World Savings and Retail Banking Institute/European Savings and Retail Banking Group (WSBI/ESBG), Canadian MSB Association, The Netherlands Association of Money transaction offices (NVGTK), Western Union Company and Hong Kong Association of banks (HKAB).

- Assist countries in the implementation of the *FATF Recommendations* with respect to MVTS, particularly Recommendations 14 and 26; and
- Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on preventive and mitigating measures.

C. TARGET AUDIENCE, STATUS AND CONTENT OF THE GUIDANCE

5. This Guidance is aimed at the following audience:

- Countries and their competent authorities, including AML/CFT supervisors of MVTS providers and AML/CFT supervisors of banks that have MVTS providers as customers, and Financial Intelligence Units (FIU);
- Practitioners in the MVTS sector; and
- Practitioners in the banking sector that have or considering MVTS providers as customers.

6. It consists of four sections. Section I sets out the key elements of the RBA and needs to be read in conjunction with Sections II to IV, which provide specific Guidance to MVTS providers (Section II), to supervisors of MVTS providers on the effective implementation of a RBA (Section III) and to banks that have MVTS providers as customers and supervisors of banks that have MVTS providers as customers (Section IV). There are five annexes which provide examples of:

- countries' actions against unauthorised MVTS providers (Annex 1),
- supervisory practices for the implementation of the RBA to MVTS (Annex 2),
- supervisory practices for the implementation of the RBA to banking MVTS customers (Annex 3),
- private sector effective practices in application of RBA (Annex 4) and,
- compliance practices of and in relation to a low risk MVTS (Annex 5).

7. This Guidance recognises that an effective RBA will reflect the nature, diversity and maturity of a country's MVTS sector, the risk profile of the sector, the risk profile of individual MVTS providers operating in the sector and the legal and regulatory approach in the country. It sets out different elements that countries and MVTS providers could consider when designing and implementing a RBA. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the supervisory approach and legal framework as well as the risks present in their jurisdiction.

8. The Guidance takes into account that any financial institution, including certain MVTS providers can be abused for ML or TF. The TF risks were also highlighted in the recent FATF report in the context of emerging terrorist threats[7]. However, the Guidance also seeks to clarify that while certain MVTS providers may act as a conduit for such illegal funds transfers, this should not necessarily result into categorisation of all MVTS providers as inherently high ML/TF risk. The

[7] FATF (2015c).

overall risks and threats are influenced by the extent and quality of regulatory and supervisory framework as well as the implementation of risk-based controls and mitigating measures by each MVTS provider. The Guidance also recognises that despite these measures, there may still be left some residual risk, which would need to be considered by competent authorities and MVTS providers in devising appropriate solutions.

9. This Guidance is non-binding and does not overrule the purview of national authorities, including on their assessment and categorisation of the MVTS sector as per the country or regional circumstances, the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector and may assist competent authorities and financial institutions to effectively implement applicable *FATF Recommendations* using a risk-based approach.

D. SCOPE OF THE GUIDANCE: TERMINOLOGY, KEY FEATURES AND BUSINESS MODELS

Terminology

10. This Guidance applies to the provision of Money or Value Transfer Services (MVTS) as defined by the FATF:

> *Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi, and fei-chen.[8]

11. There is a range of participants involved in the provision of MVTS. For the purpose of this Guidance, the following terminology is used:

- *MVTS provider*: Any natural or legal person who is licensed or registered to provide MVTS as a business, by a competent authority, including through agents or a network of agents.[9] This also includes HOSSPs meeting the aforementioned criteria.
- *Hawala and other similar service providers ("HOSSP")*: Generally referred to as entities that provide MVTS, particularly with ties to specific geographical regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value which is settled through trade, cash and/or net settlement over an extended period of time, rather than simultaneously with the transfer.[10]
- *Agent*: Any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.[11]

---

8 Glossary to the *FATF Recommendations.*

9 Consistent with the definition of *financial institution* in the Glossary to the *FATF Recommendations*. This does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. Refer interpretive Note to Recommendation 16.

10 For a full description, refer to the FATF typology report on *The role of Hawala and other similar service providers in money laundering and terrorist financing* (FATF, 2013b, 12-13). The report also lists out legitimate reasons for existence of these services as well as their vulnerability to abuse based on survey results. In some countries, these types of transactions are considered illegal.

11 Glossary to the *FATF Recommendations.*

MVTS Key features

12. Some of the key features of MVTS are as follows:

- MVTS can be an attractive, often lower cost option for persons that need to send money quickly to another person as funds can be picked up by a recipient in a relatively short timeframe, as opposed to waiting for domestic or international wire transfers that may take several days to process in some cases. The financial service provided by MVTS providers is often cheaper than more conventional banking services and is frequently used in regions with limited or no banking services.

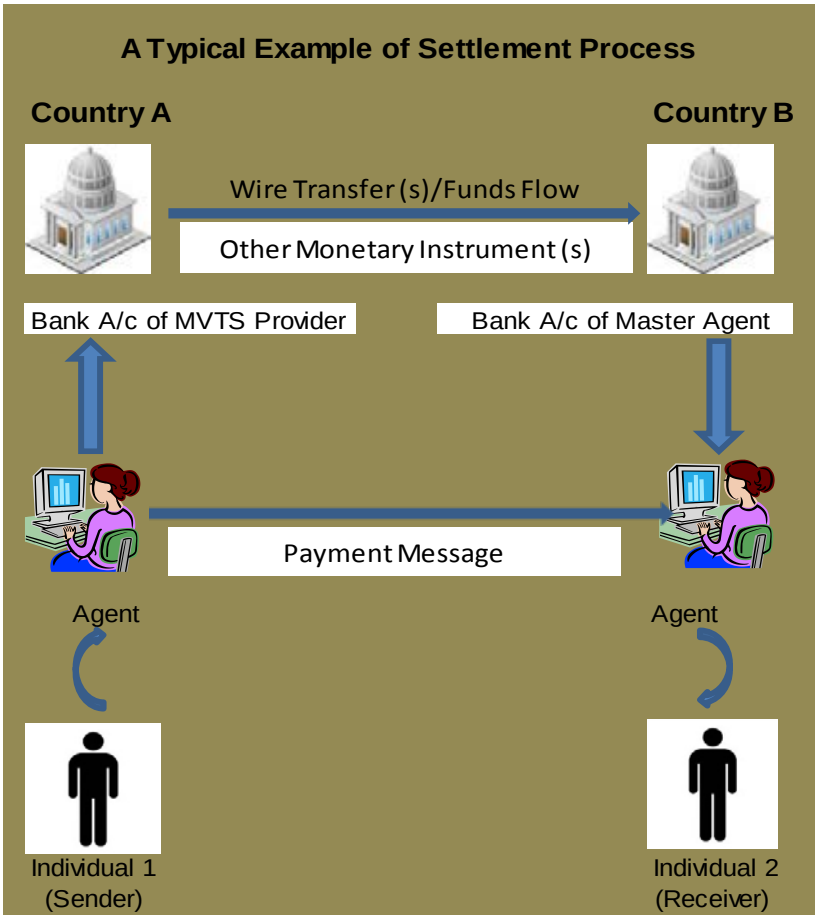
- MVTS providers operate in a variety of ways, but typically a MVTS provider or sending agent (acting on behalf of a MVTS provider) accepts payment of the money transfer, collects the required identification information, and enters the transaction and sender's applicable identification information and the destined receiver systematically at the point of origination.

- In the case of money transfer, the MVTS providers transfer the payment details to the pay-out agent that will provide the funds or their equivalent to the beneficiary of the transfer. The message is either sent directly to the agents or through a centralized clearing house that serves as a centralized hub for information that connects different agents of a provider.

- The money transfer is made available to the ultimate recipient, in the appropriate currency, at a receiving agent (acting also on behalf of a MVTS provider) location in the paying jurisdiction. The receiving agent will also collect and maintain the required identification information at the point of destination in accordance with the local applicable law.

- Pay-out methods vary by jurisdiction, but may include cash, cheque, money order, pay-out cards, mobile wallet, bank deposit or a combination.

13. A simple MVTS transaction and settlement process can be presented as follows:



14. The MVTS sector is made up of a very diverse group of organisations. An MVTS provider may be a small organisation with limited outlet locations such as grocery stores, drug-stores, pharmacies or convenience stores. It may also include a regional network of post offices or banks or other entities, which can be branches or agents. Most licensed or registered MVTS providers hold accounts at banks in order to process transfers and settle accounts with agents both domestically and internationally. However, settlement may be done through wire transfers, often involving aggregated amounts, processed through the international banking system. In addition, settlement can be done through third party payment providers.[12] However, settlement between and among MVTS providers and agents may also be undertaken through cash courier, net settlement or other mechanisms, without any direct wire transfer[13] between the originator and beneficiary.

12 FATF (2013b), p. 14.

13 The term wire transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to beneficiary person at a beneficiary financial institution. The originator and the beneficiary may be the same person. See Glossary Interpretative Note to Recommendation 16.

MVTS business models

15. There is a wide range of MVTS business models around the world. Not all MVTS providers are the same as they vary in size from small independent business to large multinational corporations. Some engage only in domestic transfers and others have a global footprint and transfer funds internationally. Others still may only have limited global transactions or operate in limited corridors, often between two countries that have a diaspora community. Besides the brick and mortar business models, there are also some MVTS providers that operate exclusively through the internet without any physical premise or network of agents. This Section does not seek to provide a complete description of all the MVTS business models; rather it seeks to provide an overview of common business models.

16. For the purposes of this Guidance, MVTS providers generally fall into the following broad groups:[14]

- **Banking institution offering MVTS** – Institutions that provide banking services including acceptance of deposits and other repayable funds from public; lending; and issuing or managing means of payment.[15]
- **Non-banking institution offering MVTS** – Any natural or legal person that provide MVTS as business, including through agents or a network, most commonly without the acceptance of deposits and other repayable funds from public. This includes HOSSP. Non-banking institutions offering MVTS may settle through the banking system and/or outside the banking system by cash or net settlement. Many MVTS providers may settle with agents, through the banking system either through centralized account and sub-accounts or through settlement between a centralized bank account held by the provider and individual bank accounts held by agents of the MVTS. It may also include virtual currency exchangers that fall within the definition of MVTS, where regulated as such.

17. Within the market of non-banking MVTS providers, the size and complexity of the providers vary significantly and various business models are adopted. Providers can include international MVTS providers, post offices, micro-finance institutions, mobile network operators[16], exchange houses, payment institutions[17], escrow account services, bill payment and IT and digital payment services and money transfer operators. Providers of MVTS services typically specialise along retail, commercial and wholesale lines.

---

14 Described based on financial activity being performed and may vary depending upon the regulatory framework of each jurisdiction.

15 Banking activities are activities or operations described in the FATF Glossary under "Financial Institutions", in particular 1, 2, and 5.

16 *Mobile Network Operator*: An entity that provides the technical platform to allow access to the funds through the mobile phone. In some jurisdictions, these can also be MVTS providers if they extend remittance services.

17 The term *"Payment Institutions"* is mostly related to the EU context (Payment Services Directive), which offer payment services alongside banks and other financial institutions.

18. While this Guidance is applicable to all MVTS providers, it is primarily intended for non-banking institution MVTS, including HOSSP. Banking institutions offering MVTS should consider this Guidance in conjunction with the *FATF Guidance for a Risk-Based Approach: The Banking Sector*.

Distribution channels: Agents

19. The nature and structure of agents and their relationships with MVTS providers similarly vary. International MVTS providers often have extensive agent networks spread across multiple jurisdictions. Some MVTS providers operate only domestically. Agents can include small independent entities with a contractual relationship directly with the MVTS provider to provide services on their behalf. Alternatively, agent networks may operate on a tiered structure where an agent operating on behalf of its established network of entities (e.g. through a chain of retail outlets) enters into a contractual relationship with the MVTS provider. Depending on domestic regulations, agents may require licensing or registration. Some agents may be financial institutions or obliged entities in their own right, while others may provide financial services as an ancillary business only.

20. MVTS providers may rely on foreign banks or other MVTS providers to pay funds to beneficiaries through currency drawing arrangements or otherwise, without entering into an agent relationship with these counterparties.

21. MVTS providers that are not multinational institutions may also use agents or a network of agents. The number of agents may be limited and they may be present only in certain geographical areas. In such cases, agents may have a contractual relationship with the principal MVTS provider, or services may be offered on behalf of the MVTS provider without the presence of a formal, written contract.

HOSSP

22. MVTS providers also include providers of *hawala* and other similar services. Providers of *hawala* and other similar services, like many other MVTS providers, generally send remittances of low value, though at times, this may also include high value business transfers. Such providers provide services to migrant communities, operate within a community, and are visible and accessible to their customers. Many such providers often run other businesses in addition to MVTS, and belong to networks of similar operators in other countries.[18] Some hawala providers also offer a more 'mainstream' non-hawala MVTS and mix and match the two approaches.

Relation to NPPS and VC Guidance

23. Some New Payment Products and Services (NPPS) fall within the definition of MVTS and should be licensed or registered and subject to effective monitoring systems as required by Recommendation 14. The *FATF 2013 Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (FATF 2013 NPPS Guidance) is relevant for NPPS

[18] FATF (2013b), p. 13. The report further highlights that while the most significant reasons for vulnerability of these services are jurisdiction-specific, lack of supervisory resources and settlement through value or cash makes HOSSPs transactions particularly difficult for law enforcement to follow the money.

which fall within the definition of MVTS. In some jurisdictions virtual currency exchangers may fall within the definition of MVTS. The FATF published a separate Guidance document on a Risk- Based Approach to Virtual Currencies in 2015.[19]

E. FATF RECOMMENDATIONS APPLICABLE TO MVTS PROVIDERS

24. The *FATF Recommendations* relating to MVTS under Recommendation 14 and its Interpretive Note include specific requirements for countries with respect to MVTS. Additionally, MVTS providers are also considered to be *financial institutions* under *FATF Recommendations*[20] and should be subject to the full range of AML/CFT preventive measures in Recommendations 9-23, including, for example, Customer Due Diligence (CDD), record keeping and reporting of suspicious transactions. R.10 requires financial institutions to conduct CDD measures when:

i) establishing business relations;

ii) carrying out occasional transactions:

   1. above the applicable designated threshold (USD/EUR 15 000); or

   2. that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

iii) there is a suspicion of money laundering or terrorist financing;

iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

25. Under Recommendation 26, MVTS providers should be subject to adequate regulation and supervision or monitoring, having regard to the ML/TF risks in that sector. This is outlined further in Section III(b) of this Guidance.

Box 1. **Recommendation 14: Money or value transfer services**

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use

19 FATF (2015b).

20 MVTS providers are considered financial institutions- Refer point 4 of the definition of the term 'financial institution' as contained in Glossary.

agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

Interpretive Note to Recommendation 14

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the *FATF Recommendations*) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the *FATF Recommendations*.

Box 2. **Interpretive Note to Recommendation 16**

[…]

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

(a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

[…]

Cross-border provision of services

26. Some MVTS providers provide services across national borders through establishments, including through a network of agents operating in another country. Competent authorities of the MVTS provider, acting across national borders with a physical presence through one or several agents established in another country (home country licensing/registration competent authorities), should liaise with the MVTS's host authorities to ensure any ML/TF concerns are adequately addressed[21]. Under the *FATF Recommendations*, countries should ensure that MVTS providers are

[21] Through applicable passport mechanisms. In the context of MVTS' cross border activities through agents established in another country, refer to the directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and

subject to supervision and monitoring for compliance with AML/CFT laws[22], in accordance with the institutional framework of the host country. This is without prejudice to supranational rules that would enable MVTS providers to supply services throughout the supranational jurisdiction on the basis of the legislation prevailing in the countries in which they are situated, without requiring from the host country to impose licensing or registration obligations on entities situated in another country and providing cross-border services.

27. In certain cases, MVTS are also often offered over the internet and there may be no physical presence (i.e. head office, branch or agent network) in the country where the transaction is sent or received. Competent authorities of the host jurisdiction in which the MVTS provider provides services without being physically present should liaise with the MVTS's home authority (which licenses/registers that MVTS provider and in whose jurisdiction, the MVTS provider is incorporated or resides), as appropriate to ensure that any ML/TF concerns are adequately addressed without prejudice to the right of the host country to require the submission of STRs, other threshold reports or other relevant information to the local authorities of the country where the MVTS provider operates. Similarly for AML/CFT supervision or monitoring of the MVTS providers, the home country authorities should also engage with the competent authorities of the host country where MVTS provider provides services.

28. Cross-border provision of services (including through agents or over the internet or otherwise) highlights the importance of international cooperation among the competent authorities of the relevant jurisdictions. Such international cooperation can be spontaneous or on request depending upon the nature of the specific situation.

SECTION I – THE FATF'S RISK-BASED APPROACH TO AML/CFT

A. WHAT IS THE RISK-BASED APPROACH?

29. The RBA to AML/CFT means that countries, competent authorities and MVTS providers[23], are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively and efficiently.

30. When assessing ML/TF risk[24], countries, competent authorities and MVTS providers should analyse and seek to understand how the ML/TF risks they identify affect them and take appropriate measures to mitigate and manage those risks. The risk assessment, therefore, provides the basis for the risk-based application of AML/CFT measures.[25] For MVTS providers, this will require an investment of resources and training in order to maintain an understanding of the ML/TF risk faced

repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

22 R.14, R.16 and R.26.

23 Including both legal and natural persons, see definition of "Financial institutions" in the FATF Glossary.

24 FATF (2013a), paragraph 10.

25 FATF (2013a), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

by the sector as well as specific to its products and services, its customer base, jurisdictions operated in, and the effectiveness of actual and potential risk controls that are or can be put in place. For supervisors, this will require maintaining an understanding of the ML/TF risks specific to the MVTS providers they supervise, and the degree to which AML/CFT measures can be expected to mitigate such risks. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken reasonable AML/CFT measures to identify and mitigate risks, but is still used for ML or TF purposes in isolated instances.

B. THE RATIONALE FOR A NEW APPROACH

31. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards in order to further protect the integrity of the financial system by providing governments with the tools they need to take action against financial crime.

32. One of the most important changes introduced was the increased emphasis on the RBA to AML/CFT, especially in relation to preventive measures and supervision. Whereas the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations consider the RBA to be an 'essential foundation' of a country's AML/CFT framework.[26] This is an over-arching requirement applicable to all relevant *FATF Recommendations*.

33. According to the introduction to the *FATF Recommendations*, the RBA allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.

34. The application of a RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Recommendations by countries and financial institutions.[27]

C. APPLICATION OF THE RISK-BASED APPROACH

35. The FATF standards do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF; however the overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of risk including products, services, customers, geography and the strength of the entity's compliance program. Recommendation 1 sets out the scope of the application of the RBA as follows:

- Who should be subject to a country's AML/CFT regime: In addition to the sectors and activities already included in the scope of the *FATF*

26 R. 1.

27 The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take the risks, and the flexibility allowed by the RBA, into account when determining whether there are deficiencies in a country's AML/CFT measures, and their importance (FATF, 2013f).

Recommendations[28], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.[29]

- How those subject to the AML/CFT regime should be supervised or monitored for compliance with this regime: Supervisors should ensure that financial institutions and DNFBPs are implementing their obligations under R.1. AML/CFT supervisors should consider a MVTS provider's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA, while INR 26 further requires supervisors to themselves adopt a RBA to AML/CFT supervision.
- How those subject to the AML/CFT regime should be required to comply: The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are assessed as lower, simplified measures may be permitted. This means that the range, degree, frequency or intensity of preventive measures and controls conducted will be stronger in higher risk scenarios. Conversely, where the ML/TF risk is assessed as lower, standard AML/CFT measures may be reduced, which means that measures must respond to each of the required four CDD components at applicable thresholds[30]. ((i) identification and verification of the customer's identity; (ii) identification of the beneficial owner; (iii) understanding the purpose of the business relationship; and (iv) on-going monitoring of the relationship), but the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. In all the individual cases of MVTS providers, where risk is assessed at a standard level, the standard AML/CFT controls should apply.
- Consideration of the engagement in customer relationships with MVTS providers: Through the implementation of the RBA, financial institutions should identify, assess and understand their ML/TF risks, and manage the risk by taking commensurate action to mitigate the identified risks. This does not imply that institutions should seek to avoid risk entirely, for example, through wholesale termination of customer relationships for certain sectors. Wholesale refusal of services or termination of services to a

28 See Glossary, definitions of "Financial institutions" and "Designated non-financial businesses and professions".

29 See INR.1.

30 Recommendation 10 requires that CDD measures are always required where there is a suspicion of ML/TF.

class of customers may give rise to financial exclusion risk and may also give rise to reputational risk. Even if the MVTS services are considered as vulnerable to the risks of ML/TF based on risk assessment, it does not mean that all MVTS providers and all MVTS customers or operations pose a higher risk when taking into account the risk mitigating measures that have been put in place.

- The FATF does not support the wholesale termination or restriction of business relationships to MVTS providers (or other sectors) to avoid, rather than manage, risk in line with the FATF's risk-based approach. Rather, financial institutions should take into account the level of ML/TF risk of each individual MVTS provider customer and any applicable risk mitigation measures whether these are implemented by the financial institution or the MVTS provider customer. Usually the RBA presumes that the risk associated with any type of customer group is not static and the expectation is that within a customer group, based on a variety of factors, individual customers could also be classified into risk categories, such as low, medium or high risk, as appropriate. Measures to mitigate risk should be applied accordingly.

D. FINANCIAL INCLUSION AND AML/CFT

36. MVTS play an important role in supporting financial inclusion. In general terms, financial inclusion is about providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural and undocumented persons, who have been underserved or excluded from the regulated financial sector at an affordable cost in a fair and transparent manner. It is also about making a broader range of financial services available to individuals who currently may have access to only basic financial products.

37. Money transmitters, a type of MVTS, transfer remittances. Remittances are an important financial service for people in many developing countries and are a powerful enabler of financial inclusion. However, for AML/CFT purposes, it is important that financial products and services, including MVTS, are provided through financial institutions subject to adequate regulation in line with the *FATF Recommendation.*[31] This will potentially reduce overall ML/TF risk in the financial system by bringing customers into the regulated sector. MVTS may be many customers' first or only interaction with the financial sector. Therefore, a well-designed and functioning AML/CFT policy and supervisory framework for MVTS may foster greater financial inclusion. Similarly policies that encourage financial inclusion may in turn lead to stronger AML/CFT regime, thereby reinforcing the complementary objectives of the two approaches.

38. A RBA may help foster financial inclusion, especially in the case of low-income individuals who experience difficulties in accessing the mainstream financial system. On the contrary, an indiscriminate termination or restriction of business relationships to MVTS providers without

31 FATF (2013d), p. 12.

proper risk assessment and mitigation measures could potentially increase the level of financial exclusion, diverting the customers towards services and channels bearing an increased level of risk.

SECTION II – GUIDANCE FOR MVTS PROVIDERS

39. The RBA to AML/CFT aims to foster the development of managing and mitigating measures that are commensurate with the ML/TF risks identified. In the case of MVTS providers, this applies to the types of products and services MVTS providers offer, the way they allocate their compliance resources, organise their internal controls and internal structures, and implement policies and procedures to manage and mitigate risk and deter and detect ML/TF, also taking into account agent networks.

A. RISK ASSESSMENT

40. The risk assessment forms the basis of a MVTS provider's RBA. It should enable the MVTS provider to understand how, and to what extent, it is vulnerable to ML/TF. It will often result in a stylised categorisation of risk, which will help MVTS providers determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk. It should always be properly documented, regularly updated and communicated to relevant personnel within the MVTS provider. MVTS provider's risk assessment should be commensurate with the nature and complexity of the business, the type of products and services offered, the conditions of the proposed transactions, the distribution channels used and the customers' characteristics. This includes consideration of the following factors: the nature and size of the MVTS providers' business, including whether there are multiple subsidiaries, branches or agent networks offering a wide range and variety of financial products and services; the risk profile of its customers, including whether their customer base is more diverse across different geographical locations; the extent to which the products and services offered are consistently below a given threshold; and the extent to which the MVTS provider is vulnerable to ML/TF threats.

41. Combating terrorist financing and money laundering is a global priority. MVTS providers should consult various sources of information in order to identify, manage and mitigate these risks.[32] This includes taking into account the typologies, risk indicators, red flags, guidance and/or advisories issued by the national competent authorities and FATF. Furthermore, in identifying and assessing indicators of ML/TF risk to which they are exposed, MVTS providers should consider a range of factors which may include:

- The nature, scale, diversity and complexity of their business and their target markets;
- The proportion of customers already identified as high risk;
- The jurisdictions the MVTS provider is operating in or otherwise exposed to, either through its own activities or the activities of customers, especially in jurisdictions with greater vulnerability due to contextual and various risk

[32] For example, in relation to terrorist financing, see the FATF, 2015c and 2015d, and the countries that are in the FATF's International Cooperation Review Group (ICRG) process.

factors such as the prevalence of crime, corruption, financing of terrorism, as well as the general level and quality of governance, law enforcement, AML/CFT controls, regulation and supervision, including those listed by FATF;

- The distribution channels, including the extent to which the MVTS provider deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD, the complexity of the payment chain and the settlement systems used between operators in the payment chain, the use of technology and the extent to which agent networks are used;
- The internal audit and regulatory findings; and
- The volume and size of its transactions, considering the usual activity of the MVTS provider and the profile of its customers.[33]

42. Where appropriate, MVTS providers may cooperate, for example, at an industry or country level to produce institutional assessment tools that may be used by individual providers to produce their risk assessments.[34]

43. In preparing their assessment, MVTS providers should take into account quantitative and qualitative information obtained from relevant internal and external sources, such as heads of business, national and sector risk and threat assessments, crime statistics, lists and reports issued by inter-governmental international organisations and national governments, and AML/CFT mutual evaluation and follow-up reports by FATF or associated assessment bodies as well as typologies. They should review their assessment periodically and in any case, when their circumstances change or relevant new threats emerge.

44. ML/TF risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling MVTS providers to subject customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer risk; product/service risk and agent risk. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary from one institution to another, depending on their respective circumstances and risk management. Consequently, MVTS providers will have to make their own determination as to the risk weights; however, parameters set by law or regulation may limit a business's discretion.

45. While there is no agreed upon set of risk categories, the examples provided herein are the most commonly identified risk categories. There is no one single methodology to apply to these risk categories, and the application of these risk categories is intended to provide a strategy for

33 INR 1 and 10.

34 The *Groupe Speciale Mobile Association* (GSMA), which is a global association of mobile service providers, has developed a paper which sets out their view and interpretation of how the *FATF Recommendations* apply to mobile payment service providers and what risks and risk mitigation measures might apply. This paper has not been endorsed by the FATF, but is referenced here as one example of a relevant industry initiative. See also Chatain *et al* (2011) for a mobile money risk assessment matrix.

managing the potential risks. The following risk categories could be considered alone or in conjunction with other risk categories:

Country/Geographic Risk

46. There is no universally agreed upon definition or methodology for determining whether a particular country or geographic area (including the country/geographical area within which the MVTS provider operates) represents a higher risk for ML/TF. Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may be considered as indicators of risk include:

- Countries/areas identified by credible sources[35] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations organisation.
- Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

Customer Risk

47. MVTS providers should determine whether a particular customer poses higher risk and the potential impact of any mitigating factors on that assessment. Such categorisation may be due to customer's occupation, behaviour or activity. These factors individually, may not be an indication of higher risk in all cases, but a combination thereof may certainly require greater scrutiny. Categories of customers whose business or activities may indicate a higher risk include:

- Customer or counterpart is another MVTS or a financial institution which has been sanctioned by respective national competent authority for its non-compliance with the AML/CFT applicable regime and is not engaging in remediation to improve its compliance.

35 "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

- Customer conducting their business relationship or transactions in unusual circumstances, such as:
  - Customer who travels unexplained distances to locations to conduct transactions.
  - Customer networks; i.e. defined groups of individuals conducting transactions at single or multiple outlet locations or across multiple services.
  - Customer owns or operates a cash-based business that appears to be a front or shell company or is intermingling illicit and licit proceeds as determined from a review of transactions that seem inconsistent with financial standing or occupation.
- Politically Exposed Person or his/her family members or close associates and where beneficial owner of a customer is a politically exposed person, as covered under Recommendation 12.
- Non face-to-face customer, where doubts exist about the identity of such customer.
- Customer who uses agents or associates where the nature of the relationship or transaction(s) makes it difficult to identify the beneficial owner of the funds.
- Customer knows little or is reluctant to disclose details about the payee (address/contact info, etc.)
- Consumer gives inconsistent information (e.g. provides different names).
- Customer involved in the transactions that have no apparent ties to the destination country and with no reasonable explanations.
- Suspicion that the customer is acting on behalf of a third party but not disclosing that information or is being controlled by someone else (his/her handler). For example, the customer picks up a money transfer and immediately hands it to someone else or someone else speaks for the customer, but puts the transaction in his/her name.
- Customer who has been the subject of law enforcement sanctions (in relation to proceeds generating crimes), known to the MVTS provider.
- Customer who offers false/fraudulent identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents (e.g. use of identification cards or documents in different names without reasonable explanation).
- Customer whose transactions and activities indicate connection with potential criminal involvement, typologies or red flags provided in reports

produced by the FATF or national competent authorities (e.g. FIU, law enforcement etc.).

- Customer whose transaction patterns appear consistent with generation of criminal proceeds; *e.g.* illegal drug growing season, drug trafficking, illegal immigration and human trafficking, corruption etc.; based on information available with the MVTS provider.

Product/Transactions/Service Risk

48. An overall risk assessment should also include determining the potential risks presented by products and services offered by a MVTS provider. A MVTS provider should be mindful of the risks associated with new or innovative products or services not specifically offered by the MVTS provider, but that make use of the MVTS provider's systems to deliver the product or service. The FATF 2013 NPPS Guidance determines the risks involved in the provision of NPPS, including through consideration of any relevant risk factors and risk mitigation measures. Determining the risks of products and services could include a consideration of their attributes as well as any risk mitigation measures put in place in respect thereof and could include factors such as:

- Products or services that may inherently favour anonymity or products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone.
- Products or services that have a very high or no transaction limit.
- The global reach of the product or service offered.
- The complexity of the product or service offered.
- Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.

49. The risk associated with the transaction may also vary depending on whether the MVTS provider is sending or receiving the transaction. An overall risk assessment should include a review of transactions as a whole. This should include a consideration of such factors as:

a) Transactions sent or attempted:

- Customer's behaviour at point of origination:
  - Customer structures transaction in an apparent attempt to break up amounts to stay under any applicable CDD threshold- avoiding reporting or record keeping.
  - Transaction is unnecessarily complex with no apparent business or lawful purpose.
  - Number or value of transactions is inconsistent with financial standing or occupation, or is outside the normal course of business of the customer in light of the information provided by the customer when

conducting the transaction or during subsequent contact (such as an interview, discussion or based on information provided to tax authorities and made available to the MVTS provider etc.)

- Customer offers a bribe or a tip other than where a tip is customary or is willing to pay unusual fees to have transactions conducted.
- Customer has vague knowledge about amount of money involved in the transaction.
- Customer makes unusual inquiries, threatens or tries to convince staff to avoid reporting.
- Customer sends money internationally and then expects to receive an equal incoming transfer or vice versa.
- Customer wires money to illegal online gambling sites. Email addresses containing gambling references or transfers to countries with large numbers of internet gambling sites.
- Customer wires money to higher-risk jurisdiction/country/corridor.
- Customer attempts a transaction, but given he or she would likely be subject to the CDD monitoring, cancels transaction to avoid reporting or other requirements.
- Customer transfers money to claim lottery or prize winnings or to someone he or she met only online. Transfer towards credit card or loan fee or for employment opportunity or mystery shopping opportunity. All indicators of potential consumer fraud.
- Senders appear to have no familial relationship with the receiver and no explanation forthcoming for the transfer.

- Activity detected during monitoring (in many of these scenarios the customer's activity may be apparent both during point-of-sale interaction and during back-end transaction monitoring):
  - Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
  - Unusually large aggregate wire transfers or high volume or frequency of transactions with no logical or apparent reason.
  - Customer uses aliases, nominees or a variety of different addresses.
  - Customers whose concentration ratio of transfers made to a jurisdiction is notably higher than what is to be expected considering overall customer base.
  - Customer transfers/receives funds from persons involved in criminal activities as per the information available.

- A network of customers using shared contact information, such as address, telephone or e-mail, where such sharing is not normal or reasonable explicable.
- Transfers to HOSSPs in destinations where such transactions are known to the MVTS provider to be considered illegal.

b) Transactions received:

- Concerning the implementation of R16 on wire transfers, MVTS providers should pay special attention:
  - To transactions that are not accompanied by the required originator or beneficiary information.
  - When additional customer or transactional information has been requested from an ordering MVTS provider, but has not been received.
- Large number of transactions received at once or over a certain period of time which do not seem to match the recipient's usual past pattern (e.g. during illicit drug production seasons, towards migrant smuggling etc.).

Distribution Channels Risk, namely Agent Risk

50. An overall risk assessment should analyse specific factors which arise from the use of agents as a business model to facilitate the delivery of MVTS. In some cases these agents may also use the products and services themselves. It is important for MVTS providers to ensure that they understand who the agent is, and that they are not criminals or criminal associates. Assessing agent risk is more complex for MVTS providers with an international presence due to varying jurisdictional requirements and potential risk of non-compliance by agents of the applicable local AML/CFT regulations and the logistics of agent oversight. This agent risk analysis should include such factors as the following based on the extent that these are relevant to the MVTS providers' business model:

- Agents representing more than one MVTS provider.
- Agents located in a higher-risk jurisdiction/country or serving high-risk customers or transactions.
- Agents determined to have "politically exposed person" status.
- Agents conducting an unusually high number of transactions with another agent location, particularly with an agent in a high risk geographic area or corridor.
- The transaction volume of the agent is inconsistent with either overall or relative to typical past transaction volume.
- Transaction pattern indicating value of transactions just beneath any applicable CDD threshold.

- Agents that have been the subject of negative attention from credible media or law enforcement sanctions.
- Agents that have failed to attend or complete the training programs.
- Agents that operate sub-standard compliance programs, i.e. programs that do not effectively manage compliance with internal policies, monetary limits, external regulation, etc.
- Agents with a history of regulatory non-compliance and that are unwilling to follow compliance program review recommendations, and therefore subject to probation, suspension or termination.
- Agents who fail to provide required originator information upon request.
- Agents whose data collection or record keeping is lax, sloppy or inconsistent.
- Agents willing to accept false identification or identification records that contain false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers.
- Agents with a send-to-receive ratio that is not balanced, consistent with other agents in the locale, or whose transactions and activities indicate potential complicity in criminal activity.
- Agents whose seasonal business fluctuation is not consistent with their incomes or with other agents in the locale or is consistent with patterns of criminal proceeds.
- Agents whose ratio of questionable or anomalous customers to customers who are not in such groups is out of the norm for comparable locations.

B. CUSTOMER DUE DILIGENCE AND WIRE TRANSFERS

51. CDD processes should be designed to meet the FATF standards and national legal requirements. The CDD process should help MVTS providers assess the ML/TF risk associated with a proposed business relationship or occasional transaction above the threshold. The initial CDD comprises identifying the customer and, where applicable, the customer's beneficial owner and verifying the customer's identity on a risk basis on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework. It also includes understanding the purpose and intended nature of the business relationship (where relevant) and, in higher risk situations, obtaining further information.

52. Non-banking institution providing MVTS typically carry out occasional transactions and generally do not open or maintain accounts. However, MVTS providers sometimes may also introduce customer loyalty schemes and relationship management tools, which coupled with an agreement between the MVTS providers and customers, indicate that a business relationship has been formed. The MVTS providers should have procedures, which are effectively implemented and

used to identify and verify, on a risk basis, the identity of a customer (a) when establishing business relations with that customer; (b) when carrying out occasional transactions above the applicable designated threshold[36]; (c) where they have suspicions of ML/TF regardless of any exemption or thresholds; and (d) where they have doubts about the veracity or adequacy of previously obtained identification data.

53. The legal frameworks of some countries go further than Recommendation 10 requires[37] by requiring full CDD for all transactions performed by MVTS providers, including those which are de facto occasional transactions below the USD/EUR 15 000 threshold. Such an approach may be consistent with the risk-based approach, as set out in Recommendation 1, provided that it is justified on the basis of the country's assessment of risks (e.g. through the identification of higher risks). One factor which should be taken into account is whether this would increase the risk of driving transactions to unregulated sectors.

54. Recommendation 16 establishes the requirements for countries with respect to wire transfers. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers.[38] MVTS providers must include relevant originator and beneficiary information on wire transfers and ensure that the information remains with the wire transfer throughout the payment chain as set out in the Interpretive Note to Recommendation 16. It is important to note, that countries may adopt a *de minimis* threshold for cross-border wire transfers, below which verification of the customer, and beneficiary information need not be required unless there is an ML/TF suspicion.[39] That is, for occasional cross-border wire transfers below USD/EUR 1 000, the requirements of the Interpretive Note to Recommendation 16 apply and the name of the originator and of the beneficiary will be requested, as well as an account number for each or a unique transaction reference number; however such information will not have to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to customer should be verified.

55. The MVTS provider should adopt effective risk-based policies and procedures for determining when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information and the appropriate follow-up action.[40]

56. Based on a holistic view of the information obtained in the context of their application of CDD measures, MVTS providers should be able to prepare a customer risk profile in appropriate cases. This will determine the level and type of ongoing monitoring and support the MVTS providers' decision whether to enter into, continue or terminate the business relationship. Risk profiles can apply at the individual customer level or, where a cluster of customers displays homogenous characteristics (for example, clients conducting similar types of transactions or with the same economic activity), at the cluster level. MVTS providers should periodically update customer risk

36 The FATF Recommendations require that any national threshold is no higher than USD/EUR 15 000 for occasional transactions (other than wire transfers), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked. See INR. 10.

37 Recommendation 10 required CDD measures to be undertaken.

38 INR. 16 at paragraph 3.

39 INR. 16 at paragraph 5.

40 INR. 16 at paragraph 18 and 22.

profiles[41] of business relationships, which serve to help MVTS providers apply the appropriate level of CDD. In addition, MVTS providers should take measures to comply with international sanctions lists issued by the UN and with national AML/CFT lists issued by the competent national authorities (e.g. national lists of designated persons and organisations for TF) by screening the customer's and beneficial owner's as well as beneficiary's names against such lists. Smaller MVTS providers may consider joining industry groups to have access to sanctions screening services, wherever appropriate.

57. The extent of CDD measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk, if any, associated with the individual business relationship as discussed above under Risk Assessment. This means that the amount or type of information obtained, or the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher. It may also be simplified where the risk associated with the business relationship is lower. It should, however be noted that the ability to apply simplified CDD or an exemption from other preventive measures, simply on the basis that MVTS is being carried out by natural or legal persons on an occasional or very limited basis is not to be applied (INR. 1.6(b)). Also SDD measures are not acceptable whenever there is a suspicion of ML or TF, or where specific higher-risk scenarios apply.

Box 3. **Examples of Enhanced Due Diligence/Simplified Due Diligence measures**
(see also INR 10)

- Enhanced Due Diligence
  - obtaining and corroborating additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk profiling
  - carrying out additional searches (e.g. verifiable adverse internet searches) to better inform the individual customer risk profiling
  -
  - where appropriate, undertaking further verification procedures on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may be involved in criminal activity
  - verifying the source of funds or wealth involved in the transaction or business relationship to be satisfied that they do not constitute the proceeds from crime
  - evaluating the information provided with regard to the destination of funds and the reasons for transaction
  - seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship

41 Based on the MVTS provider's own risk assessment and taking into account risk factors such as those outlined in the FATF standards, e.g. in INR 10 and Recommendations/INR 12-16.

- Simplified Due Diligence
  - obtaining fewer elements of customer identification data, seeking less robust verification of the customer's identity
  - not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established
  - verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if transaction values rise above a defined monetary threshold)
  - reducing the frequency of customer identification updates in case of business relationship
  - reducing the degree and extent of on-going monitoring and scrutiny of transactions, based on a reasonable monetary threshold

58. Where MVTS providers cannot apply the appropriate level of CDD, Recommendation 10 requires the MVTS provider to not enter into a business relationship or carry out an occasional transaction or to terminate an already-existing business relationship; and considering making a suspicious transaction report in relation to the customer.

Ongoing CDD and Monitoring

59. Ongoing monitoring on a risk basis means the scrutiny of transactions to determine whether those transactions are consistent with the MVTS provider's information about the customer and the nature and purpose of the business relationship, wherever appropriate. Monitoring also involves identifying changes to the customer profile (for example, their behaviour, use of products and the amount of money involved), and keeping it up to date, which may require the application of enhanced CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may be potentially suspicious.

60. Monitoring should be carried out on a continuous basis and may also be triggered by specific transactions. It need not require electronic systems, although for some types of MVTS activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, MVTS providers should understand their operating rules, verify their integrity on a regular basis and check that they take account of the identified ML/TF risks.

61. MVTS providers should adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for higher risk situations. The adequacy of monitoring systems and the factors leading

MVTS providers to adjust the level of monitoring should be reviewed regularly for continued relevance to the MVTS provider's AML/CFT risk programme. Transactions performed/triggered by agents must be subject to regular monitoring under the same conditions as transactions of MVTS provider itself. The monitoring should be conducted by the MVTS provider itself or in collaboration with the agent, based on appropriate agreement and under the MVTS provider's controls.

62. Monitoring under a risk-based approach allows MVTS providers to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. MVTS providers should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be transparent.

63. To this end, MVTS providers should properly document, retain and communicate to the relevant personnel the results of their monitoring as well as any queries raised and resolved.

Suspicious Transaction Monitoring and Reporting

64. Recommendation 20 requires all financial institutions including MVTS providers that suspect, or have reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, to report their suspicions promptly to the relevant FIU. MVTS providers should have the ability to flag unusual movements of funds or transactions for further analysis. MVTS providers should have appropriate systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether the funds or transaction are suspicious.

65. Funds or transactions that are suspicious should be promptly reported to the FIU and in the manner specified by competent authorities. The processes MVTS providers put in place to escalate suspicions and ultimately report to the FIU should reflect this. While the policies and processes leading MVTS providers to form a suspicion can be applied on a risk-sensitive basis, a MVTS provider should report once ML/TF suspicion has been formed.

66. MVTS providers should comply with applicable STR requirements when established through a network of agents in different host jurisdictions. The territorial approach requires the STR and any other information to be submitted, on behalf of the MVTS provider, to the FIU in the country in which the agent is established.

67. Consistent with paragraph 22 of the INR 16, MVTS providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a funds transfer, the MVTS provider: (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether this gives rise to suspicion; and (b) where necessary should file an STR with the appropriate FIU, and make relevant transaction information available to the FIU.

68. The lack of required originator or beneficiary information should be considered as a factor in assessing whether an electronic funds or wire transfer is suspicious and whether it is thus required to be reported to the FIU.

C. INTERNAL CONTROLS AND COMPLIANCE

Internal Controls and Governance

69. Adequate internal controls are a prerequisite to an effective implementation of policies and processes to mitigate ML/TF risk. Internal controls include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated, controls to monitor the integrity of staff and agents, which are implemented in accordance with the applicable local legislation. MVTS providers should consider national or sectoral risk assessments and controls to validate that their policies and processes are effective tools for identifying, assessing, and monitoring ML/TF risk in the region. It is appropriate that MVTS providers modify their internal controls according to relevant changes in their size, operational complexity, or risk exposure. Accordingly, MVTS providers should maintain systems that are adequate to manage and mitigate their risks. Where the risks are low (see for example Annex 5 for indicators of lower risk), less sophisticated systems will suffice.

70. For MVTS providers which work through agent networks, they should include these networks in their AML/CFT internal control processes and monitor them for compliance with their AML/CFT programs.

71. The successful implementation and effective operation of a RBA to AML/CFT depends on strong senior management leadership, which includes oversight of the development and implementation of the RBA across the MVTS provider.

72. Senior management should consider various ways to support AML/CFT initiatives:

- create a culture of compliance and promote compliance as a core value of the MVTS provider by sending a clear message that the MVTS provider will develop processes to ensure that:
- ML/TF risks can be managed before entering into, or maintaining, business relationships or offering services that are associated with excessive ML/TF risks;
- business relationships are not established when the ML/TF risks cannot be mitigated and managed.
- Senior management, together with the company board of directors, are responsible for setting up robust risk management governance and controls mechanisms that:
- reflect the company's established risk policy;
- implement adequate internal communication processes appropriate for the actual or potential ML/TF risks faced by the MVTS provider. These mechanisms should link (where applicable) the board of directors, the AML/CFT chief officer, any relevant or specialised committee within the MVTS provider (e.g. the risks or the ethics/compliance committee), the IT division and where applicable, each of the business areas;

- helps decide on the measures needed to mitigate the ML/TF risks identified and on the extent of residual risk the MVTS provider is prepared to accept; and
- adequately resource the MVTS provider's AML/CFT function.

73. This implies that senior management should not only know about the ML/TF risks to which the MVTS provider is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. This would require that senior management:

- understands the regulatory and supervisory requirements where the MVTS provider operates;
- receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the MVTS provider is exposed through its activities and individual business relationships;
- receives sufficient and objective information to understand whether the MVTS provider's AML/CFT controls are effective;
- receives updates on government communications or enforcement actions related to the AML/CFT obligations of MVTS providers and ML/TF risks;
- ensures that processes are in place to escalate important decisions that directly impact the ability of the MVTS provider to address and control risks.

74. Responsibility for the consistency and effectiveness of AML/CFT controls should be clearly allocated to an individual of sufficient seniority within the MVTS provider to signal the importance of ML/TF risk management and compliance, and that ML/TF issues are brought to senior management's attention. This includes the appointment of a skilled compliance officer at management level.[42] The compliance officer should have the necessary independence, authority, seniority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including across lines of business, and foreign branches, subsidiaries and agents). Where an MVTS provider is situated via one or more agents in various host countries, an individual with functions of compliance officer may be appointed in each host country to ensure compliance with the local AML/CFT requirements (CDD, record keeping, STR and any other reporting obligation to the host FIU among others).

75. Recommendation 18 requires countries to require financial institutions to have an independent audit function to test the AML/CFT programme with a view to establishing the effectiveness of its AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. Senior management will need to have a means of independently validating the development and operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based methodology reflects the risk profile of

42 INR 18.

the MVTS provider. This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, specialist consultants or other qualified parties who are not involved in the implementation or operation of the MVTS provider's AML/CFT compliance programme. The testing should be risk-based, taking into account the risk profile of the MVTS provider; should evaluate the adequacy of the MVTS provider's overall AML/CFT policies and programme, the quality of risk management for the MVTS provider's operations, departments and subsidiaries; should include comprehensive procedures and testing; and should cover all activities.

76. Both the compliance and audit functions should base their assessment on all information relevant to their task including, where relevant and appropriate, information obtained confidentially through relevant internal mechanisms or whistleblowing hotlines. Other sources of information can include training pass rates, compliance process or control failures or analysis of questions received from staff.

Internal Mechanisms to Ensure Compliance

77. A MVTS provider's internal control environment should be conducive to assuring the integrity, competence and compliance of staff with relevant policies and procedures. The measures relevant to AML/CFT controls should be consistent with the broader set of controls in place to address business, financial and operating risks generally.

78. The nature and extent of AML/CFT controls will depend upon a number of factors, including the nature, scale and complexity of a MVTS provider's business, the diversity of its operations, including geographical diversity, its customer base, product and activity profile, the degree of risk associated with each area of its operations and distribution channels, i.e. the extent to which the MVTS provider is dealing directly with the customer or is dealing through intermediaries, agents, third parties, or in a non-face-to-face setting without appropriate mitigating measures.

79. The framework of AML/CFT compliance function and internal controls should:

- Place priority on the MVTS provider's operations (products, services, customers and geographic locations) that are more vulnerable to abuse.
- Provide for regular review of the risk assessment and risk management processes, taking into account the environment within which the MVTS provider operates and the activity in its market place.
- Provide for an AML/CFT compliance function and review programme.
- Ensure that adequate risk assessment and controls are in place before new products are offered.
- Inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.
- Provide for programme continuity despite changes in management or employee composition or structure.

- Focus on meeting all appropriate regulatory record keeping and reporting requirements and for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Provide for adequate controls for higher risk customers, transactions and products, agents, as necessary, such as transaction limits or management approvals.
- Enable the timely identification and filing of reportable transactions.
- Provide for adequate management and oversight of its agents, including initial agent due diligence, AML/CFT training, and ongoing risk-based monitoring.
- Provide for adequate supervision of employees who handle transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the business's AML/CFT programme.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- Provide for appropriate initial and refresher training to be given to all relevant staff.
- Provide for appropriate initial and refresher training for agents at appropriate intervals.

Vetting and recruitment

80. MVTS providers should recruit through background checks and satisfy themselves that the staff they employ have integrity, are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls, whether in compliance or in front-line function.

81. The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

Training and Awareness

82. The effective application of AML/CFT policies and procedures depends on staff within MVTS providers understanding not only the processes they are required to follow but also the risks these processes are designed to mitigate, as well as the possible consequences of those risks. It is therefore important that staff receive AML/CFT training, which should be:

- Relevant to the MVTS provider's ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls;
- Obligatory for all relevant staff;

- Tailored to particular lines of business within the MVTS provider, equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks;
- Effective: training should have the desired effect, and this can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the MVTS provider's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;
- Ongoing: in line with INR 18, AML/CFT training should be regular, relevant, and not be a one-off exercise when staff are hired;
- Complemented by AML/CFT information and updates that are disseminated to relevant staff as appropriate.

83. Overall, the training should also seek to build up a working culture where compliance is embedded in the activities and decisions of the entire MVTS provider's staff.

D. AGENTS OF MVTS PROVIDERS

Agent Due Diligence

84. Agent Due Diligence is intended to enable a MVTS provider to ensure that it knows the legal and ownership structure of its agents and that it will be forming business relationships with legitimate and viable agents that will reliably implement or adhere to (depending on local regulations) AML/CFT requirements, program responsibilities, policies, and procedures. The MVTS provider's procedures must take into considerations such factors as:

- Upon application, identify the agent and perform the necessary background checks and due diligence, such as a recent change from current relationship with other product/service providers, whether the agent is representing more than one MVTS provider or is licensed/registered by the relevant national supervisory authority to provide payment services, length of time in business, ownership structure, creditworthiness, financial viability, class of trade or industry, licensing and regulatory structure and other regulatory licensing or registration to which the agent may be subject.
- Obtain appropriate additional information to understand the applicant's business, such as offering other MVTS services, the agent's past record of legal and regulatory compliance, expected nature and level of transactions and customer base, and geographical exposure.
- Upon approval, conduct new agent AML/CFT training encompassing applicable AML/CFT requirements, AML compliance program responsibilities, and MVTS internal policies and procedures. Provide AML/CFT compliance materials, tools, and training to agents on an ongoing and regular basis.

- Provide guidelines and assistance to the agent to assess its own compliance program regime and to develop its own risk assessment based upon its unique risk profile for its products and services, customers, geography, and subagents or outlets (if applicable).
- Ensure compliance regime adherence to internal policies and external regulation, such as reporting suspicious or attempted suspicious activities, large transactions, monitoring the risk behaviours described above, reporting and record keeping, through periodic AML compliance program reviews.
- Provide prompt attention and remediation of risk behaviours by onsite or offsite contact with the agent, which may result in further training, or probation, suspension or termination of the agent.

Training and Awareness of Agents

85. As a preventive measure, MVTS providers should check the agent's integrity before and during the business relationship, in order to avoid the abuse of their services. Agents must have appropriate training with regard to AML/CFT either provided by the MVTS providers or by themselves. Putting in place and maintaining effective controls relies on both training and awareness. This requires an enterprise-wide effort to provide all relevant employees and agents with appropriate information on AML/CFT laws, regulations and internal policies.

86. Applying a risk-based approach to the various methods available for training gives each MVTS provider additional flexibility regarding the frequency, delivery mechanisms and focus of such training. Agent training should be documented and training records should be maintained according to applicable record keeping requirements. A MVTS provider should review its agent base and available resources and implement training programmes that provide appropriate AML/CFT information that is at the appropriate level of detail.

87. Agent training may include onsite or offsite initial training (*i.e.* upon activation), and ongoing training via web-based programmes, periodic mailings or newsletters, websites or pop-up messages at point of origination. In conjunction with or in addition to such training, the MVTS provider may provide periodic compliance program reviews involving a comprehensive assessment of the agent's compliance with internal and external AML regulatory requirements.

Monitoring of Agents

88. Agent monitoring is a very important element for an effective MVTS provider's AML/CFT program. All agents require monitoring to assess and address systemic risks such as inadequate training, new or changing services or products, and poor individual judgment or performance. The degree and nature of agent monitoring will depend on the transaction volume of the agent, the monitoring method being utilised (manual, automated or some combination), countries where the funds are sent, outcomes of previous monitoring mechanisms (where relevant), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, the degree of monitoring will be based on the perceived risks, both external and internal, associated with the agent, such as

the products or services being provided by the agent, the location of the agent and the nature of the activity. Prompt attention and remediation of risk behaviours should be addressed by appropriate means, such as enhanced examination of the agent's transaction history and data integrity, obtaining and evaluating the agent's explanation of these behaviours, confidential sampling of the questioned aspects of the agent's services, or onsite or offsite contact with the agent, which may result in further training, or probation, suspension or termination.

89. Agent monitoring under a risk-based approach allows a MVTS provider to create monetary or other thresholds or specific red flags to determine which agent activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. MVTS providers should also assess the adequacy and integrity of any systems and processes on a periodic basis.

90. Competent authorities and MVTS providers (as well their industry associations) may consider collaborating to address and mitigate the specific risks emanating from certain agent behaviour. Some of the measures that can be implemented in this regard may include:

- an industry-held register of high-risk agents (or the so-called "bad agents"), through which MVTS providers can share alerts with each other about potential bad actors.
- requiring application of enhanced CDD measures in appropriate cases.
- applying thresholds on cash transactions.
- providing specific training sessions on STR indicators to MVTS providers in order to enhance their understanding and improve reporting standards, with the expectation that the MVTS provider would then train its agents or alternatively training to both the MVTS providers and their agents.

SECTION III – GUIDANCE FOR SUPERVISORS

A. THE RISK-BASED APPROACH TO SUPERVISION AND/OR MONITORING

91. The RBA to AML/CFT aims to develop prevention or mitigation measures which are commensurate with the ML/TF risks identified. In the case of supervision, this applies to the way supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that is conducive to the application of RBA by MVTS providers.

92. Recommendation 26 requires countries to subject MVTS providers to effective systems for AML/CFT supervision and/or monitoring. INR 26 requires supervisors to allocate greater supervisory resources to areas of higher ML/TF risk, on the basis that supervisors understand the ML/TF risk in their country and have on-site and off-site access to all information relevant to determining a MVTS provider's risk profile.

Box 4. **Recommendation 26: Regulation and Supervision of Financial Institutions**

[.....]

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

[.....]

Understanding ML/TF Risks

93. An effective risk-based regime reflects a country's policy, legal and regulatory approach. The national policy, legal and regulatory framework should also reflect the broader context of financial sector policy objectives that the country is pursuing. These would include financial inclusion, financial stability, financial integrity and financial consumer protection and include considerations such as competition. The extent to which the national framework allows MVTS to apply a risk-based approach should also reflect the nature, diversity and maturity of the MVTS sector, and its risk profile as well the ML/TF risks associated with individual MVTS providers.

94. Supervisors should also develop a deep understanding of the MVTS market, its structure and role in the financial system and the country's economy to better inform risk assessment of the sector. Supervisors should draw on a variety of sources to identify and assess ML/TF risks. This will include but not limited to jurisdiction's national or sectoral risk assessments, domestic or international typologies and supervisory expertise, as well as FIU feedback. Where competent authorities do not adequately understand the MVTS environment operating in the country, it may be appropriate for competent authorities to consider undertaking a more targeted sectoral risk assessment in relation to the MVTS sector to develop a national level understanding of the relevant ML/TF risks and to also inform the institutional assessments to be undertaken by the MVTS providers.[43]

95. Access to information about ML/TF risks is fundamental for an effective RBA. INR 1.3 requires countries to take appropriate steps to identify and assess ML/TF risks for the country, on an ongoing basis in order to make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs. In situations where some parts of the MVTS sector have potentially limited capacity to identify ML/TF risks, countries should particularly work with the sector to understand their risks. Depending on their capacity, general information or more granular information and support may be required.

43 FATF (2013a), paragraphs 17-19.

96. For individual MVTS providers, supervisors should take into account the level of risk associated with the MVTS providers' products and services, business model, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location, countries of operation and the level of compliance with the AML/CFT measures. Supervisors should also look at the controls in place, including the quality of the risk management policy, the functioning of the internal oversight functions etc. Other information, which may be relevant in the AML/CFT context, includes the fitness and propriety of the management and the compliance function.

97. Some of this information can be obtained through prudential supervision in countries where MVTS providers are subject to prudential regulation. This involves appropriate information-sharing and collaboration between prudential and AML/CFT supervisors, especially when the responsibilities belong to two separate agencies. In other regulatory models, such as those focusing on licensing/registration at the national level, but with shared oversight and enforcement at the state level and/or with SRBs, information sharing should include the sharing of examination findings.

98. Where relevant, information from other stakeholders such as other supervisors (including overseas supervisors, and supervisors of payment systems and instruments), the FIU and law enforcement agencies may also be helpful in determining the extent to which a MVTS provider is able to effectively manage the ML/TF risk to which it is exposed. Some regimes, such as those only requiring registration (without extensive background testing) may still enable law enforcement and regulators to be aware of the existence of the institution, its lines of business, or controlling interests.

99. Supervisors should review their assessment of both the sector's and MVTS providers' ML/TF risk profiles periodically and in any case when MVTS providers' circumstances change materially or relevant new threats emerge.

100. Examples of different ways MVTS supervisors assess ML/TF risk in the MVTS sector and in individual MVTS providers can be found in *Annex 2.*

Mitigating ML/TF risk

101. The *FATF Recommendations* require supervisors to allocate and prioritize more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risk to which the sector and individual MVTS providers are exposed. Supervisors should give priority to the areas of higher risk, either in the individual MVTS provider or to MVTS providers operating in a particular sector. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to get some granularity for the appropriate categorisation of individual MVTS providers within the sector based on their customer base, countries they deal with and applicable AML/CFT controls etc.

102. It is also important that competent authorities acknowledge that in a risk-based regime, not all MVTS providers will adopt identical AML/CFT controls and that single, unwitting and isolated incidents involving the transfer or exchange of illicit proceeds do not necessarily invalidate the

integrity of a MVTS provider's AML/CFT controls. On the other hand, MVTS providers should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

103. Examples of ways in which supervisors can adjust their approach include:

a) Adjusting the type of AML/CFT supervision or monitoring: supervisors should always have both off-site and on-site access to all relevant risk and compliance information. However, to the extent permitted by their regime, supervisors can determine the correct mix of off-site and on-site supervision or monitoring of MVTS providers. Off-site supervision alone may not be appropriate in higher risk situations. However, where supervisory findings in previous examination (either off-site or on-site) suggest a low risk for ML/TF, resources can be allocated to focus on higher risk MVTS providers. In that case lower risk MVTS providers could be supervised off-site, for example through transaction analysis and questionnaires.

b) Adjusting the frequency and nature of ongoing AML/CFT supervision or monitoring: supervisors should adjust the frequency of AML/CFT examination in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge, e.g. as a result of whistleblowing, information from law enforcement, analysis of financial reporting or other supervisory findings. Other risk-based approaches to supervision could consider geographic location, customer base, cash intensity, number of accounts, the nature and number of agents, revenue, prior history of non-compliance, significant changes in management, and/or acquisitions.

c) Adjusting the intensity of AML/CFT supervision or monitoring: supervisors should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of MVTS providers' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the MVTS providers' risk assessment, reporting and record keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT risk assessment in particular lines of business.

104. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and AML/CFT rules and guidance remains adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to MVTS providers to enable them to enhance the quality of their RBA.

105. Under *FATF Recommendation* 27 and 35, supervisors should have the power to impose adequate sanctions on MVTS providers when they fail to comply with regulatory requirements. Supervisors should use proportionate actions, which may include a range of supervisory interventions, including corrective actions to ensure proper and timely correction of identified deficiencies as well as punitive sanctions for more egregious non-compliance, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or significantly inadequate controls will result in a more severe supervisory response.

B. SUPERVISION OF THE RISK-BASED APPROACH

Licensing or Registration

106. *FATF Recommendations* 14 and 26 require countries to ensure that MVTS providers are licensed or registered by a competent authority, including the requirement to ensure that agents of MVTS providers are licensed or registered, or that the MVTS provider maintains a current list of its agents accessible by competent authorities in the countries in which the provider and its agents operate. These requirements should take into account the benefits of bringing MVTS providers into the regulatory framework.

General approach

107. Supervisors should understand the ML/TF risks faced by the sector and by a MVTS provider. They should have a comprehensive understanding of higher, standard as well as lower risk lines of business, with a particularly thorough understanding of the higher risk lines, leading to a sound judgment about the proportionality and adequacy of AML/CFT controls. As part of their exam procedures, supervisors should communicate findings and their views about the individual MVTS provider's AML/CFT controls. It is important to understand why institutions may decline to adopt proportionate controls. Where this is due to a lack of understanding of the flexibility available, supervisors should be able to provide appropriate guidance. Equally supervisors should understand the reasons why an institution engages in instances which go beyond the law (also called conservative or over-compliance) and provide further guidance, where considered appropriate.

108. It is important that supervisors discharge their functions in a way that takes into consideration the adoption of a RBA by MVTS providers. This means that supervisors should ensure that their staff are equipped to assess whether a MVTS provider's policies, procedures and controls are appropriate and proportional in view of the MVTS provider's risk assessment and risk management procedures. Supervisors should satisfy themselves that the MVTS provider adheres to its own policies, procedures and controls, and makes sound decisions. It is also important that supervisors should articulate and communicate clearly their expectations of the measures needed for MVTS providers to comply with the applicable legal and regulatory framework.

109. To support supervisors' understanding of the overall strength of measures in the MVTS sector, comparative analysis between MVTS providers' AML/CFT programs could be considered as a means to inform their judgment of the quality of an individual MVTS provider's controls. Supervisors should, however, note that under the RBA, there may be valid reasons why MVTS providers' controls differ.

110. In the context of the RBA, the primary focus for supervisors should be to assess whether the MVTS provider, in its own risk assessment, has reasonably and fairly gauged the risk to the business. In doing so, the supervisors should take into account the individual business circumstances; in addition to the overall sector risk. Supervisors should also determine whether or not the MVTS provider's AML/CFT compliance and risk management program is adequate to a) meet the regulatory requirements, and b) appropriately and effectively mitigate and manage the risks. The effective application of the RBA means that risk is assessed by institution and customer, not to an entire category of financial institutions or customer groups. In the case an MVTS provider

operates across different jurisdictions on the basis of a single licence or registration, the home supervisor (that licences or registers the entity) should take into consideration the risk the entity is exposed to and the extent to which those risks are adequately mitigated.

Guidance

111. Supervisors should communicate their expectations of MVTS providers' compliance with their legal and regulatory obligations, and may consider engaging in a consultative process, where appropriate with relevant stakeholders. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based obligations, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied.

112. Guidance for the MVTS sector is essential and is a requirement under *FATF Recommendation* 34. Some MVTS providers may have limited experience in, or ability to, identify relevant ML/TF risk factors. In particular, for MVTS providers with lower capacity, the guidance provided would need to be more detailed than that provided for other MVTS, and could include extensive information on conducting a risk assessment and implementing a RBA. The guidance could include tools that enable small MVTS providers with lower capacity to undertake assessments and develop risk mitigation and compliance management systems to meet their legal obligations. Supporting ongoing and effective communication between supervisors and MVTS providers is an essential prerequisite for the successful implementation of a RBA.

113. Supervisors should also consider liaising with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of the legal obligations and to promote a level playing field, including overseers of payment systems and instruments. This is particularly important where more than one supervisor is responsible for supervision (for example, where the prudential supervisor and the AML/CFT supervisors are in different agencies, or in separate divisions of the same agency or when the MVTS provider has agents in several jurisdictions). Multiple sources of guidance should not create opportunities for regulatory arbitrage, loopholes or unnecessary confusion among MVTS providers. When possible, relevant regulatory and supervisory authorities within a jurisdiction should consider preparing joint guidance.

Training

114. Training is important for supervision staff to understand the MVTS sector and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of a MVTS provider's ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of the MVTS provider's AML/CFT policies, procedures and internal controls in light of its risk assessment.

115. Training should allow supervisory staff to form sound judgments about the quality of the MVTS provider's risk assessment and the adequacy and proportionality of a MVTS provider's AML/CFT controls. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Information exchange

116. Information exchange between the public and private sector is of importance in the MVTS sector and may form an integral part of a country's strategy for combating ML/TF. In situations where MVTS providers do not have experience, or have limited capacity for an effective assessment of ML/TF risk, it will be important for public authorities to share risk information to better help inform the risk assessments of MVTS providers.

117. The type of information that could be shared between the public and private sectors include:

- ML/TF risk assessments;
- Typologies of how money launderers or terrorist financers have misused MVTS;
- General feedback on STRs and other relevant reports;
- Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with MVTS providers as a class or individually; and
- Countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by *FATF Recommendation* 6.

118. Domestic cooperation and information exchange between the supervisors of the banking sector and the MVTS sector, central bank and MVTS supervisors for monitoring and feedback of the remittance flows, among law enforcement, intelligence, FIU and MVTS supervisors and between the FIU and supervisor of the MVTS sector is also of vital importance for effective monitoring/supervision of the sector.

119. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the MVTS sector, taking into account the multi-jurisdictional reach of many MVTS providers.

Supervision or monitoring of agent networks

120. Some MVTS providers operate through a network of agents, sometimes in different jurisdictions. The use of agents can create vulnerabilities where an agent may not itself be a financial service professional. In all cases, MVTS providers that use agents should be required to include them in their AML/CFT programs and MVTS providers should monitor them for compliance with applicable AML/CFT legislation and regulation.[44]

121. Recommendation 14 requires that agents of MVTS providers should either be licensed/ registered, as is the case for their provider, or countries could also choose another option, which is requiring the MVTS provider to maintain a current list of agents that is accessible by competent authorities. Countries should carefully consider the risks involved in each approach, the practical

[44] R.14

feasibility, and the resources required before making a final decision on whether to license/ register, or require the MVTS provider to maintain a current list of agents. In all cases, countries should ensure that under their legal framework, the MVTS provider remains responsible for its AML/CFT obligations and is accountable for the actions of its agents consistent with established principles of agency law. Supervisors that license MVTS providers to operate outside of their own jurisdiction should consider the risks such activities represent to those host jurisdictions, and should ensure that the obliged entity mitigates risks adequately.

122. Countries should determine on a risk-sensitive basis whether the supervision of agents is undertaken indirectly through the MVTS providers or through direct contact with the agents, to ensure that supervision or monitoring is proportionate and commensurate with the level of ML/TF risk. In line with the risk-based approach, countries may consider imposing AML/CFT regulation on MVTS agents, as well as the MVTS providers. Under this approach, the agents would themselves be subject to AML/CFT obligations and be directly supervised for compliance with these obligations by the relevant supervisory authority. This approach may be beneficial in situations where the MVTS provider is located in another country which creates difficulties in effectively supervising that entity. Countries could consider supervisory mechanisms such as central contact points or home/host supervisory cooperation between relevant AML supervisors of the sector, in order to ensure effective supervision and monitoring of compliance with the applicable AML/CFT obligations and to facilitate information exchange.

123. In establishing the supervisory framework, countries should clearly establish the competent authority that is responsible for the AML/CFT supervision or monitoring of MVTS providers. When a MVTS provider is a multinational entity or operates through a network of agents in different jurisdictions, the cooperation between supervisors in these jurisdictions becomes even more important. It is necessary to clarify the responsibilities of the supervisors, to ensure mechanisms and arrangements (such as protocol on cooperation in AML/CFT supervision) for effective cooperation, exchange of information about agents and the MVTS provider and to clarify the regulatory position.

SECTION IV – ACCESS OF MVTS TO BANKING SERVICES[45]

This section should be read in conjunction with the *2014 FATF RBA Guidance for the banking sector.*

A. AML/CFT REQUIREMENTS AND BANKING MVTS PROVIDERS

Regulatory Expectations

124. As a financial institution subject to FATF requirements, a MVTS provider is subject to the full range of AML/CFT controls with which it has to comply vis-à-vis its customers, such as: CDD, wire transfer rules and ongoing monitoring mechanisms apart from record keeping, suspicious transactions reporting etc. (Section II). The review of the AML/CFT measures and programme put in

45 All reference to access of MVTS providers to banking service in this section and elsewhere in the paper includes access to non-banking financial institutions, which may hold payment accounts of MVTS providers as customers.

place by the MVTS provider will often be part of the overall MVTS customer risk assessment conducted by the bank before on-boarding the MVTS provider as a customer.

125. As stated earlier, MVTS agents should either be licensed or registered with a competent authority or be part of a list maintained by the MVTS provider and accessible by competent authorities in the country where they operate. As a starting point, the MVTS provider should provide evidence or confirmation that it has conducted the relevant agent due diligence, that its AML/CFT program includes its agents and that compliance is monitored. When they are themselves MVTS providers, agents are required to establish AML/CFT programs and comply with due diligence, record keeping and other AML/CFT requirements.

B. BANKS' RISK-BASED APPROACH TO MVTS PROVIDERS

MVTS Risk Assessment

126. It should also be noted that in many cases, MVTS providers are reliant on access to the banking system in order to commence or continue their operations. It is important that banks apply the RBA properly and do not resort to the wholesale termination or exclusion of customer relationships within the MVTS sector without being informed by a proper risk assessment.

127. Where banks propose to enter into a business relationship with a MVTS provider, they should evaluate the ML/TF risk of the business relationship and assess whether those risks can be appropriately mitigated and managed. This should include control measures to mitigate the risks of the MVTS provider as a customer currently assessed as low, medium or high risk, and a process for escalation to deal with MVTS providers or particular aspects of their business, which become higher risk in the course of the business relationship.

128. When assessing the risks associated with MVTS providers, different risk factors (types of products and services offered, types of customers, distribution channels, and jurisdictions they are exposed to, experience of the provider, purpose of the account, anticipated account activity etc.) should be weighed; as MVTS providers will not present the same levels of ML/TF risk. While some will pose a higher risk, there are others that will not. An effective risk assessment should be a composite of multiple factors, and important elements in the case of MVTS will include the scope of markets served (domestic or international), the purpose of the bank account and the anticipated account activity, the regulatory oversight effectiveness in the countries of operation, and the effectiveness of the MVTS's risk management and compliance programs.

129. Depending upon the circumstances, certain factors may be weighed more heavily than others. For example, one of the elements which could act as a risk mitigant is the fact that MVTS providers are regulated financial institutions that are subject to the full range of AML/CFT obligations, supervision and monitoring. Factors which could potentially increase the ML/TF risks are the geographic coverage (especially countries with weaknesses in their AML/CFT framework), bulk transfers (where the transfer represents a collection of underlying transactions), third party payments, inadequate supervisory framework in its home jurisdiction, or the fact that the provider is a new business without an established operating history. Factors that may decrease the risk are geographic coverage (for example, where a money remitter offers services only domestically or to countries which are largely compliant with the FATF standards or present a relatively low ML/TF

risk); that the business operator has an established operating history etc. Other factors that may be relevant include whether transactions are small remittances for family members, or where there are high levels of transparency of payment information (e.g. purpose of sending funds is clearly explained, MVTS provider has visibility into both sender and recipient, all parties are adequately identified including beneficial ownership and it involves a direct transaction without any further intermediation).

130. The bank may consider, on a risk-sensitive basis whether the MVTS provider acts as a principal or is an agent of another provider. In this case, the way in which the principal monitors and controls compliance by its agents needs to be considered as an element of risk. Thus agents' due diligence procedures and adequacy and effectiveness of their supervision/monitoring by MVTS providers may be considered by banks and factored in when assessing the overall ML/TF risks being posed by such MVTS providers to banks as their customers. Where the MVTS provider itself is not a bank's customer but the MVTS agent is a customer, bank may also consider obtaining information/reference from the MVTS provider; in order to assist in its understanding of the MVTS agent's business and source of funds.

Risk-based AML/CFT Obligations for Banking MVTS Providers

MVTS Provider Due Diligence

131. Based on AML/CFT requirements applicable to banks, proper due diligence associated with opening and maintaining accounts for MVTS providers is required, in relation to the customer, the beneficial owner(s), and the business relationship (i.e. determine the structure and ownership of the MVTS provider, the nature of its business and operations including the target market, the purpose of the relationship and the expected account activity). In all cases, the level and extent of due diligence applied will be dictated by the risks associated with the particular MVTS customer provider.

132. Depending on the level and nature of risk identified, and the size and sophistication of the particular MVTS provider, banks may pursue different types of action as part of an appropriate due diligence process. When identified risks are higher, enhanced due diligence should be applied, which can include reviewing the AML/CFT (group-wide) programmes, their internal or external audit and other expert's reports, review of the list of agents and their monitoring, management and screening practices. A visit to the place of business and/or informative statements sent to third parties to verify the alignment with operating history, where appropriate, may prove helpful to check the existence and activities of the provider. Bank may also rely and/or verify from publicly available information (such as licensed or registered person lists with competent authorities) in such cases. If a bank becomes aware of changes in the profile of a MVTS provider to which services are being provided, additional steps or enhanced due diligence may be necessary.

Ongoing Monitoring of MVTS Accounts

133. Risk-based monitoring of accounts maintained for all customers, including MVTS providers, is a key element of an effective system to identify and, where appropriate, report violations and suspicious transactions. The level and frequency of such monitoring will depend, among other things, on the bank's risk assessment and the activity across the MVTS provider's accounts (including reconciling the activities of the MVTS providers together with the MVTS agents in order

to ascertain the full risk exposure where both the MVTS provider and its agents are bank's customers). Risk-based review of transactions should be conducted to detect any significant unexplained variations in transaction size, nature or frequency through the account which could reveal potentially suspicious operations.

MVTS Suspicious Transaction Reporting

134. While the policies and processes leading banks to form a suspicion can be applied on a risk-sensitive basis, a bank should report once a suspicion of ML/TF has formed. Banks should have the ability to flag unusual movements of funds or transactions conducted by MVTS providers for further analysis. They should also have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether they are suspicious. Similarly, if a bank is aware that an MVTS provider is breaching the applicable licensing or registration requirements, it should not accept the MVTS provider as a customer and should file a STR, if appropriate, in such cases.

C. GUIDANCE FOR THE SUPERVISION OF BANKS WITH MVTS PROVIDERS AS CUSTOMERS

General approach

135. Banks' considerations before providing services to MVTS providers are varied, including ML/TF risks, the compliance costs to effectively mitigate those risks, profitability, reputational risk and requirements imposed by international correspondent banks. There may also be some circumstances in which a bank may choose not to provide financial services to some or any MVTS providers for reasons including limited product lines that do not include MVTS related service, adequacy of supervision over MVTS, cross-border information-sharing barriers, the risks associated with specific jurisdictions which it deems unmanageable.

136. While the decision to accept or maintain a business relationship is ultimately a commercial one for the bank, supervisors need to ensure that they understand the drivers of and reasons for those commercial decisions and they communicate the importance of banks following the risk-based approach to managing the risks of individual accountholders. It is possible that financial institutions go beyond the requirements of relevant laws and regulations (also called conservative or over-compliance) for example, by deciding not to implement simplified due diligence measures, where allowed, in relation to lower risk products or by refusing or closing accounts due to lack of understanding of the law, lack of compliance expertise or on account of business factors that are not compliance related.[46] Where decision to restrict or terminate relationship with MVTS is due to a lack of understanding of the flexibility of the risk-based approach, supervisors will be able to provide appropriate guidance as to what the RBA entails.

137. Banks should identify, assess, manage and mitigate the risks posed by their customers, sectors in which those customers operate and the products and services offered. Banks themselves are best placed to assess and manage the risks posed by their customers and the products and services offered. Effective supervision can assist banks to understand the implementation of the RBA, thereby avoiding wholesale termination of customer relationships. Systematic termination of

46 De Koker, Louis and Symington, John (2014).

business relationships and refusal to on-board MVTS clients without proper risk assessment and mitigation measures, could, drive remittance flows to unregistered and unregulated channels. This may exacerbate the AML/CFT risk rather than address it. In any case, the wholesale cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risks or risk mitigation measures for individual customers within a particular sector, cannot be considered as being in line with FATF standards. In addition to increasing ML/TF risks, such action may give rise to reputational and legal risks for banks, amongst others relating to unfair discrimination, competition and consumer protection.

Guidance

138. All supervisors should sufficiently and consistently clarify their MVTS related supervisory expectations over the RBA as part of their day-to day supervision and when wholesale de-risking occurs as a result of misinterpreting the RBA. Supervisors may take the opportunity to clarify that the intention of a RBA is not to eliminate risk by refusing services to any particular sector, but to manage risk effectively. Supervisors should provide meaningful and actionable guidance on the effective implementation of the RBA to both the banking sector and supervisory staff. With appropriate systems and controls in place, banks should be able to manage and mitigate the potential ML/TF risks posed by some MVTS providers. Other relevant FATF guidance on the supervision of banks can be found in the FATF RBA Guidance for the banking sector and the FATF Guidance on the Risk-Based Approach for Effective Supervision and Enforcement.

139. Supervisors could emphasise the varying degrees of risks in the MVTS sector and encourage banks to take into account risk mitigating factors, such as AML/CFT procedures and controls, which are put in place by MVTS providers to manage their ML/TF risks. Often, supervisors of banking and non-banking MVTS providers are different (e.g. central bank/financial regulator *vis-à-vis* FIU, non-banking supervisors/different departments within the bank/supervisors etc.). Supervisory compliance expectations and tolerance for risk in these cases are also often inconsistent. Thus, stress should be given to coordination among different supervisors so that all MVTS providers and banks could have similar expectations and similar approaches to RBA.

140. Supervisors could clarify the expectations on banks concerning the assessment of CDD policies and procedures implemented by a MVTS provider. Supervisors could inform bank decisions by providing examples of CDD practices that they deem adequate for small, lower risk MVTS providers.

141. Supervisors could encourage banks to engage with the MVTS sector on the measures that the sector could take immediately and in the longer term to meet the banks' risk standards which would enable a continuation or start of the business relationship. Such encouragement will be more meaningful when accompanied by supervisory statements on risk tolerance.

ANNEX 1. UNAUTHORISED MVTS PROVIDERS

Recommendation 14 requires countries to take action to identify natural or legal persons that carry out MVTS without a licence or registration, and to apply appropriate sanctions. Countries should take a systematic and pro-active approach by identifying and taking action against unauthorised providers on a regular basis. For many jurisdictions, proactive identification of informal MVT services and awareness-raising is an integral element of establishing and maintaining an effective registration / licensing regime.

Countries should ensure that a competent authority has the responsibility for the identification and sanctioning of unauthorised MVT providers. Depending on the institutional framework in a country, the authority may be, for example, the supervisor, the FIU, the law enforcement agencies or another agency with regulatory authority over the financial sector. Countries should consider which competent authority is best placed to be responsible for this issue, which will differ between countries depending on the circumstances and institutional structure. When determining the responsible authority, counties should consider a range of factors including the powers and capacity of competent authorities, the level of interaction with MVTS providers, and the information available to competent authorities to support this function.

There is a range of information sources which may indicate MVT activity and could be useful to identify unauthorised MVTS providers, for example:

- Applications for licencing or registration, including those that were unsuccessful or historical applications which were not renewed or where licenses or registrations have been withdrawn;
- Marketing by MVTS providers, including advertisements in the various media outlets;
- Suspicious transaction reports;
- Data by MVTS organisations, reporting those entities which do not form part of their organisation or association;
- Information provided by whistle blowers;
- Policing and intelligence reports; and
- Reports of international funds transfers or cross-border movements of funds (if applicable in a country)

Whichever authority is responsible, coordination between various authorities is important as they may hold information relating to unauthorised providers. Countries should be aware of the information that is available in their jurisdiction and ensure information is shared as appropriate to support the identification and sanctioning of unauthorised MVTS providers.

There can be a number of ways for awareness raising campaigns in respect of unauthorised MVTS. This should be done on a risk basis, i.e. not all countries should conduct awareness raising campaigns with the same intensity. Some of these examples include:

- Ensuring that the competent authorities responsible for overseeing and/or registering or licensing unauthorised MVTS providers know how to detect those services that have not registered or been licensed and are adequately resourced to do so.
- Making unauthorised MVTS providers aware of their obligations to license or register, as well as any other obligations with which they may have to comply. Using education and compliance programs, including visits to advise businesses which may be operating unauthorised MVTS of licensing or registration and reporting obligations, as opportunities to seek information about others in their industry. Using these outreach efforts by law enforcement and regulatory agencies to enhance their understanding about the operations, record keeping functions and customer bases of unauthorised MVTS operations. Extending outreach campaigns to businesses typically servicing unauthorised MVTS providers (such as shipping services, courier services and trading companies). Placing in trade journals, newspapers, web-pages or other publications of general distribution notices of the need for unauthorised MVTS providers to register or license and comply with other relevant requirements.
- Ensuring that law enforcement is aware of the compliance requirements for MVTS providers in addition to the methods by which those services are used for illicit purposes. Ensuring that the full range of training, awareness opportunities and other forms of education are provided to investigators with information about MVTS operations, their obligations under the regulatory regime and ways in which their services can be used for ML/TF. This information can be provided through training courses, presentations at seminars and conferences, articles in policing journals and other publications.
- Publishing guidelines to encourage licensing or registration and compliance with other relevant requirements. Additionally, issuing material to ensure financial institutions currently subject to STR requirements (e.g. banking sector) develop an understanding of MVTS. Informing potential customers about the risks of utilising illegal MVTS and their role in ML/TF.
- Requiring entities to display their registration/license to customers once they are registered/licensed. Legitimate clients will likely have a higher degree of confidence in using registered/licensed operators and may therefore seek out those operators displaying such documentation.
- Making a comprehensive and up-to-date list of all licensed or registered persons that provide MVTS publicly available.

The FATF has identified a number of effective practices in the area of identification strategies for unauthorised MVTS, which include[47]:

- Increasing and strengthening communication between supervisory authorities including self-regulatory bodies, MVTS organisations and the general public, in order to identify those institutions which have lost their licenses or registrations, specifically due to not complying with AML/CFT provisions.
- Examining the full range of media to detect advertising conducted by unauthorised MVTS providers and informing operators of their registration/licensing obligations. This includes national, local and community newspapers, radio and the internet; giving particular attention to the printed media in various communities; and monitoring activities in neighbourhoods or areas where unauthorised MVTS providers may be operating.
- Passing on, to the competent authorities, information about unauthorised MVTS providers uncovered during investigations effective practices include encouraging investigators to pay particular attention to ledgers of business that may be associated with unauthorised MVTS; encouraging enforcement agencies to look for patterns of activity that might indicate involvement of unauthorised MVTS; and, where possible, encouraging enforcement agencies to consider using undercover techniques or other specific investigative techniques to detect MVTS that may be operating illegally.
- Consulting with of registered / licensed MVTS providers and banks for potential leads on MVTS providers that are unregistered or unlicensed.
- Being aware that unauthorised MVTS are often utilised where there is bulk currency moved internationally, particularly when couriers are involved. Paying particular attention to the origin and owners of any such currency. Coordinating with border control agencies to identify instances of cross-border currency movement via couriers. Couriers could provide insights for the identification and potential prosecution of illegal operators with whom the couriers are associated, especially when potential violations by couriers are linked back to the source of the unauthorised MVTS operation.
- Paying particular attention to domestic suspicious transaction or unusual activity reporting, as well as to domestic and international large value cash reporting, where applicable, to identify possible links to unauthorised MVTS operations.
- Assisting banks and other financial institutions in developing an understanding of what activities/indicators are suggestive of unauthorised MVTS operations and using this to identify them. Many unauthorised MVTS

47 See FATF (2003).

providers maintain bank accounts and conduct transactions in the formal financial sector as part of other business operations. Giving banks the authority to crosscheck particular accounts against a register of these operators and notify the relevant regulatory authority as appropriate. These registers can also be made available online for easy access and search and may be updated at frequent intervals.

- Once unauthorised MVTS operations are identified, international exchange of information and intelligence on these entities between the relevant agencies can be facilitated. Consideration could be given to sharing domestic registers with international counterparts. This strategy would also assist jurisdictions to identify local operators not previously known.

Where unauthorised MVTS providers are identified, it is important to consider the reasons why they conducted their business without authorisation. If this is due to a lack of information, improved communication of the need for authorisation may be required. If operators do not register because they are concerned about their ability to meet compliance requirements, it is important to understand the concerns and to consider whether these can be addressed, for example by providing appropriate guidance.

EXAMPLES OF ACTION TAKEN BY AUTHORITIES AGAINST UNAUTHORISED MVTS PROVIDERS.

Mexico

According to Mexican Law (Article 101 of General Law of Auxiliary Credit Organizations and Activities), the provision of those services of the Mexican entity analogous to the MVTS (the "*transmisor de dinero*" or "money remitter") by someone who has not been registered for those purposes by the National Banking And Securities Commission, is a crime punished with prison from 3 to 15 years, and a fine of up to 100 000 days of wage (article 101 of the General Law of Auxiliary Credit Organizations and Activities).

The National Banking and Securities Commission (CNBV) has broad faculties to investigate and sanction natural and/or legal persons who are carrying out financial activities without authorisation. Thus, the CNBV imposes the suspension of activities to those offenders, among others effective, proportionate and dissuasive sanctions.

Moreover, in order to ensure that users and financial institutions are able to know which entities are authorised as MVTS, the CNBV website publishes a list of the registered MSBs and MVTS. Likewise, money remitters should indicate in any kind of advertisement their registration number and its issuance date. Additionally, the CNBV website has a mechanism in which people can report any MVTS without registration.

Netherlands

In the Netherlands, De Nederlandsche Bank N.V. (DNB) is authorised to supervise MVTS. Transferring money to and from foreign countries without prior authorisation by DNB is considered to be a violation of the Financial Supervision Act.

DNB is authorised to impose fines (max. EUR 4 million) and to issue a cease and desist order to stop the illegal activities. These activities also constitute a criminal offence, which is liable to proceedings by the Public Prosecutor.

In the autumn of 2014, DNB conducted several examinations into people and offices suspected of transferring money to and from foreign countries without prior authorisation by DNB. The goal of this project was to make a stand against illegal practices and to show the authorised payment institutions that illegal activities are not acceptable. These examinations involved an on-site inspection supported by the police. The on-site inspections revealed that several violations of the Dutch Financial Supervision Act had been committed. DNB has therefore imposed fines in several cases. DNB has also issued a press release on this subject in which the general public as well as the authorised MVTS providers were incited to report illegal MVTS activities to DNB. In addition, DNB used social media to get across its message[48].

Singapore:

Singapore has the following mechanism to deal with the issue:

- Physical surveillance: police look out for illegal remittance operators when patrolling areas where they are more likely to be active, such as places where migrant workers congregate.
- Public database of licensed operators: A public database of the names and addresses of licensed remittance businesses allows the public to cross-check remittance businesses and alert authorities to unlicensed activities.
- Outreach to likely users of unlicensed services: Target groups, such as migrant workers, are educated on the risks of using unlicensed remittance operators and directed towards the licensed operators. Siting licenced remittance services in convenient locations, such as foreign worker dormitories/ recreation centres.

48 Eenheid Rotterdam (5 January 2015), “Underground Banking”, www.youtube.com/watch?v=ThgVR6jM6kI

ANNEX 2. EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH TO THE MVTS SECTOR

Argentina

Law 25246, as amended, in its Section 20, subsection 2, establishes as legally bound reporting parties "the institutions governed by Law 18924, as amended, and natural or artificial persons authorized by the Central Bank of the Argentine Republic to operate in the purchase and sale of foreign currency in the form of cash money or cheques drawn in foreign currency, or by means of credit or debit cards or in the transfer of funds within the national territory and abroad".

FIU Resolution 66/2012 regulates the measures and procedures that shall be observed by fund remitters, in order to prevent, detect and report facts, acts, transactions or omissions that may constitute crimes of Money Laundering and Terrorist Financing.

Section 3 of this Resolution establishes the prevention policy for the purposes of correctly complying with the obligations arising from Law 25246. Among other aspects, said policy shall include the development of records of analysis and risk management about Money Laundering and Financing of Terrorism of detected unusual transactions and those that have been considered suspicious and thus have been reported.

As legally bound reporting parties, fund remitters shall adopt risk analysis policies. Section 18, subsection l) of this Resolution indicates that: Said risk analysis policies shall be gradual; enhanced measures shall be performed over higher risk customers and updates and analysis of information on the customer's economic, assets, financial and tax situation and corporate and control structure shall be conducted more frequently.

A regards to supervision, during 2014, the overall supervisory system has been strengthened to ensure correct implementation of AML/CFT prevention measures on part of the legally bound reporting parties, among which fund remitters are included. Verification procedure, both on-site and off-site, is performed based on a risk approach, according to FIU Resolution 229/2014. With respect to sanctions, in 2014, administrative summaries were applied to two fund remitters for non-compliance of the current AML/CFT obligations.

In addition, twice a year, the FIU coordinates intensified cross-border control of currency and negotiable instruments with the participation of country members of GAFILAT

Canada

Example of Guidance on the RBA:

FINTRAC provides guidance to reporting entities on operationalizing a risk-based approach to combatting money laundering and terrorist financing. This guidance is designed to help reporting entities to:

1) Consider business-wide elements or factors that may impact ML/TF risk and apply controls and measures to mitigate the risks, addressing:

- Products, services and delivery channels;
- The business' geography; and
- Other factors relevant to the business' specific activities (e.g. legal, environmental, etc.)

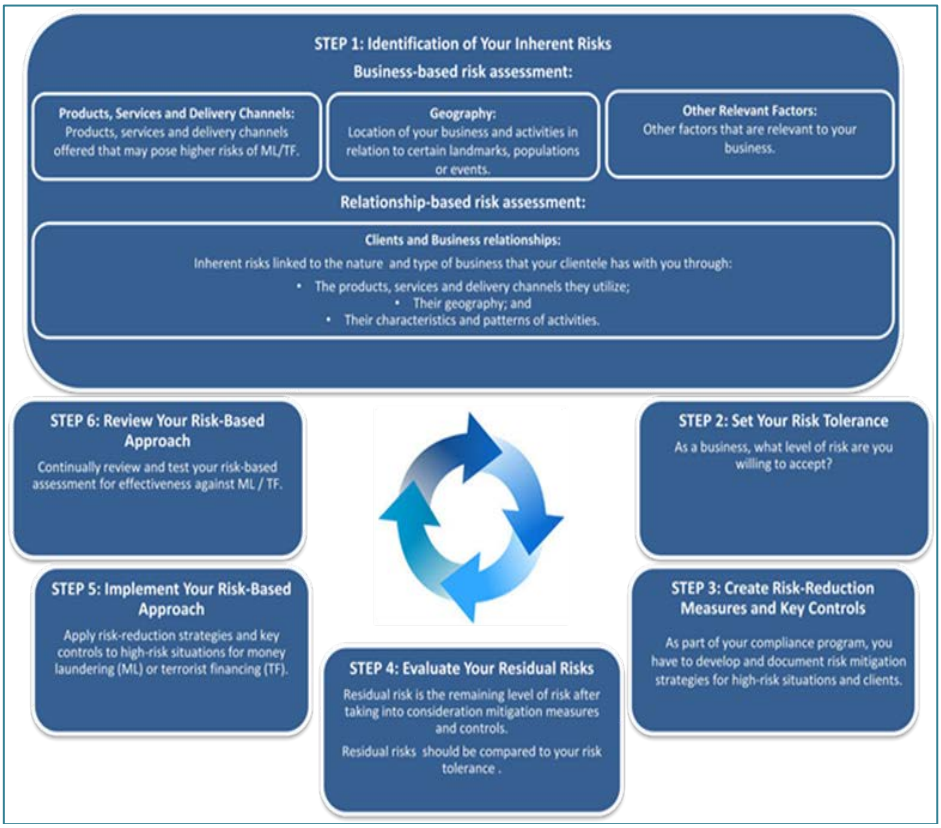
2) Evaluate the risks associated with the clients and business relationships by looking at:
   - The products, services and delivery channels they utilize;
   - The geography related to the clients (their location, links to high-risk countries, where they conduct their business and transactions, etc.); and
   - Their activities, transaction patterns, characteristics, etc.

   This specific assessment will allow reporting entities to identify high-risk business relationships and apply the prescribed special measures.

3) Identify and validate controls to mitigate high-risk activities and business relationships, including prescribed special measures; and

4) Review and assess the status of the business' compliance regime with Canada's laws as well as the adequacy of your current controls to mitigate the identified high risks.

This guidance accomplishes these four tasks through the following six step approach:



This document was prepared generally for all of Canada's FIs and DNFBPs and can be found at www.fintrac-canafe.gc.ca/publications/rba/rba-eng.asp. FINTRAC is aware that all sectors require more specific information to operationalize a meaningful risk-based assessment to combat ML/TF. To accommodate this need, FINTRAC is preparing sector specific workbooks to aid reporting entities in operationalizing their risk-based approach.

Italy

Money Transfer Proceeding ("Money River" Operation) - December 2014

As a result of systematic criminal behaviour committed by the suspects, eighteen (18) money transfer operators based in Rome were addressed by custody order on 17 December 2014 (10 out of 18 in prison and 8 under house arrest). Money transfer plays a significant role within Rome's economy and is almost exclusively consisting of foreign countries operators. The investigated operators illegally transferred abroad approx. EUR 1 billion, as a result of several predicate offences: import and sale of counterfeit goods, market fraud, sales of industrial products with false or misleading trademarks and tax evasion.

In particular, a huge sum of money was transferred abroad through a large number of illicit transfers of cash amounts (approx. EUR 785 000) below the threshold set by law, and illegally, since the operations were fictitious, performed without customer identification and with no indications of the nature of the underlying relationships. None of the requirements set by the Italian AML legislation was fulfilled.

Transfer operations were always made below the threshold – i.e. whereby the threshold for cash transactions was set at EUR 5 000 (up to 12 August 2011), operations then amounted to EUR 4 999 each; whereby the threshold was EUR 2 500 (up to 5 December 2011), operations then amounted to EUR2 499; and, most recently, with the threshold set at EUR 1 000, transactions amounted to EUR 999.

"*The money was transferred without any tax trace in Italy*" (as reported by the Judge in the mentioned custody order).

The convicted individuals were accused of: transnational criminal association and money-laundering arising from the related predicate offences (ascribed to the economic operators who made use of the activity carried out by money-launderers). In compliance with the law regulating legal persons' liability, the offences related to the crimes committed by their managers were also notified.

The case involved multiple criminal associations operating through the Rome-based Italian branch of the *XYZ* payment institution (i.e. a multinational company specialised in worldwide money transfers based in a foreign country), as well as 7 Rome-based money transfer agencies operating in the circuit headed by the mentioned Payment Institution.

The association members include the branch leaders and the representative in charge of AML checks, as well as a number of operators that violated laws on money transfer in order to carry out the above transactions.

Preliminary investigations lasted for about two years and were performed by the *Nucleo di Polizia Valutaria* of the *Guardia di Finanza* (*GdF*) through a wide array of investigative tools: wiretaps, video surveillance services, searches, seizures, watching and shadowing services, AML inspections and documentation analysis.

The investigations were inspired by the AML inspection into a Rome-based money transfer agency carried out by GdF upon own initiative. The inspection revealed abnormal operations involving a considerable amount of money transfer operations almost exclusively requested by non EU-citizens and addressed to their respective countries of origin.

Investigations (subsequently extended to another 6 Rome-based agencies of the Italian branch of the Payment Institution and numerous foreign traders) enabled shedding light on a widespread criminal network which – by making use of the services provided by the money transfer circuit headed by the Payment Institution, and taking advantage of systematic violation of AML legislation – managed to transfer huge cash flows by laundering the proceeds of tax evasion and unlawful activities related to trade of counterfeit products.

The cash was delivered to money transfer agencies or by their representatives who used to pick it up directly at the premises of the persons ordering the transfer operations.
The names used to perform the operations were invented, or belonged to deceased persons, or even to unsuspecting customers already registered in the Payment Institution management database and made accessible to the agencies operating within the circuit.

The fictitious character of the operations resulted from multiple sources:

- Documentation obtained;
- Wiretaps;
- Uneconomic character of operations compared to larger bank transfers (expressly chosen as they guaranteed anonymity, tax evasion, money-laundering and large profits to the money transfer operators, thus favouring combined economic and criminal interests for those committing predicate offences and money-launderers);
- Video surveillance agencies (few customers entering but huge volumes of transactions recorded);

Following inspections carried out by GdF at the premises of money transfer agencies, operators decided to resort to pick-up of the funds to be transferred directly from the premises of the subjects ordering the operations.

The subjects requesting money transfer operations were foreign entrepreneurs and traders operating in Italy (especially in Rome), with criminal records for committing crimes of various kinds (smuggling, counterfeiting, tax evasion).

The illegal transfer was managed and directed by persons who held important positions within the Payment Institution and enacted systems aimed at "circumventing" proper tracking of the origin of the sums. Among those addressed by restrictive measures: the temporary regional director, the AML supervisor, the sales department manager, and the head of unsettled debts office of the Italian branch. GdF executed the seizure of assets worth over EUR 13 million, equivalent to the profits

made by the Payment Institution and money transfer agencies through the illicit transactions performed.

Mexico

Ministry of Finance:

The Mexican Ministry of Finance modified the administrative rules so that the professional organisations of MVTS are able to draft the AML/CFT internal compliance manuals. This reduces costs due to scale economies, while taking into consideration the differences of specific sectors of MVTS and, ultimately, fostering AML/CFT compliance.

National Banking and Securities Commission (CNBV):

Several questionnaires have been conducted to Money Transmitters to deepen operability mechanisms, which is used to determine the risk degree of Money Transmitter. The questionnaire enables to know the geographical areas of increased operation, the number of related agents, the number of specific operations, parameters or amounts, among other data. This allows updating information on supervisory requirements based on major elements of risk and not just random or geographical information.

The Money Transmitters must inform the CNBV the name of related agents having a contractual relationship, as well as other parties that operate with their related agents; with this information corridors can be known.

Whenever an inspection is conducted, information of the entities is requested to the FIU regarding the behaviour that have generated them concern based on information analysis of relevant, unusual and internal reports and such reports sent to that authority.

The CNBV counts with a risk matrix that qualifies the risk to which every Money Transmitter is exposed; this matrix integrates information from geographic areas of major transactions, the number of branches and related agents to each society, the average number of employees, specific transactions, parameters or amounts, as well as the mitigating measures implemented by these. Based on such matrix, and concerns of the FIU, CNBV implements the Annual Inspection Visits Program with tasks that will be reviewed during the inspection visits.

Every time a Money Transmitter is cancelled because it did not complied correctly with its AML/CFT obligations, the CNBV monitors if it still sends any kind of operational report and, if it does, an specific area visits the cancelled entity and if it is still operating starts the corresponding administrative or criminal procedure to sanction the illegal entity.

Netherlands

In the Netherlands, De Nederlandsche Bank N.V. (DNB) is responsible for the supervision of MVTS. In addition to supervising MVTS authorised in the Netherlands, DNB also supervises Dutch-based agents of foreign MVTS, by virtue of the Anti-Money Laundering and Anti-Terrorist Financing Act *(Wet ter voorkoming van witwassen en het financieren van terrorisme – Wwft)*.

Each quarter, DNB analyses all money transfers made in the Netherlands and performs a network analysis on these transfers. Based on this network analysis, DNB is able to detect potentially unusual transaction patterns and take direct action by arranging on-site inspections. This working method allows DNB to perform her supervisory tasks effectively and efficiently. At present, DNB leverages this technique to supervise around a thousand locations in the Netherlands. Over the past year, DNB has imposed several formal measures as a result of this supervisory practice and made one report to the Public Prosecutor's Office with respect to a suspected case of money laundering.

Singapore

To balance the need to focus on the higher risk MVTS operators, while not being blind-sided by the broader population, supervisors could augment their resources by engaging external auditors/consultants to assist in performing periodic reviews of lower-risk entities. The MVTS sector may be more suited for such an approach where its operations and business model are generally less complex than banks.

Spain

At the end of 2009, SEPBLAC, in its FIU capacity, detected a fresh money laundering operation, carried out by criminals who, taking up the position of agents of payment institutions, were splitting amounts of cash into numerous remittances, which were attributed to fictitious identities and transferred to China. These funds were associated with payments for smuggled goods, tax fraud and other criminal activities.

SEPBLAC received suspicious activity reports with respect to this pattern of operation not only from payment institutions, but also from banking institutions in which certain agents had opened accounts, from which they were sending funds to be transferred to the MVTS. SEPBLAC examined the STRs and concluded that the suspicious activity reported did not refer to end-customer transactions, but rather that it was the agents themselves who were connected with ML/FT activities, and not the alleged customers, who were in reality inexistent.

Following a scrutiny of such reports, the relevant financial intelligence reports were sent by SEPBLAC to law enforcement agencies and Customs authorities. In October 2012, Spanish media revealed the results of this investigation, known as "*Operacion Emperador*". This large ML network is currently being prosecuted in Spain. A total of 110 people are being prosecuted in Spain, Germany and Italy and EUR 11.6 million in cash and EUR 11 million in bank accounts have been seized. The case involved laundering the proceeds of numerous predicate offences, including smuggling (undeclared or undervalued goods imported) and fiscal crimes.

At the same time, this problem was reported to SEPBLAC's Supervision Area which decided to undertake measures of a general nature applicable to the entire sector, as well as specific measures in relation to certain institutions.

1) General measures:

- Requirement for the payment institutions to send monthly statistical information broken-down by country and agent. This requirement expanded the statistical information which the Bank of Spain had been

collecting and which was accessible by SEPBLAC and it enabled SEPBLAC Supervision Area to conduct a strategic analysis on the money remittance sector. The findings of this strategic analysis were used to implement additional risk-based supervisory measures, selecting the targets according to the level of risk detected in the analysis and to adapt SEPBLAC's operational analysis to be more useful for competent authorities.

- Training and awareness-raising of institutions with respect to the need to control the activity of their agents, in order to comply with the obligation expressly contained in AML/CFT legislation. This objective was achieved by means of circulars sent to the representatives of the payment institutions and the organisation of specific meetings with the sector, where the problems posed by the laundering of money through agents and the ways to detect it and curtail it were explained.

2) Specific measures:

- SEPBLAC's Supervision Area decided to undertake extensive on-site inspections of certain money remitters in order to verify the nature of the phenomenon, its extent and how it was being managed by the various institutions. The outcome of these inspections caused, in the first place, the opening of several sanctioning case files against a number of institutions and, as a consequence thereof, there was a very significant increase in STRs filed by money remitters in relation to their agents. The result of these new STRs was incorporated by the police authorities into investigations already in progress, which made it possible to finally compile the information for initiating criminal proceedings.

Moreover, from the point of view of the activity of these companies, the outcome of this entire process has led to:

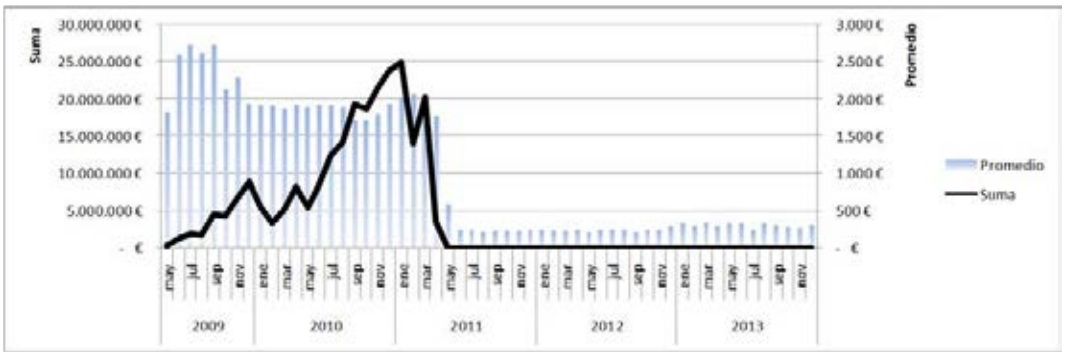
1) A "purging" process of the MVT sector, with the disappearance of several institutions and a general improvement in the controls existing among those remaining. A particularly significant development among the latter measures was the creation by the association of MVTs of a database of agents whose activity has been the subject of an STR. Money remitters are thus able to know immediately whether the person or company they are intending to contract as an agent, or which they have already engaged, has been the subject of an STR by another money remitter.

2) A reduction in the flows of illegal money channelled through money remitters, due to the improvements introduced into their AML/CFT systems and to the measures put into place by the sector overall. In 2013, SEPBLAC measured the impact of the decisions and measures taken as a result of its strategic analysis, and established that the total amount of high risk transactions in the money remittance sector has considerably decreased as revealed by graphs below:

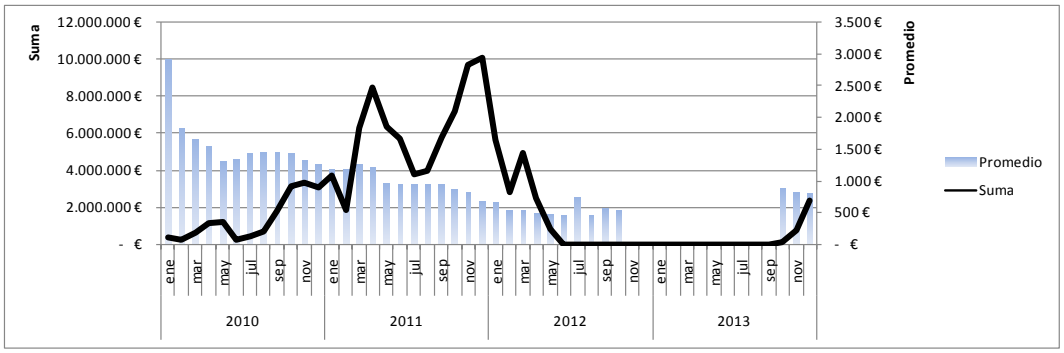
China

Remittances to China

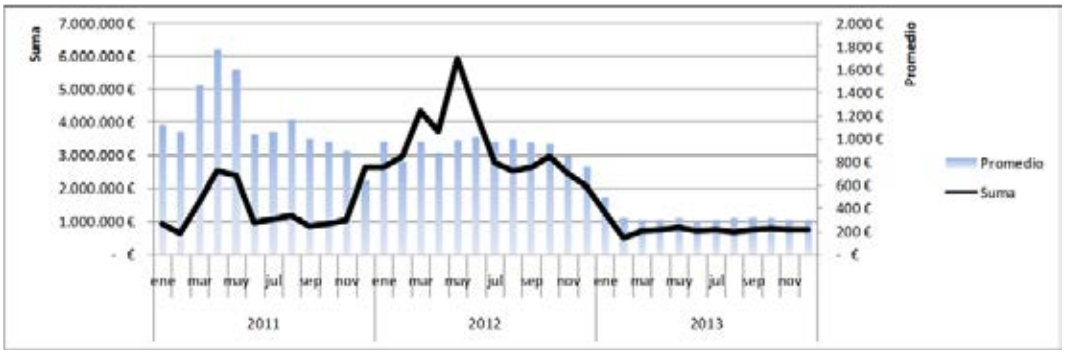
Institution A (2009 – 2013)



Institution B. (2010 – 2013)



Institution C. (2011 – 2013)



United States

Supervisory Guidance on Risk Management Associated with MVTS

- The office of the comptroller of the currency (OCC), a US banking supervisor, issued a "statement on risk management associated with money services businesses" to provide clarification to national banks, federal savings associations, and federal branches and agencies of foreign banks (collectively, banks) on the agency's supervisory expectations with

regard to offering banking services to money services businesses (MSB). Available at www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-58.html

- Joint guidance – FIU and supervisor. In 2005, the US FIU (FinCEN), together with all the US. Banking supervisors collectively called the "federal banking agencies", jointly issued a statement to address expectations regarding banking institutions' obligations under the Bank Secrecy Act for money services businesses, such as check cashers and money transmitters. Available at www.fincen.gov/news_room/nr/html/20050330.html

ANNEX 3. EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH TO THE BANKING SECTOR WITH MVTS PROVIDERS AS CUSTOMERS

Mexico

National Banking and Securities Commission (CNBV)

The CNBV published on its website a compliance chart with the levels of legal compliance on AML/CFT matters, including Money Transmitters, among others. The chart aims to increase financial transparency and build trust between the supervised entities and users of financial services.

The CNBV has practiced visits to the main FIs that send their customers' resources through concentration accounts, as well as to such banks that have opened concentration accounts of brokerage firms, it has been recommended since 2009, to this sector, to implement the following measures:

Privilege:

a) The use of a referenced number for those accounts being used in concentration and dispersion of resources.

b) The use of electronic transfers to concentrate resources on these kinds of accounts, since it allows the identification of the resource's origin.

Implement:

a) Special monitoring to identify the source of the received funds by means of transfers.

b) Random special monitoring in order to identify the origin of the resources received through documents (checks).

c) Prohibition of receiving cash deposits through concentration accounts.

d) Information exchange with FIs where concentration accounts are opened.

As a result of the financial reform published in the Official Journal of the Federation (DOF -for its acronym in Spanish-) on January 10th 2014, the CNBV will certify professionals, compliance officers and independent external auditors who provide services to entities and persons subject to supervision by the CNBV on AML/CFT matters. This certification will provide the FIs and supervised subjects with confidence and will foster stability of the Mexican financial system. On October 2nd 2014, was published in the DOF the general provisions for certification of independent, external auditors, compliance officers and other professionals in the prevention of transactions with illegal proceeds and terrorist financing; and on March 13th 2015, was published through the same means the Agreement by which it is disclosed the Calendar to start the certification process of independent external auditors, compliance officers and other professionals in the prevention of operations with resources illegal proceeds and terrorist financing.

According to this calendar the certification program will start with the banking sector, followed by brokerage firms and regulated multiple purpose financial companies (Sofoms) before the end of 2015.

ANNEX 4. EXAMPLES OF PRIVATE SECTOR PRACTICES IN APPLICATION OF RBA

Canada

Example of private sector effective practices for Agent Risk

a.) When onboarding agents, conduct beneficial ownership assessment, criminal background check, media scan for negative press, check of compliance credentials.

b) In dealing with agents on an ongoing basis, conduct an ongoing risk assessment of their business and provide training, outreach, and transaction monitoring in accordance with their risk. Conduct mystery shopping and compliance testing internally.

c) Having a clear and defined process for resolving customer complaints and de-registering agents.

d) Sharing information on de-marketed agents and customers with other industry participants.

Example of private sector effective practices for Customer Risk

e) When on-boarding clients, checking beneficial ownership, criminal background, and media scan of clientele.

Example of private sector effective practices for Internal Controls

f) Dedicated compliance staff that are not compensated in accordance with transactions, business relationships or on-boarding agents.

Japan

One MVTS provider has been voluntarily setting maximum fund transfer amount from JPY 100 000 to JPY 500 000 yen per one day according to the beneficiary countries' risk situations, and also the fund transfer has been limited to two transactions in maximum per one day (fund transfer from different business locations is not permitted).These measures have been taken due to the increasing illegal fund transfer case using money mule in Japan.

The Netherlands

In the Netherlands, the Dutch Association of Money Transfer Companies has developed a code of conduct. This code of conduct applies to all members of the Dutch Association of Money Transfer Offices (NVGTK) and is intended to set minimum requirements for risk management and compliance with regard to money laundering and other criminal activities. This code of conduct strives to implement these requirements based on the following themes: compliance, customer agreement, risk criteria, customer due diligence, monitoring, reporting unusual transactions, payment service agent due diligence, training and knowledge level, retaining evidence, and complaints procedure. (www.nvgtk.nl/actueel/gedragscode--code-of-conduct)

Spain

As a consequence of the awareness-raising process developed with this sector regarding the risks of agents, the main association of MVTS providers has created a database of "bad agents".

This is an industry-held register of high risk agents (or the so-called "bad agents"), through which MVTS providers can share alerts with each other about those agents whose transactions(not singular transactions, but the whole business managed by that agent) have been reported to the FIU and business relationships terminated. Usually, these decisions are based on the suspicious that these agents are splitting amounts of cash into numerous remittances, which are attributed to fictitious identities and transferred to third countries.

Making use of that database, every time a MVTS provider is going to initiate business relationships with a new agent, they can check whether his/her transactions have been reported to the FIU as suspicious or not.

ANNEX 5. EXAMPLE OF COMPLIANCE PRACTICES OF AND IN RELATION TO A LOW RISK MVTS

This Annex is intended to support supervisors and banks to identify lower risk MVTS providers. This Annex can assist in bridging the gap between the current guidance and supervisory and compliance practices in relation to lower risk MVTS providers.

Characteristics that may factor into lower risk MVTS may be as follows:

- Registered/Licensed with annual audits and regulatory exams.
- Publicly-traded or well capitalized.
- Stable track history with substantial infrastructure.
- Established AML/CFT program.
- Ability to quickly and accurately provide customer specific information (i.e. transaction logs).
- Direct interaction with consumers (as opposed to nested wholesalers or large commercial transactions).
- Low dollar, domestic consumer-based transactions (non-cross border).
- Low dollar, cross-border consumer remittances.
- Licensed agents monitored by licensed parent.
- Established and transparent network of counterparties (foreign).
- A small number of known, regular customers with a pattern of repeat micro-transactions often linked to a pay or salary cycle and with senders and recipients normally linked by family ties.

REFERENCES AND BIBLIOGRAPHY

Chatain *et al* (2011), *Protecting Mobile Money Against Financial Crimes*, World Bank, Washington, D.C., http://dx.doi.org/10.1596/978-0-8213-8669-9

De Koker, Louis and Symington, John (2014), "Conservative corporate compliance: Reflections on a study of compliance responses by South African banks" in *Law in Context*, Volume 30, 2014: 228-256

FATF (2015a), *Guidance for a risk-based approach: effective supervision and enforcement by AML/CFT supervisors of the financial sector and law enforcement*, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-effective-supervision-and-enforcement.html

FATF (2015b), *Guidance for a risk-based approach to virtual currencies*, FATF, Paris, www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

FATF (2015c), *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html

FATF (2015d), *Emerging Terrorist Financing Risks*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

FATF (2014), *Guidance for a risk-based approach for the banking sector*, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html

FATF (2013a), *National money laundering and terrorist financing risk assessment*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

FATF (2013b), *The role of Hawala and other similar service providers in money laundering and terrorist financing*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html

FATF (2013c), *Politically exposed persons (Recommendations 12 and 22)*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/peps-r12-r22.html

FATF (2013d), *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, FATF, Paris, www.fatf-gafi.org/publications/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html

FATF (2013e), *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html

FATF (2013f), *Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems,* FATF, Paris, www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (the "FATF Recommendations"), FATF, Paris, www.fatf-gafi.org/recommendations

FATF and MONEYVAL (2010), *Money laundering through money remittance and currency exchange providers*, FATF, Paris and MONEYVAL, Strasbourg, www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingthroughmoneyremittanceandcurrencyexchangeproviders.html

FATF (2003), *Combating the abuse of alternative remittance systems*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/internationalbestpracticescombatingtheabuseofalternativeremittancesystemssrvi.html

FATF

GUIDANCE FOR A RISK-BASED APPROACH
MONEY OR VALUE TRANSFER SERVICES

Money or Value Transfer Services (MVTS) providers play an important role in the international financial system, in particular for the migrant communities around the world.

This guidance will assist countries and their competent authorities, as well as the practitioners in the MTVS sector and in the banking sector that have or are considering MVTS providers as customers, to apply the risk-based approach to the development of measures to combat money laundering and terrorist financing for the MVTS sector.

The risk-based approach, the cornerstone of the FATF Standards, requires that measures to combat money laundering and terrorist financing are commensurate with the risks.

www.fatf-gafi.org | February 2016

Appendix II:

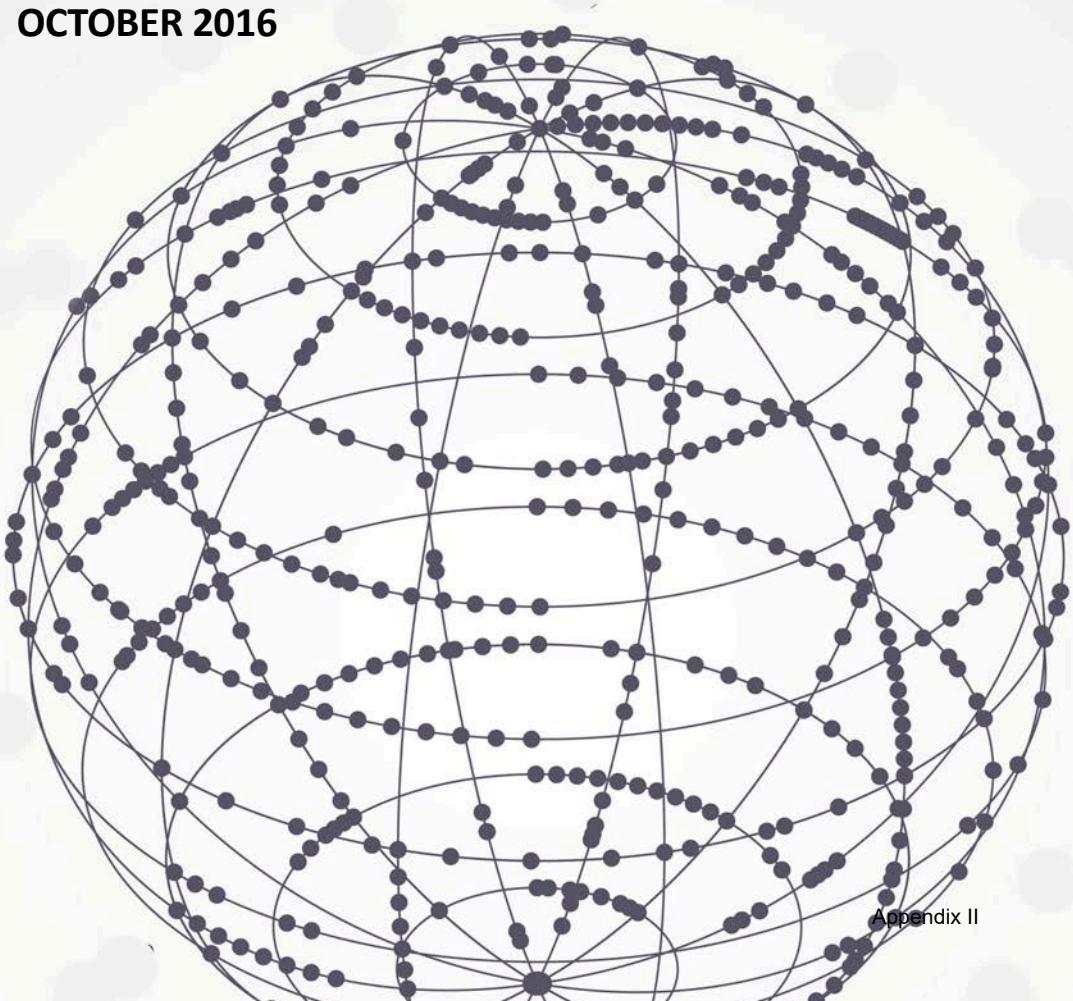
FATF, *FATF Guidance: Correspondent Banking Services* (Paris: FATF, 2016).

FATF

FATF GUIDANCE

CORRESPONDENT BANKING SERVICES

OCTOBER 2016



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2016), *Guidance on correspondent banking services,* FATF, Paris
www.fatf-gafi.org/publications/fatfrecommendations/documents/correspondent-banking-services.html

LIST OF ACRONYMS

AML	Anti-money laundering
BCBS	Basel Committee on Banking Supervision
CDD	Customer Due Diligence
CFT	Counter-terrorist financing
CPMI	Committee on Payments and Market Infrastructures
DNFBP	Designated Non-Financial Business Professions
EDD	Enhanced Due Diligence
MVTS	Money or value transfers service
RBA	Risk-based approach

GUIDANCE ON CORRESPONDENT BANKING SERVICES

This Guidance should be read in conjunction with the *FATF Recommendations*, especially Recommendations 1, 6, 7, 10, 11, 13, 14, 16, 20 and 26, their Interpretive Notes and the Glossary.

This Guidance should also be read in conjunction with the following FATF guidance papers and typologies reports which relate to proper implementation of the risk-based approach (RBA) in the banking and money or value transfer (MVTS) sectors:

- FATF RBA Guidance for the banking sector, 2014
- FATF RBA Guidance for Money or Value Transfer Services, 2016
- Guidance on the Risk-Based Approach for Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement, 2015
- FATF Guidance on AML/CFT and Financial Inclusion, 2013
- FATF Guidance on Politically Exposed Persons, 2013
- FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers, 2010 and
- FATF Report: The role of Hawala and other similar service providers in money laundering and terrorist financing, 2013.

The following guidance papers and tools are also relevant sources of information on how to manage the risks of correspondent banking relationships:

- Basel Committee on Banking Supervision, Guidance on Sound Management of Risks Related to Money Laundering and Financing of Terrorism, 2014
- Wolfsberg Group, Anti-Money Laundering Principles for Correspondent Banking, 2014, and
- Wolfsberg Group, Anti-Money Laundering Questionnaire, 2014.
- Committee on Payments and Market Infrastructures, Correspondent Banking – consultative report, 2015
- Basel Committee on Banking Supervision Supervisory Guidance for Managing Risks Associated with the Settlement of Foreign Exchange Transactions, 2016

I. INTRODUCTION

A. BACKGROUND – FATF ACTION TO ADDRESS DE-RISKING IN THE CORRESPONDENT BANKING CONTEXT

1. In the wake of the global financial crisis and countries' response to it, the international community has been increasingly concerned about *de-risking.* The FATF understands this term to mean situations where financial institutions terminate or restrict business relationships with entire countries or classes of customer in order to avoid, rather than manage, risks in line with the FATF's risk-based approach (RBA). This is a serious concern for the FATF and the FATF-style regional bodies (FSRBs) to the extent that de-risking may drive financial transactions into less/non-regulated channels, reducing transparency of financial flows and creating financial exclusion, thereby increasing exposure to money laundering and terrorist financing (ML/TF) risks.

2. Analytical work undertaken so far by different bodies, including the FATF,[1] shows that de-risking is a complex issue driven by various considerations including: profitability; reputational and liability risks; changes in banks' financial risk appetites; the amount of financial penalties imposed by supervisory and law enforcement authorities, increased compliance costs associated with implementing conflicting regulatory requirements, including anti-money laundering and counter-terrorist financing (AML/CFT) and confusion caused by the term Know-Your-Customer's-Customer (KYCC). A recent survey[2] also shows that in some cases, banks will exit the relationship solely on the basis of profits ("de-marketing"), irrespective of the risk context and of market circumstances.

3. The term KYCC has created a lot of confusion. To clarify, the *FATF Recommendations* do not require financial institutions to conduct customer due diligence on the customers of their customer (i.e., each individual customer). In a correspondent banking relationship, the correspondent institution will monitor the respondent institution's transactions with a view to detecting any changes in the respondent institution's risk profile or implementation of risk mitigation measures (i.e. compliance with AML/CFT measures and applicable targeted financial sanctions), any unusual activity or transaction on the part of the respondent, or any potential deviations from the agreed terms of the arrangements governing the correspondent relationship. In practice, where such concerns are detected, the correspondent institution will follow up with the respondent institution by making a request for information (RFI) on any particular transaction(s), possibly leading to more information being requested on a specific customer or customers of the respondent bank. There is no expectation, intention or requirement for the correspondent institution to conduct customer due diligence on its respondent institution' customers.

[1] The FATF circulated a questionnaire to banks and MVTS in late 2015 to gather information from the private sector which helped to form the basis of this guidance.

[2] ACAMS/Dow Jones (2016), *Global Anti-Money Laundering Survey Results 2016,* http://files.acams.org/pdfs/2016/Dow_Jones_and_ACAMS_Global_Anti-Money_Laundering_Survey_Results_2016.pdf.

4. In June 2015, the FATF issued a public statement[3] to clarify that, when establishing correspondent banking relationships, correspondent institutions are required to perform customer due diligence (CDD) on the respondent institution, and gather sufficient information about the respondent institution to understand its business, reputation and the quality of its supervision, including whether it has been subject to a ML/TF investigation or regulatory action, and to assess the respondent institution's AML/CFT controls. It was clarified that the *FATF Recommendations* do not require correspondent institutions to perform CDD on the customers of their respondent institutions when establishing correspondent banking relationships or in the course of the relationship.

5. Although the financial sector welcomed that and other FATF public statements on de-risking,[4] it also sought further clarification on supervisory expectations for conducting customer due diligence on correspondent institution's respondents. In turn, supervisors and regulators need to be clear about how they assess financial institutions against those expectations. For that reason, the FATF committed to developing guidance to further clarify supervisory expectations for correspondent banking relationships in relation to the obligations defined by the FATF standards. This clarification is consistent with the FATF's overall approach to de-risking which is based on the effective implementation of the global AML/CFT standards, in line with the FATF's RBA. The *FATF Recommendations* require financial institutions to identify, assess and understand their ML/TF risks, and implement AML/CFT measures that are commensurate with the risks identified. Indeed, the RBA is the cornerstone of an effective AML/CFT system, and is essential to effectively managing risks.

6. Prudential and other regulatory requirements as well as the complexity, number and changes in sanctions regimes, and also uncertainty related to the interplay of different sanctions regimes and their applicability to financial institutions, were also mentioned as drivers of de-risking. AML/CFT regulations are therefore only one of a multitude of factors cited for closing correspondent banking relationships. These results are largely in line with the prevailing understanding of the FATF and other international organisations doing work in this area, including the Financial Stability Board (FSB), Committee on Payments and Market Infrastructures (CPMI), Basel Committee for Banking Supervision (BCBS)'s Anti-Money Laundering Experts Group (AMLEG), International Monetary Fund (IMF) and the World Bank.

7. Although many of the factors contributing to de-risking go far beyond AML/CFT and the FATF mandate, the FATF is committed to addressing this issue to the extent it can by issuing guidance clarifying how to implement the FATF's RBA properly and effectively, consistent with previous FATF guidance.[5]

[3] See FATF(2015), *Drivers for "de-risking" go beyond anti-money laundering / terrorist financing* www.fatf-gafi.org/publications/fatfrecommendations/documents/derisking-goes-beyond-amlcft.html.

[4] See the public statements issued by FATF on de-risking in October 2014, June 2015 and October 2015.

[5] Including *Revised Guidance on AML/CFT and Financial Inclusion* (2013).

8. Correspondent banking is an activity that has been negatively impacted by de-risking in certain regions[6] and sectors. This is of concern to the international community, as correspondent banking is an important means of facilitating cross-border movements of funds, and enabling financial institutions to access financial services in different currencies and foreign jurisdictions, thereby supporting international trade, charitable giving, commerce and remittances flows, all of which contributing to promoting financial inclusion.

B. THE PURPOSE OF THIS GUIDANCE, THE TARGET AUDIENCE, AND THE STATUS OF THIS GUIDANCE

9. The purpose of this Guidance is to address de-risking by clarifying the application of the FATF standards in the context of correspondent banking relationships and money or value transfer service (MVTS) providers rendering similar services (i.e. MVTS acting as intermediaries in processing and/or executing the transactions of their own customers through accounts – see II d) below) by:

a) supporting the development of a common understanding of what the RBA entails for banks engaged in correspondent banking activity and MVTS providers rendering similar services; respondent institutions with MVTS providers as customers; and financial institutions relying on third-party MVTS providers, in their role as intermediaries, to execute payment transactions,

b) clarifying the interplay between the FATF standards on cross-border correspondent banking (Recommendation 13) and MVTS providers acting as intermediaries, and the FATF standards on customer due diligence (Recommendation 10) and wire transfers (Recommendation 16), as well as on targeted financial sanctions (Recommendations 6 and 7),

c) highlighting the extent to which correspondent institutions and MVTS providers offering similar services may gain a sufficient understanding of the customers of the respondent institutions and the associated risks, and

d) clarifying the expectations for correspondent institutions when dealing with respondents whose customer bases include MVTS providers.

10. The target audiences of this Guidance are:

a) banks and MVTS providers engaged in providing correspondent banking or respondent banking services,

b) financial institutions with account holders that are MVTS which in turn provide correspondent banking-type services to their own customers (as opposed to MVTS providers who are holding and using their account for their own corporate purposes), and

[6] Refer to: Joint Survey by the Union of Arab Banks (UAB) and the International Monetary Fund (IMF); The World Bank's Fact Finding Summary from De-risking Surveys and Withdrawal from Correspondent Banking: Where, Why, and What to Do About It.

c) competent authorities (particularly AML/CFT regulators and supervisors of banks and of MVTS providers).

11. It should be noted that this Guidance has been prepared in collaboration with the FSB, which is coordinating work to assess and address the extent and causes of banks' withdrawal from correspondent banking to identify possible policy responses to address this issue[7], through the implementation of a four-point action plan (data collection, clarification of regulatory expectations, domestic capacity building, and strengthening the tools for due diligence) coordinated by the Correspondent Banking Coordination Group. Other international organisations doing related work in the correspondent banking area (for ex. CPMI and BCBS) have also been closely associated to development of this FATF Guidance.

12. This Guidance draws on the experiences of countries and of the private sector to assist competent authorities and financial institutions in effectively implementing applicable *FATF Recommendations* using the risk-based approach to avoid the unintended consequences of de-risking. It also uses input from other relevant standard setters, and especially the BCBS with its Guidance on *Sound management of risks related to money laundering and financing of terrorism* (Annex II on correspondent banking). This FATF Guidance is non-binding and does not overrule the purview of national authorities to, among other things, assess and regulate correspondent banking activities and MVTS sectors as per the legal, supervisory and regulatory frameworks established in each country and/or region, the ML/TF risks present in each jurisdiction, individual institution's risk assessments and other contextual factors (e.g. sophistication and maturity of the national regulatory and supervisory regime).

II. DEFINITIONS

13. The following definitions apply for the purposes of this Guidance:

a) *Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services[8].

Correspondent banking does not include one-off transactions or the mere exchange of SWIFT Relationship Management Application keys (RMA)[9] in the context of non-

[7] FSB (2015), *Report to the G20 on actions taken to assess and address the decline in correspondent banking*. www.fsb.org/wp-content/uploads/Correspondent-banking-report-to-G20-Summit.pdf

[8] FATF Glossary

[9] The SWIFT RMA is a messaging capability enabling SWIFT members to exchange messages over the network and can create a non-customer relationship in particular cases of cash management, custody, trade finance, exchange of messages with payments and securities markets infrastructure entities, e.g., exchanges depositories

customer relationships, but rather is characterised by its on-going, repetitive nature.

Correspondent banking services encompass a wide range of services which do not all carry the same level of ML/TF risks. Some correspondent banking services present a higher ML/FT risk because the correspondent institution processes or executes transactions for its customer's customers.

Hence, the focus of this guidance is correspondent banking relationships that are higher risk, in particular cross-border correspondent banking relationships involving the execution of third party payments.

This guidance also applies to money or value transfer services (MVTS) acting as intermediaries for the transfer of funds or value (see d below), in line with Recommendation 13 which applies to financial institutions engaging in cross-border correspondent banking *and other similar relationships*. This guidance does not apply to securities transactions,

b) *correspondent institution* means the bank or MVTS provider which processes and/or executes transactions for customers of the respondent institution or MVTS provider the account of which is used to process and/or execute the transaction of its customer. The correspondent institution generally does not have direct business relationships with the customers of the respondent institution, unless it provides payable-through-account services (see paragraph 21 below). Those respondents' customers may be individuals, corporations or financial services firms.[10] In addition to the processing of third-party payments, a correspondent institution may also provide other services to the respondent institution, such as trade-finance related services, cash clearing, liquidity management and short-term borrowing, foreign exchange or investment in a particular currency,

c) *respondent institution* means the financial institution that is the direct customer of the correspondent institution,

d) *money or value transfer service (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other means of stored value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such service providers can involve one or more intermediaries and a final payment to a third party, and may include new payment methods. Sometimes these services

[10] This definition is generally in line with the definition of *correspondent bank* set out of page 24 of the Basel Committee on Banking Supervision guidance on *Sound management of risks related to money laundering and financing of terrorism*, which has been extended for the purposes of this guidance to also include MVTS which are providing financial services as intermediaries in the same way that a correspondent bank would.

have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen.*[11]

MVTS providers "offer similar services" as correspondent institutions when they act as intermediaries for other MVTS providers or where an MVTS provider is accessing banking or similar services through the account of another MVTS customer of the bank,

e) from the Glossary of the *FATF Recommendations*, the definitions of *competent authorities*,[12] *and financial institutions*.[13]

III. IDENTIFYING THE RISKS – THE INTERPLAY OF RECOMMENDATIONS 10 AND 13

A. DUE DILIGENCE ON THE RESPONDENT INSTITUTION

14. The requirements of both FATF Recommendations 10 and 13 must be met in all cases before cross-border correspondent banking services may be provided to a respondent institution. FATF Recommendation 13 requires additional measures to be applied to cross-border correspondent banking relationships, in addition to performing the CDD and enhanced due diligence (EDD) measures in FATF Recommendation 10 for high risk customers.[14] Such additional measures are appropriate because cross-border correspondent banking relationships are seen to be inherently higher risk than domestic correspondent customer relationships. Consequently, simplified CDD measures are never appropriate in the cross-border correspondent banking context, when activities described in para. 13 (a) are conducted.

---

[11] This definition can be found in the Glossary to the *FATF Recommendations.*

[12] *Competent authorities* refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as competent authorities.

[13] *Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public; 2. Lending; 3. Financial leasing; 4. Money or value transfer services; 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money); 6. Financial guarantees and commitments; 7. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading. 8. Participation in securities issues and the provision of financial services related to such issues; 9. Individual and collective portfolio management; 10. Safekeeping and administration of cash or liquid securities on behalf of other persons; 11. Otherwise investing, administering or managing funds or money on behalf of other persons; 12. Underwriting and placement of life insurance and other investment related insurance; 13. Money and currency changing.

[14] For information on cases in which enhanced CDD measures are required, refer to the Interpretive Note for FATF Recommendation 10, paragraph 20.

15. Although additional CDD measures always apply to cross-border correspondent banking relationships as described above, correspondent banking relationships may be diverse in nature and therefore some may be higher risk than others. Financial institutions should therefore recognise the degree of risk of different types correspondent banking activity, including in activities considered as higher risks, as described in para. 13 (a).

16. Correspondent institutions, in assessing the risks of their respondent must ensure that the assessment is sufficiently robust to consider all the relevant risk factors. By doing so, the different levels of inherent risks are clearly understood and appropriate controls applied to each, ensuring the effective management of these risks. Accordingly, the extent to which additional measures should be applied will vary on a case-by-case basis, depending on the level or type of residual risk, including the measures the respondent institution has implemented to mitigate its own ML/TF risks. Factors to consider in assessing correspondent banking risks could include for instance the respondent institution's jurisdiction, the products/services it offers and its customer base. It is not possible to develop a conclusive list of types of higher risk relationships for several reasons. First, there is no exhaustive list of risk factors that could be used to identify such relationships that would apply equally to all relationships. Second, both relevant risk factors and applicable risk mitigation measures must be considered together to form an accurate and comprehensive picture of the risks. For these reasons, any effort to define what constitutes a higher risk relationship could have the unintended consequence of encouraging rather than discouraging de-risking by promoting a more rules-based and tick-the-box approach to risk management. The risk factors included in the Annex II of the BCBS Guidelines on *Sound management of risks related to money laundering and financing of terrorism*[15] are examples of factors which correspondent institutions can use when assessing the risks of their correspondent banking relationships.

17. When entering into a business relationship, as a first step, the correspondent institution should identify and verify the identity of the respondent institution, using reliable, independent source documents, data or information (Recommendation 10 (a)). It should also identify and take reasonable measures to verify the identity of the beneficial owner(s), such that the correspondent institution is satisfied that it knows who the beneficial owner(s) of the respondent institution is/are. In order to do that, the correspondent institution should also understand the ownership and control structure of the respondent institution.[16] The information about the ownership and control structure includes conducting verification enabling the correspondent institution to be satisfied that the respondent institution is not a shell bank.[17]

18. Additionally, the correspondent institution should gather sufficient information to understand the purpose and intended nature of the correspondent banking relationship with the

[15] Para 7.

[16] FATF Recommendation 10, sub-paragraph 4(a) and (b)

[17] FATF Recommendation 13 prohibits financial institutions from entering into correspondent banking relationships with shell banks. The Glossary to the *FATF Recommendations* defines the term *shell bank* to mean a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not in itself constitute physical presence.

respondent institution.[18] This includes understanding what types of customers the respondent institution intends to service through the correspondent banking relationship and how it will offer services (e.g. through nested relationships as noted in para. 21), including the expected activity level, the transaction volume and value, the nature of the planned transactions and the extent to which any of these are assessed as high risk by the respondent institution.

19. The correspondent institution should also gather sufficient information and determine from publicly available information the reputation of the respondent institution and the quality of its supervision, including whether (and when) it has been subject to a ML/TF investigation or regulatory action.[19]

20. In addition, the correspondent institution should assess the respondent institution's AML/CFT controls.[20] In practice, such an assessment should involve reviewing the respondent institution's AML/CFT systems and controls framework. The assessment should include confirming that the respondent institution's AML/CFT controls are subject to independent audit (which could be external or internal). A more detailed/in-depth review should be conducted for higher risk relationships, possibly including reviewing the independent audit, interview of compliance officers, a third party review and potentially an onsite visit.

21. The correspondent institution should also understand how the respondent institution will be offering services available through the correspondent banking relationship to its customers and assess the nature and level of risk associated with offering arrangements. There are several possible arrangements for offering services, e.g.

- by establishing correspondent accounts to which the respondent institution's financial institution customers do not have direct access, but instead transact indirectly through the account via payment instructions delivered to the respondent institution;
- by establishing *nested relationships*[21] (i.e. downstream banking) which require that:
  - ✓ the correspondent institution is duly informed about the existence of such relationships and the operations/transactions of the customers of the nested institutions, that the locations in which the nested institutions conduct business are transparent to, and understood by, the correspondent institution, and the respondent is transparent in formatting payment instruction so all involved parties are included for monitoring and screening purposes;

[18] FATF Recommendation 10, sub-paragraph 4(c).

[19] FATF Recommendation 13, sub-paragraph (a).

[20] FATF Recommendation 13, sub-paragraph (b). One of the tools that could be used as a starting point is the Wolfsberg questionnaire

[21] "Nested correspondent banking refers to the use of a bank's correspondent relationship by a number of respondent banks through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services." (footnote 43 in Annex II of the BCBS *Guidelines on Sound management of risks related to money laundering and financing of terrorism*)

- ✓ the correspondent institution has measures in place to detect potential, undisclosed nested relationships provided by the respondent and takes appropriate follow-up action when a respondent does not disclose the existence of a nested relationship;

- ✓ the correspondent institution understands the respondent's control framework with respect to those relationships. Such review should take into account the implementation of appropriate controls to address the underlying risks posed by these relationships (for instance, if the transaction monitoring procedures are comprehensive of the relevant factors, whether they are based on manual transaction reviews and the accuracy of the automated ones, whether the institution has the resources to conduct such reviews, etc.);

- by establishing *payable-through accounts*[22] which can also be offered provided that the correspondent institution identifies risks associated with the relationship and applies enhanced controls to monitor transaction activity that are commensurate with the identified risks. The correspondent should have policies, procedures and processes in place to enable it to identify the ultimate user of the account and needs to be satisfied that the respondent institution has conducted sufficient CDD on the customers having direct access to the account of the correspondent institution, has appropriate controls in place to identify and monitor the transactions conducted by those customers and is able to provide relevant, individual CDD information upon request to the correspondent institution.[23]

B. DEVELOPING AN UNDERSTANDING OF THE RESPONDENT INSTITUTION'S BUSINESS

22. The correspondent institution should also gather sufficient information to understand the nature of the respondent institution's business in line with the risks identified.[24] This means that correspondent institutions are required to understand the target markets and customer segments that are served by their respondent (as outlined in para. 18) as part of their assessment of risks. Understanding the business profile of the respondent institution requires the correspondent to consider all relevant risk factors[25] (e.g. developing a general overview of the respondent institution's products and services and customer base, including nested relationships; countries and markets in which it operates; transactions in which it engages on behalf of its customer base and

[22] Payable-through-accounts (pass-by accounts) are correspondent accounts that are used directly by third parties to transact business on their own behalf (INR 13). They are used by foreign financial institutions to give their customers access to the domestic banking system. This enables the foreign bank's customers to write checks and make deposits at a bank in the jurisdiction like any other accountholder (in effect, giving customers of respondent banks access to more services).

[23] FATF Recommendation 13, sub-paragraph (e).

[24] FATF Recommendation 13, sub-paragraph (a).

[25] In the context of a correspondent banking relationship, the correspondent institution's customer is the respondent institution.

delivery channels it uses).[26] This includes verification by the correspondent institution that the respondent institution does not permit its accounts to be used by shell banks.[27]

IV. VERIFYING RESPONDENT INSTITUTIONS' INFORMATION, AND ASSESSING/DOCUMENTING HIGHER RISKS

23. When establishing new correspondent banking relationships, the correspondent institution may obtain information required by Recommendations 10 and 13 directly from the respondent institution. However, as noted in para. 17 above, this information needs to be verified in order to meet the requirements of those Recommendations.

24. Examples of potential reliable, independent sources of information for the verification of identity of natural persons, legal persons and arrangements include: corporate registries, registries maintained by competent authorities on the creation or licencing of respondent institutions, registries of beneficial ownership and other examples mentioned in the BCBS General Guide on Account Opening.[28]

25. Some examples of potential sources of information on level of risks include, but are not limited to: the AML/CFT laws and regulations of the home country or the host country where the respondent institution is doing business and how they apply, public databases of legal decisions and/or regulatory or enforcement actions, annual reports that have been filed with a stock exchange, country assessment reports or other information published by international bodies which measure compliance and address ML/TF risks (including the FATF, FSRBs, BCBS, IMF and World Bank), lists issued by the FATF in the context of its International Cooperation Review Group process, reputable newspapers, journals or other open source electronic media, third party databases, national or supranational risk assessments, information from the respondent institution's management and compliance officer(s) and public information from the regulator and supervisor.

26. Where the correspondent institution has identified a higher risk correspondent banking relationship, it should apply enhanced measures that are in line with the risks associated to that relationship. For example, in some circumstances, closer interaction (conference phones or face-to-face meetings) with the respondent institution's management and compliance officer(s) may be appropriate.

27. Where correspondent institutions are permitted to rely on other banks (that may already have a correspondent relationship with the respondent institution), they should ensure that a copy of the CDD information relied on will be made available upon request without delay, be satisfied they can obtain supporting documentation, be satisfied the bank being relied on is regulated and has

[26] FATF Interpretive Note to Recommendation 10, paragraph 15.

[27] FATF Recommendation 13, second paragraph.

[28] Annex 4, General Guide to Account Opening, pages 29 to 39 of the Basel Committee on Banking Supervision guidance on Sound management of risks related to money laundering and financing of terrorism (February 2016).

measures in place that are reliable.[29] The ultimate responsibility for implementing AML/CFT measures remains with the correspondent institution.

28. In all cases, the correspondent institution should obtain approval from senior management before establishing new cross-border correspondent relationships, as required by FATF Recommendation 13.[30]

V. MANAGING THE RISKS

A. ONGOING DUE DILIGENCE ON THE RESPONDENT INSTITUTION

29. Correspondent institutions are required to conduct ongoing due diligence of the correspondent banking relationship, including periodical reviews of the CDD information on the respondent institution. This is to ensure that such information is kept up-to-date in line with the risks associated with the relationship.[31] The process of managing ML/TF risk in the relationship should be ongoing, and applied to existing relationships as well as new ones. The frequency with which periodic reviews are undertaken will depend on the level of risk associated with the respondent institution. Where such reviews reveal changes in the respondent institution, the correspondent institution should consider whether it should adjust its risk assessment of the respondent institution and what further information may be needed to support this adjustment. Potential obstacles may relate to how data protection and privacy laws are applied.[32]

B. ONGOING TRANSACTION MONITORING

30. In line with Recommendation 10, ongoing monitoring of the correspondent banking account activity has to be conducted for compliance with targeted financial sanctions and to detect any changes in the respondent institution's transaction pattern or activity that may indicate unusual activity, or any potential deviations from the correspondent relationship. Depending on the risks associated with the correspondent banking relationship, various monitoring techniques and tools can be used. Correspondent institutions should put in place and periodically review risk-based procedures specifying the applicable monitoring techniques and the criteria triggering their adoption. While deciding the type and extent of the monitoring technique, correspondent institutions should take into consideration the respondent's past behaviour in the course of the correspondent relationship, in particular any failures to satisfy previous requests for information. In higher risk scenarios for example, real-time monitoring of transactions can take place to ensure that controls are effective in detecting any unusual activity that may be occurring in the account, with a view to analysing it and reporting any suspicious transactions.

[29] FATF Recommendation 17.

[30] Sub-paragraph (c).

[31] FATF Interpretive Note to Recommendation 10, paragraph 23.

[32] The FATF is currently developing best practices on information sharing (enterprise-wide, between financial institutions not part of the same group, and between public and private authorities).

C. ONGOING MONITORING AND THE INTERPLAY WITH RECOMMENDATIONS 6, 7 AND 16

31. Correspondent banking relationships should always be subject to on-going monitoring. They may also be subject to targeted monitoring depending on any unique risk factors, e.g. high suspicious activity report filing, payment flows inconsistent with stated purpose of account. The level and nature of transaction monitoring will vary, depending on the risks and the nature of the correspondent banking services being provided. For example, if the main purpose of the correspondent banking relationship is to process cross-border wire transfers[33] on behalf of the respondent institution's customers, the focus of account monitoring could be how well the respondent institution is implementing sanctions screening and its requirements under FATF Recommendations 6, 7 and 16. In such cases, particular areas of interest could include information on the respondent institution's mechanisms for screening transactions lacking required originator and beneficiary information in a manner that is consistent with straight-through processing,[34] its risk-based policies and procedures for determining how to handle such transactions, its systems for sanctions screening,[35] and its procedures and systems for clearing false positives.[36]

D. ONGOING MONITORING AND REQUEST FOR INFORMATION ABOUT TRANSACTIONS

32. Where the monitoring system of the correspondent institution flags a transaction which could signal unusual activity, the correspondent institution should have internal processes to further review the activity, which may involve requesting transaction information of the respondent institution in order to clarify the situation and possibly clear the alert. This request for additional information should be targeted on the specific transaction which created an alert in the system, and could include, depending on the risk level of the transaction, a request to access information about the customer of the respondent institution as a means to get a proper understanding of the reasonableness of the transaction. This does not amount to a requirement to conduct CDD on the customer of the respondent. In practice, the correspondent institution will follow up with the respondent institution after the transaction is completed by making a request for information on that particular transaction(s) (RFI). Subsequently, the correspondent institution should also review its control systems in order to detect similar transactions. Such questions may include some, but not necessarily all, of the following:

- Duration of customer "X" relationship with the respondent institution and whether the respondent institution classifies the customer as a high risk customer.
- Purpose of the account(s) maintained by customer "X" (business, personal, other).

[33] As defined in Recommendation 16.

[34] FATF Interpretive Note to Recommendation 16, paragraphs 17 and 18.

[35] FATF Recommendations 6 and 7 requires financial institutions to freeze the funds of persons and entities designated by, or under the authority of, the United Nations Security Council or designated by countries pursuant to resolution 1373 (2001), and prohibits financial institutions from making funds available to such designated persons and entities.

[36] This does not relieve the correspondent institution of the obligation to have procedures in place to identify the missing originator and beneficiary information.

- Details of customer's "X" parent company and the name(s) of the beneficial owner(s).
- Source of the funds of customer "X".
- Consistency between the transactional history in the account profile of customer "X", and his KYC data, or with any other information available to the bank.
- Rationale of the transaction between customers "X" and a counterparty.
- Nature of the relationship between customers "X" and a counterparty.
- Possible affiliation of customers "X" with a third-party.
- Additional details regarding the goods/services being exchanged by the customers "X"and third-parties that are not found directly in the payment details of the transaction that may explain it.
- If possible, location of customer or third-party as originator/beneficiary and/or,
- Status of the bank account of customer "X" (opened/closed).

33. Where the correspondent institution requests further information on a transaction from the respondent, it expects the respondent to respond in a timely fashion and provide documents/information to the level of detail requested. Where that does not happen, it may trigger concerns that the respondent is unable to manage its risks and lead to the filing of a suspicious transaction report by the correspondent institution. A request for information could be followed by a reassessment of the respondent's business and risk profile where/when necessary.

E. CLEAR TERMS GOVERNING THE CORRESPONDENT BANKING RELATIONSHIP

34. One way for correspondent institutions to manage their risks more effectively from the outset is to enter into a written agreement with the respondent institution before correspondent services are provided. This is consistent with FATF Recommendation 13 that requires a clear understanding of the respective responsibilities of each institution.[37] The content of the agreement should include how the correspondent institution will monitor the relationship to ascertain how effectively the respondent institution is applying CDD measures to its customers, and implementing AML/CFT controls.

35. Such an agreement could also specify the products and services to be provided under the correspondent banking relationship, the respondent institution's responsibilities concerning compliance with AML/CFT requirements, permitted third-party usage of the correspondent account and applicable internal controls to these situations, any potential restrictions that the correspondent institution may want to place on the use of the correspondent account (e.g. limiting transaction types, volumes, etc.), conditions regarding the requests for information on particular transactions, especially in the case of "payable through accounts" relationships, and cases and procedures for terminating or limiting a business relationship. Contractual details would vary depending on the circumstances including the nature of the correspondent banking relationship and the level of risk.

[37] Sub-paragraph (d).

36. Written agreements also have the advantage of documenting the intended purpose and use of correspondent banking relationships, which may have the added benefit of allowing the correspondent institution to demonstrate to its regulator some of the steps it has taken to understand the risks presented by its correspondent relationships.

F. ONGOING COMMUNICATION AND DIALOGUE

37. Correspondent banking relationships are, by their nature, based on mutual trust between the correspondent and the respondent institutions, particularly that the AML/CFT controls are being effectively implemented by the respondent institution. Consequently, it is important for correspondent institutions to maintain an ongoing and open dialogue with the respondent institution(s), including helping them understand the correspondent's AML/CFT policy and expectations, and when needed, engaging with them to improve their AML/CFT controls and processes. Such communication supports the monitoring requirement by helping to flag new and emerging risks and better understand existing ones, clear up in a timely manner any incidents that may arise during the course of the business relationship, strengthen risk mitigation measures, and resolve any issues that may arise concerning the exchange of information. This process can also assist in building the capacity of respondent institutions. It can also help to avoid unnecessary restriction on or termination of a relationship without a thorough assessment of the risks associated with the specific customer (rather than the class of customers) in line with the RBA (i.e. avoiding de-risking).[38] It can also prevent a "cascade" effect, where respondent institutions close their (highest risk) client accounts as a way to reduce their own corporate risk profile and maintain the relationships with their own correspondent institutions.

38. It is also important that regulators and supervisors maintain an open dialogue with correspondent institutions to clarify regulatory/supervisory expectations regarding the management of risks associated with foreign correspondent banking relationships.

G. ADJUSTING THE MITIGATION MEASURES TO THE EVOLUTION OF RISKS

39. As noted above, correspondent banking relationships are very diverse in nature and therefore covering a large range of high risk levels. The level and nature of risk may fluctuate over the course of any relationship and adjustments should be made in the correspondent institution's risk management strategy to reflect these changes. This is why ongoing monitoring, including periodic reviews, is important, so that the correspondent institution is aware of when the level/nature of residual risk (i.e. the risk remaining after a financial institution's AML/CFT control framework is applied to a particular situation) changes.

[38] "Regulators and supervisors should also ensure that financial institutions are taking a risk-based approach to implementing AML/CFT measures, without prejudice to rules-based measures such as targeted financial sanctions. Implementation by financial institutions should be aimed at managing (not avoiding) risks. What is not in line with the FATF standards is the wholesale cutting loose of entire countries and classes of customer, without taking into account, seriously and comprehensively, their level of money laundering and terrorist financing risk and applicable risk mitigation measures for those countries and for customers within a particular sector" (FATF Takes Action to Tackle De-risking, FATF public statement of October 2015).

40. Correspondent institutions should have policies and procedures in place tailored to the different categories of higher risk respondent relationships, and the appropriate risk mitigation required or available to retain the relationship by using enhanced due diligence. If higher risks are encountered which are not mitigated by existing enhanced due diligence, the correspondent institution should use this process to further enhance the assessment of the relationship and risk mitigation applied to the account. The objective should be to determine whether the inherent risk level is justified and if so what further, more enhanced, measures can be applied. For example, if the respondent is affected by negative news regarding its beneficial owners, the correspondent institutions could decide to limit services to such a bank.

41. The *FATF Recommendations* do require customer relationships to be terminated where identified risks cannot be managed in line with the risk-based approach.[39] However, the other options offered by Recommendation 10 should be explored prior to termination (such as refusing to conduct the transaction, and/or filing a suspicious transaction report). Alternatively, a limitation of services or restriction of individual products/transactions can be considered in order to provide the possibility for clarification or remediation by the respondent institution, before the decision to terminate activity is taken. In any event, correspondent institutions should clearly communicate their concerns to respondent institutions, at senior management level, and inform them of their concerns and the measures needed to address these concerns as a condition to maintain the correspondent banking relationship. Depending on the concerns, correspondent institutions should also consider giving notice periods to respondents, allowing them to find alternatives.

VI. ADDITIONAL GUIDANCE FOR FINANCIAL INSTITUTIONS WHICH HAVE MVTS CUSTOMERS

42. As part of their normal CDD processes, financial institutions are required to understand the purpose and nature of the intended business relationship.[40] This means that, in practice, where the customer is an MVTS provider, the financial institution should understand whether the MVTS provider intends to use the account for its own corporate or settlement purposes, or whether it intends to use the account to provide correspondent services to its own customers (i.e. the MVTS will be acting as a correspondent institution for its own customers).

43. Where the MVTS provider offers correspondent services for its own customers through its account, the correspondent institution should consider all of the factors listed above in Sections III, IV and V, on a case-by-case basis, in terms of identifying the risks, verifying information, and establishing appropriate risk mitigation measures. In particular, there is no obligation triggered by the *FATF Recommendations* to a financial institution to apply CDD measures to the customers of the MVTS.

44. To facilitate its own risk management, a correspondent institution could consider encouraging or requiring MVTS customers to open one account for conducting their own corporate or settlement activities, and another separate account for providing correspondent banking services

[39] FATF Recommendation 10, 7th paragraph.

[40] FATF Recommendation 10, paragraph 4(c).

on behalf of their customers. This procedure may facilitate effective monitoring of these two activities commensurate with the different types of risk that they present. Separate accounts may also be considered for higher risk activities or higher risk customers and nested or downstream relationships to ensure an appropriate level of transparency and effective monitoring.

45. Banks should flag unusual movements of funds and transactions conducted by their MVTS customers so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether they could be suspicious. If they are suspicious, banks should file a STR.

46. In considering the risks and appropriate risk mitigation measures, it is also important to note that MVTS providers are *financial institutions* under the *FATF Recommendations*[41] and are subject to the full range of AML/CFT preventive measures in FATF Recommendations 9 to 23 applicable to MVTS providers. Countries are also required to ensure that MVTS providers are supervised and monitored in line with FATF Recommendations 14 and 26. Correspondent institutions should take into consideration the manner in which these measures are implemented, in order to understand what their MVTS customers' obligations are and how they are supervised. Countries are also encouraged to communicate their MVTS supervisory policies and approaches to promote a shared understanding of what is expected from correspondent institutions and from MVTS with respect to risk management and mitigation processes. Given the important role that MVTS providers play in facilitating financial inclusion, banks are encouraged to work closely with their MVTS customers to ensure that they understand the banks' risk management objectives and strategies for establishing and maintaining controls to ensure effective ML/TF risk monitoring and identification. The same general processes outlined in Part V above should be considered in this regard, particularly section G.

[41] See the definition of MVTS providers in the Glossary of the *FATF Recommendations.*

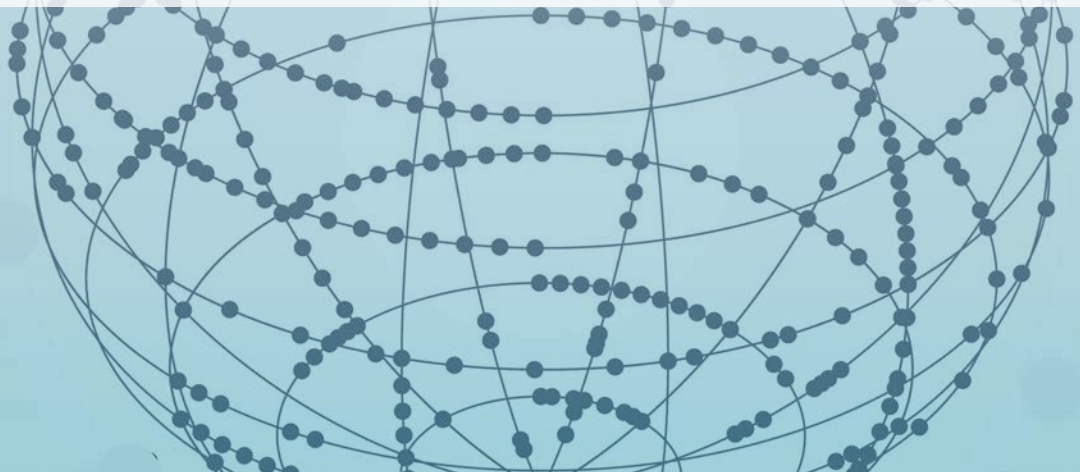
FATF

CORRESPONDENT BANKING SERVICES

This guidance explains the FATF's requirements in the context of correspondent banking services. In particular, it clarifies that the FATF Recommendations do not require correspondent financial institutions to conduct customer due diligence on each individual customer of their respondent institutions' customers. The guidance also highlights that not all correspondent banking relationships carry the same level of money laundering or terrorist financing risks, hence the enhanced due diligence measures have to be commensurate to the degree of risks identified.

The FATF developed this guidance with input from the private sector, and in collaboration with other interested international bodies, including the Financial Stability Board (FSB). The guidance should be read in conjunction with earlier FATF guidance and reports, as indicated in the guidance itself.

www.fatf-gafi.org | October 2016



Appendix JJ:

FATF, *Guidance for a Risk-Based Approach: The Banking Sector*
(Paris: FATF, 2014)

GUIDANCE FOR A RISK-BASED APPROACH

THE BANKING SECTOR

OCTOBER 2014

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BCBS	Basel Committee on Banking Supervision
BCP	Basel Core Principle
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business and Profession
FIU	Financial Intelligence Unit
INR []	Interpretive Note to Recommendation []
ML	Money Laundering
PEP	Politically Exposed Person
RBA	Risk-based approach
R. []	Recommendation []
TF	Terrorist Financing

RISK-BASED APPROACH GUIDANCE FOR THE BANKING SECTOR

This guidance paper should be read in conjunction with:

- the FATF Recommendations, especially Recommendations 1 and 26 (R. 1, R. 26) and their Interpretive Notes (INR), and the Glossary.
- other relevant FATF documents, such as the *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*, the *FATF Guidance on Politically Exposed Persons*, or the *FATF Guidance on AML/CFT and Financial Inclusion*.

INTRODUCTION

A. BACKGROUND AND CONTEXT

1. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which were adopted in 2012[1]. The FATF has reviewed its 2007 RBA guidance for the financial sector, in order to bring it in line with the new FATF requirements[2] and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version focuses on the banking sector[3], and a separate guidance will be developed for the securities sector. The FATF will also review its other RBA guidance papers, all based on the 2003 Recommendations[4].

2. The RBA guidance for the banking sector was drafted by a group of FATF members, co-led by the UK and Mexico[5]. Representatives of the private sector were associated to the work[6] and consulted on the draft revised document[7].

---

1 FATF (2012)

2 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

3 Banking activities are activities or operations described in the FATF Glossary under "Financial institutions", in particular 1., 2. and 5. The present guidance is intended for institutions providing these services.

4 Between June 2007 and October 2009, the FATF adopted a set of guidance papers on the application of the RBA for different business sectors: financial sector, real estate agents, accountants, trust and company service providers (TCSPs), dealers in precious metals and stones, casinos, legal professionals, money services businesses (MSBs) and the life insurance sector (www.fatf-gafi.org/documents/riskbasedapproach/).

5 The FATF Project group was composed of representatives from FATF members (Argentina; Australia; Austria; Belgium; Brazil; China; France; Germany; Hong Kong, China; India; Italy; Japan; Mexico; Spain; Switzerland; the Netherlands; the UK; the US), Associate members (Asia/Pacific Group on Money Laundering (APG) - through Bangladesh and Thailand and MONEYVAL - through Poland) and Observers (Basel Committee on Banking Supervision (BCBS), Organization for Security and Co-operation in Europe (OSCE), International Organisation of Securities Commissions (IOSCO), International Association of

3. The FATF adopted this updated RBA Guidance for the banking sector at its October 2014 Plenary.

B. PURPOSE OF THIS GUIDANCE

4. The purpose of this Guidance is to:

- Outline the principles involved in applying a risk-based approach to AML/CFT;
- Assist countries, competent authorities and banks in the design and implementation of a risk-based approach to AML/CFT by providing general guidelines and examples of current practice;
- Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on mitigation measures; and
- Above all, support the development of a common understanding of what the risk-based approach to AML/CFT entails.

C. TARGET AUDIENCE, STATUS AND CONTENT OF THE GUIDANCE

5. This Guidance addresses countries and their competent authorities, including banking supervisors. It also addresses practitioners in the banking sector.

6. It consists of three sections. Section I sets out the key elements of the risk-based approach and needs to be read in conjunction with Sections II and III, which provide specific guidance on the effective implementation of a RBA to banking supervisors (Section II) and banks (Section III).

7. This Guidance recognises that an effective RBA will build on, and reflect, a country's legal and regulatory approach, the nature, diversity and maturity of its banking sector and its risk profile. It sets out what countries should consider when designing and implementing a RBA; but it does not override the purview of national competent authorities. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the supervisory approach and legal framework.

Insurance Supervisors (IAIS), Group of International Finance Centre Supervisors (GIFCS), International Monetary Fund (IMF) and World Bank).

6 Amex, the Association of Development Financing Institutions in Asia and the Pacific (ADFIAP), the European Association of Co-operative Banks (EACB), the European Association of Public Banks (EAPB), the European Banking Federation (EBF), the European Banking Industry Committee (EBIC), the Latin American Banking Federation (FELABAN), the International Banking Federation (IBFed), SWIFT, the Banking Association of South Africa, the Wolfsberg Group, the Union of Arab Banks (UAB), the World Council of Credit Unions (WOCCU) and the World Savings Banks Institute/European Savings Banks Group (WSBI/ESBG) appointed representatives to the Project Group.

7 Comments were received from the Banking Association of South Africa, EBF, EBIC, EAPB, EACB, FELABAN, WOCCU, WSBI/ESBG, as well as from the International Council of Securities Association, the International Association of Money Transfer Networks, the International Consortium of Real Estate Associations, and the Russian e-money Association.

8. This guidance paper is non-binding. It draws on the experiences of countries and of the private sector and may assist competent authorities and financial institutions to effectively implement some of the Recommendations.

SECTION I – THE FATF'S RISK-BASED APPROACH (RBA) TO AML/CFT

A. WHAT IS THE RBA?

9. A RBA to AML/CFT means that countries, competent authorities and financial institutions[8], are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

10. When assessing ML/TF risk[9], countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures[10]. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CFT risks, but it is still used for ML or TF purposes.

11. A RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low[11].

B. THE RATIONALE FOR A NEW APPROACH

12. In 2012, the FATF updated its Recommendations to strengthen global safeguards and to further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime.

13. One of the most important changes was the increased emphasis on the RBA to AML/CFT, especially in relation to preventive measures and supervision. Whereas the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations consider the RBA to be an 'essential foundation' of a country's AML/CFT framework.[12] This is an over-arching requirement applicable to all relevant FATF Recommendations.

14. According to the Introduction to the 40 Recommendations, the RBA 'allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way'.

---

8 Including both physical and natural persons, see definition of "Financial institutions" in the FATF Glossary.

9 FATF (2013a), *par.* 10.

10 FATF (2013a), *par.* 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

11 Where the ML/TF risks have been assessed as low, INR 1 allows countries not to apply some of the FATF Recommendations, while INR 10 allows the application of Simplified Due Diligence measures to take into account the nature of the lower risk – see INR 1 para 6, 11 and 12 and INR 10 para 16 and 21.

12 R. 1.

15. The application of a RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Standards[13].

C. APPLICATION OF THE RISK-BASED APPROACH

16. Recommendation 1 sets out the scope of the application of the RBA. It applies in relation to:

- Who and what should be subject to a country's AML/CFT regime: in addition to the sectors and activities already included in the scope of the FATF Recommendations[14], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as an assessment that the ML/TF risks associated with those sectors or activities are low[15].
- How those subject to the AML/CFT regime should be supervised for compliance with this regime: AML/CFT supervisors should consider a bank's own risk assessment and mitigation, and acknowledge the degree of discretion allowed under the national RBA, while INR 26 further requires supervisors to themselves adopt a RBA to AML/CFT supervision; and
- How those subject to the AML/CFT regime should comply: where the ML/TF risk associated with a situation is higher, competent authorities and banks have to take enhanced measures to mitigate the higher risk. This means that the range, degree, frequency or intensity of controls conducted will be stronger. Conversely, where the ML/TF risk is lower, standard AML/CFT measures may be reduced, which means that each of the required measures has to be applied, but the degree, frequency or the intensity of the controls conducted will be lighter.[16]

---

13 The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take the risks, and the flexibility allowed by the RBA, into account when determining whether there are deficiencies in a country's AML/CFT measures, and their importance - FATF(2013b).

14 See FATF (2012) Glossary, definitions of "Financial institutions" and "Designated non-financial businesses and professions".

15 INR 1, paragraph 6.

16 R. 10; INR 10, footnote 33.

D. CHALLENGES

17. Implementing a RBA can present a number of challenges:

ALLOCATING RESPONSIBILITY UNDER A RBA

18. An effective risk-based regime builds on, and reflects, a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector, and its risk profile. Banks' identification and assessment of their own ML/TF risk should consider national risk assessments in line with Recommendation 1, and take account of the national legal and regulatory framework, including any areas of prescribed significant risk and any mitigation measures defined at legal or regulatory level. Where ML/TF risks are higher, banks should always apply enhanced due diligence, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g., varying the degree of enhanced ongoing monitoring)[17].

19. Banks may be granted flexibility in deciding on the most effective way to address other risks, including those identified in the national risk assessment or by the banks themselves. The banks' strategy to mitigate these risks has to take into account the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which banks are able to decide how to mitigate risk, countries should consider, inter alia, their banking sector's ability to effectively identify and manage ML/TF risks as well as their supervisors' expertise and resources, which should be sufficient to adequately supervise how banks manage ML/TF risks and take measures to address any failure by banks to do so. Countries may also take into account evidence from competent authorities regarding the level of compliance in the banking sector, and the sector's approach to dealing with ML/TF risk. Countries whose financial services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that banks are not equipped to effectively identify and manage ML/TF risk and any flexibility allowed under the risk-based approach should therefore be limited. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until the sector's understanding and experience is strengthened[18].

20. Institutions should not be exempted from AML/CFT supervision even where their capacity and compliance is good. However, the RBA may allow competent authorities to focus more supervisory resource on higher risk institutions.

IDENTIFYING ML/TF RISK

21. Access to accurate, timely and objective information about ML/TF risks is a prerequisite for an effective RBA. INR 1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, financial institutions and other interested parties. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share important information (i.e. due to its sensitivity) on ML/TF risks and threats, or where access to information is

17 R. 1.

18 This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or FSAP.

restricted by, for example, censorship or data protection provisions, it will be difficult for banks to correctly identify (i.e., find and list) ML/TF risk and therefore may fail to assess and mitigate it appropriately.

ASSESSING ML/TF RISK

22. Assessing ML/TF risk means that countries, competent authorities and banks have to determine how the ML/TF threats identified will affect them. They should analyse the information obtained to understand the likelihood of these risks occurring, and the impact that these would have, on the individual banks, the banking sector and possibly on the national economy for large scale, systemic financial institutions, if they did occur[19]. As a result of a risk assessment, ML/TF risks are often classified as low, medium and high, with possible combinations between the different categories (medium-high; low-medium, etc.). This classification is meant to assist understanding ML/TF risks and to help prioritise them. Assessing ML/TF risk therefore goes beyond the mere collection of quantitative and qualitative information: it forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.

23. Assessing and understanding risks means that competent authorities and banks should have skilled and trusted personnel, recruited through fit and proper tests, where appropriate. This also requires them to be technically equipped to carry out this work, which should be commensurate with the complexity of the bank's operations.

MITIGATING ML/TF RISK

24. The FATF Recommendations require that, when applying a RBA, banks, countries and competent authorities decide on the most appropriate and effective way to mitigate the ML/TF risk they have identified. This implies that they should take enhanced measures to manage and mitigate situations in which the ML/TF risk is higher; and that, correspondingly, in low risk situations, exemptions or simplified measures may be applied[20]:

- Countries looking to exempt certain institutions, sectors or activities from some of their AML/CTF obligations should assess the ML/TF risk associated with these financial institutions, activities or designated non-financial businesses and professions (DNFBPs) and be able to demonstrate that the risk is low, and that the specific conditions required for one of the exemptions of INR 1.6 are met. The complexity of the risk assessment will depend on the type of institution, sector or activity, product or services offered and the geographic scope of the activities that stands to benefit from the exemption.
- Countries and banks looking to apply simplified measures should conduct an assessment of the risks connected to the category of customers or products targeted and establish the lower level of the risks involved, and

19 Banks are not necessarily required to perform probability calculations, which may not be meaningful given the unknown volumes of illicit transactions.

20 Subject to the national legal framework providing for Simplified Due Diligence.

define the extent and the intensity of the required AML/CFT measures. Specific Recommendations set out in more detail how this general principle applies to particular requirements[21].

DEVELOPING A COMMON UNDERSTANDING OF THE RBA

25. The effectiveness of a RBA depends on a common understanding by competent authorities and banks of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, banks have to deal with the risks they identify, and it is important that competent authorities and supervisors in particular issue guidance to banks on how they expect them to meet their legal and regulatory AML/CFT obligations in a risk-sensitive way. Supporting ongoing and effective communication between competent authorities and banks is an essential prerequisite for the successful implementation of a RBA.

26. It is important that competent authorities acknowledge that in a risk-based regime, not all banks will adopt identical AML/CFT controls and that a single isolated incident of insignificant, crystallised risk may not necessarily invalidate the integrity of a bank's AML/CFT controls. On the other hand, banks should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

27. Countries and competent authorities should take account of the need for effective supervision of all entities covered by AML/CFT requirements. This will support a level playing field between all banking service providers and avoid that higher risk activities shift to institutions with insufficient or inadequate supervision.

FINANCIAL INCLUSION

28. Being financially excluded does not automatically equate to low or lower ML/TF risk; rather it is one factor in a holistic assessment. Financial exclusion can affect both individuals and businesses, and have many reasons. For individuals, this can include a poor credit rating or a customer's criminal background and institutions should not, therefore, apply simplified due diligence measures or exemptions solely on the basis that the customer is financially excluded.

29. A RBA may help foster financial inclusion, especially in the case of low-income individuals who experience difficulties in accessing the regulated financial system. When applying a RBA, countries may therefore establish specific cases for exemptions in the application of FATF Recommendations (based on proven low risks)[22], or allow financial institutions to be more flexible

---

21 For example, R. 10 on Customer Due Diligence.

22 As a general rule, CDD measures including the prohibition for financial institutions to keep anonymous accounts or accounts in obviously fictitious names, have to apply in all cases. Nevertheless, paragraphs 2 and 6 of INR 1 provide that: "*Countries may also, in strictly limited circumstances and where there is a proven low risk of ML/TF, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP*"… and "*Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided: (a) there is a proven low risk of ML and TF; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP*" (para.6). This exemption has been implemented by different countries in the interest of financial inclusion policies. See also paragraphs 56

in their application of CDD measures in case of lower ML/TF risks. In this context, financial inclusion will contribute to greater transparency and traceability of financial flows.

and 57 of the FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion on the main challenges for countries seeking to make use of the proven low risk exemption.

SECTION II – GUIDANCE FOR SUPERVISORS

30. The RBA to AML/CFT aims to develop prevention or mitigation measures which are commensurate to the ML/TF risks identified. In the case of supervision, this applies to the way supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that is conducive to the application of a risk-based approach by banks.

A. THE RISK-BASED APPROACH TO SUPERVISION

31. Recommendation 26 requires countries to subject banks to adequate AML/CFT regulation and supervision. INR 26 requires supervisors to allocate supervisory resources to areas of higher ML/TF risk, on the basis that supervisors understand the ML/TF risk in their country and have on-site and off-site access to all information relevant to determining a bank's risk profile.

Box 1. **Additional sources of information**

Report by the European Supervisory Authorities

In October 2013, the European Supervisory Authorities (European Insurance and Occupational Pensions Authority (EIOPA) for insurance and occupational pensions, European Banking Association (EBA) for banking and European Securities and Markets Authority (ESMA) for securities) published a *Preliminary report on anti-money laundering and counter financing of terrorism risk-based supervision*. This report builds on the FATF Standards and sets out what the RBA to AML/CFT supervision entails. It also lists a series of self-assessment questions supervisors may ask themselves when reviewing their approach.

BCBS Guidelines

In January 2014, the Basel Committee on Banking Supervision (BCBS) published a set of guidelines to describe how banks should include the management of risks related to money laundering and financing of terrorism within their overall risk management framework, *"Sound management of risks related to money laundering and financing of terrorism"*. These guidelines are intended to support the implementation of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation issued by the FATF in 2012. In no way should they be interpreted as modifying the FATF standards, either by strengthening or weakening them[1]. The FATF's present Guidance provides a general framework for the application of the RBA, by supervisors and the banking sector. More detailed guidelines on the implementation of the RBA by supervisors can be found in the BCBS document.

1. BCBS (2014a), par. 3.

UNDERSTANDING ML/TF RISK

32. Supervisors should understand the ML/TF risks to which the banking sector is exposed[23], and the ML/TF risks associated with individual banks and banking groups. Supervisors should draw on a variety of sources to identify and assess ML/TF risks.

33. For sectoral risks, these are likely to include, but will not be limited to, the jurisdiction's national risk assessments, domestic or international typologies and supervisory expertise, as well as Financial Intelligence Unit (FIU) feedback.

34. For individual banks, supervisors should take into account the level of inherent risk including the nature and complexity of the bank's products and services, their size, business model, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location and countries of operation. Supervisors should also look at the controls in place, including the quality of the risk management policy, the functioning of the internal oversight functions etc.

35. Some of this information can be obtained through prudential supervision. Other information, which may be relevant in the AML/CFT context, includes the fit and properness of the management and the compliance function[24]. This involves information-sharing and collaboration between prudential and AML/CFT supervisors, especially when the responsibilities belong to two separate agencies.

36. Information from the bank's other stakeholders such as other supervisors, the FIU and law enforcement agencies may also be helpful in determining the extent to which a bank is able to effectively manage the ML/TF risk to which it is exposed.

37. Supervisors should review their assessment of both the sector's and banks' ML/TF risk profile periodically and in any case when a bank's circumstances change or relevant new threats emerge.

Examples of different ways banking supervisors assess ML/TF risk in the banking sector and in individual banks can be found in Annex 1.

MITIGATING ML/TF RISK

38. The FATF Recommendations[25] require supervisors to allocate more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risk to which the sector and individual banks are exposed. It also means that where detailed supervision of all banks for AML/CFT purposes is not feasible, supervisors should give priority to the areas of higher risk, either in the individual banks or to banks operating in a particular sector.

---

23 Consistent with Basel Core Principle (BCP) 8 (BCBS, 2011).

24 As specified in BCP 5.

25 In line with BCP 9.

39. Examples of ways in which supervisors can adjust their approach include:

a) Adjusting the intensity of checks required to perform their authorisation function: supervisors can adjust the level of information they require when working to prevent criminals or their associates from holding a significant or controlling interest in a bank. For example, where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited and thus supervisors may decide to base their approval decisions on a review of relevant documentation. Where the ML/TF risk associated with the sector is high, supervisors may ask for additional information.

b) Adjusting the type of AML/CFT supervision: supervisors should always have both on-site and off-site access to all relevant risk and compliance information. However, to the extent permitted by their regime, supervisors can determine the correct mix of on-site and off-site supervision of banks. Off-site supervision alone may not be appropriate in higher risk situations.

c) Adjusting the frequency and nature of ongoing AML/CFT supervision: supervisors should adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and *ad hoc* AML/CFT supervision as issues emerge, e.g., as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from, for example, general prudential supervision or a bank's inclusion in thematic review samples.

Examples of different ways banking supervisors adjust the frequency of ML/TF supervision in line with the risks identified can be found in Annex 1.

d) Adjusting the intensity of AML/CFT supervision: supervisors should decide on the appropriate scope or level of assessment in line with the risks identified[26], with the aim of assessing the adequacy of banks' policies and procedures that are designed to prevent them from being abused[27]. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the bank's risk assessment, CDD, reporting and record keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT assessment in particular lines of business.

Examples of different ways banking supervisors adjust the intensity of ML/TF supervision in line with the risks identified can be found in Annex 1.

40. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and their AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with

26 BCP 11 considers early intervention to correct problems.

27 In line with BCP 29.

relevant confidentiality requirements, these findings should be communicated to banks to enable them to enhance their RBA.

41. In line with Recommendation 26 and the application of the Basel Core Principles relevant for AML/CFT[28], banking supervisors should consider the results of other prudential or financial supervision in their AML/CFT supervisory activities. Similarly, they should check that the broader prudential findings that drive the overall supervisory strategies of banks are informed by, and adequately address, the findings of the AML/CFT supervisory programme.

B. SUPERVISION OF THE RISK-BASED APPROACH

GENERAL APPROACH

42. It is important that supervisors discharge their functions in a way that is conducive to banks' adoption of a risk-based approach. This means that supervisors have to take steps to check that their staff are equipped to assess whether a bank's policies, procedures and controls are appropriate in view of the risks identified through the risk assessment, and its risk appetite[29]. Supervisors should make sure that the bank adheres to its own policies, procedures and controls, and that decisions are made using sound judgment. It also implies that supervisors articulate and communicate clearly their expectations of the measures needed for banks to comply with the applicable legal and regulatory framework. The aim is that supervisory actions are in most cases predictable, consistent and proportionate and to this end, training of supervisory staff and the effective communication of expectations to banks are key.

43. To support supervisors' understanding of the overall strength of measures in the banking sector, carrying out comparisons between banks' AML/CFT programmes could be considered as a means to inform their judgment of the quality of an individual bank's controls. Supervisors should, however, note that under the RBA, there may be valid reasons why banks' controls differ: supervisors should be equipped to evaluate the merits of these differences, especially when comparing banks with differing levels of operational complexity.

44. Supervisors should understand the ML/TF risks faced by the sector and by the banks. They should, in particular, have a thorough understanding of higher and lower risk lines of business, leading to a sound judgment about the proportionality and adequacy of AML/CFT controls. Supervisors should engage in a dialogue with individual banks about their views on AML/CFT controls set up by that institution.

45. The general principles outlined above in relation to domestic banks and domestic banking groups also apply to international banking groups. The application is, however, more complex as it involves legal frameworks and risks of more than one jurisdiction and also supervision by more

28 Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29, see Annex 2.

29 See also Financial Stability Board (2014).

than one national supervisory body[30]. The BCBS's "*Sound management of risks related to money laundering and financing of terrorism*" contains more information.[31]

TRAINING

46. INR 26 provides that supervisory staff in charge of the supervision of banks in their implementation of a risk-based approach should understand the degree of discretion a bank has in assessing and mitigating its ML/TF risks. In particular, supervisors should check that staff have been trained to assess the quality of a bank's ML/TF risk assessments and to consider the adequacy, proportionality and effectiveness of the bank's AML/CFT policies, procedures and internal controls in light of this risk assessment.

47. Training should allow supervisory staff to form sound judgments about the adequacy and proportionality of a bank's AML/CFT controls. It should also aim at achieving consistency in the supervisory approach conducted at national level, in case of multiple competent supervisory authorities or because of the national supervisory model.

GUIDANCE

48. Supervisors should communicate their expectations of banks' compliance with their legal and regulatory obligations[32], after considering engaging in a consultative process with relevant stakeholders. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Supervisors should also consider issuing guidance to banks on how to comply with their legal and regulatory AML/CFT obligations in a way that fosters financial inclusion.

49. Where supervisors' guidance remains high-level and principles-based, guidance written by industry sectors on how to meet the legal and regulatory obligations may be useful for explanatory and operational purposes. Banks should note, however, that the private sector guidance they take into consideration should be consistent with national legislation, based on international standards, and guidelines issued by competent authorities.

Examples of different approaches to banking supervisory guidance can be found in Annex 1.

50. Supervisors should consider liaising with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities. This is particularly important where more than one supervisor is responsible for supervision (for example, where the prudential supervisor and the AML/CFT supervisors are in different agencies, or in separate divisions of the same agency). Multiple guidance should not create opportunities for regulatory arbitrage, loopholes or unnecessary confusion among banks. When possible, relevant regulatory and supervisory authorities should consider preparing joint guidance.

---

30 General supervisory standard set out in BCPs 12 and 13.

31 Part IV. See also BCBS (2010b), and BCBS (2014a) (Consultative document) on collaboration and exchanges of information between home and host supervisors.

32 R. 34.

SECTION III – GUIDANCE FOR BANKS

51. The RBA to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. In the case of banks, this applies to the way banks allocate their compliance resources, organise their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF, including, where relevant, at group level.

52. Banking encompasses a wide range of financial products and services, which are associated with different ML/TF risks. These include, but are not limited to:

- *Retail banking*, where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products;
- *Corporate and investment banking,* where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions;
- *Investment services (or wealth management)*, where banks provide products and services to manage their customers' wealth (sometimes referred to as private banking); and
- *Correspondent services*, where banking services are provided by one bank (the "correspondent bank") to another bank (the "respondent bank")[33].

53. Banks should be mindful of those differences when assessing and mitigating the ML/TF risk to which they are exposed.

A. RISK ASSESSMENT

54. The risk assessment forms the basis of a bank's RBA. It should enable the bank to understand how, and to what extent, it is vulnerable to ML/TF. It will often result in a stylised categorisation of risk, which will help banks determine the level of AML/CFT resources necessary to mitigate that risk. It should always be properly documented, maintained and communicated to relevant personnel within the bank.

55. A bank's risk assessment need not be complex, but should be commensurate with the nature and size of the bank's business. For smaller or less complex banks, (for example where the bank's customers fall into similar categories and/or where the range of products and services the bank offers are very limited), a simple risk assessment might suffice. Conversely, where the bank's products and services are more complex, where there are multiple subsidiaries or branches offering a wide variety of products, and/or their customer base is more diverse, a more sophisticated risk assessment process will be required.

33 See FATF Glossary (FATF, 2012).

56. In identifying and assessing the ML/TF risk to which they are exposed, banks should consider a range of factors which may include:

- The nature, scale, diversity and complexity of their business;
- Their target markets;
- The number of customers already identified as high risk;
- The jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT controls and listed by FATF;
- The distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;
- The internal audit and regulatory findings;
- The volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.[34]

57. Banks should complement this information with information obtained from relevant internal and external sources, such as heads of business, relationship managers, national risk assessments, lists issued by inter-governmental international organisations and national governments, AML/CFT mutual evaluation and follow-up reports by FATF or associated assessment bodies as well as typologies. They should review their assessment periodically and in any case when their circumstances change or relevant new threats emerge.

Box 2. **Examples of ML/TF risk associated with different banking activities[1]:**

- ***Retail banking:*** provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services.
- ***Wealth management:*** culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.
- ***Investment banking:*** layering and integration, transfer of assets between parties in exchange for cash or other assets, global nature of markets.
- ***Correspondent banking:*** high value transactions, limited information about the remitter and source of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

1. The proposed categorisation of banking activities is purely indicative (see par. 52) and the list of identified risks is illustrative and non-exhaustive.

34 INR 1 and 10.

58. The risk assessment should be approved by senior management and form the basis for the development of policies and procedures to mitigate ML/TF risk, reflecting the risk appetite of the institution and stating the risk level deemed acceptable. It should be reviewed and updated on a regular basis. Policies, procedures, measures and controls to mitigate the ML/TF risks should be consistent with the risk assessment.

B. RISK MITIGATION

IDENTIFICATION, VERIFICATION AND THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP

59. Banks should develop and implement policies and procedures to mitigate the ML/TF risks they have identified through their individual risk assessment. Customer due diligence (CDD) processes should be designed to help banks understand who their customers are by requiring them to gather information on what they do and why they require banking services. The initial stages of the CDD process should be designed to help banks assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

60. Based on a holistic view of the information obtained in the context of their application of CDD measures, banks should be able to prepare a customer risk profile. This will determine the level and type of ongoing monitoring and support the bank's decision whether to enter into, continue or terminate, the business relationship. Risk profiles can apply at the individual customer level or, where groups of customers display homogenous characteristics (for example, clients with similar income range, or conducting similar types of banking transactions) can be applied to such groups. This approach is particularly relevant for retail banking customers.

61. Initial CDD comprises:

- Identifying the customer and, where applicable, the customer's beneficial owner;
- Verifying the customer's identity on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework; and
- Understanding the purpose and intended nature of the business relationship and, in higher risk situations, obtaining further information.

62. In addition, banks should take measures to comply with national and international sanctions legislation by screening the customer's and beneficial owner's names against the UN and other relevant sanctions lists.

63. As a general rule, CDD measures have to apply in all cases. The extent of these measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk, if any, associated with the individual business relationship as discussed above under *Risk Assessment*. This means that the amount and type of information obtained, and the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher. It may also be simplified where the risk associated with the business

relationship is lower. Banks therefore have to draw up, and periodically update, customer risk profiles[35], which serve to help banks apply the appropriate level of CDD.

Box 3. **Examples of Enhanced Due Diligence/Simplified Due Diligence measures (see also INR 10)**

- Enhanced Due Diligence (EDD)
  - obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment
  - carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment
  - commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity
  - verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime
  - seeking additional information from the customer about the purpose and intended nature of the business relationship
- Simplified Due Diligence (SDD)
  - obtaining less information (e.g., not requiring information on the address or the occupation of the potential client), and/or seeking less robust verification, of the customer's identity and the purpose and intended nature of the business relationship
  - postponing the verification of the customer's identity

Box 4. **CDD and financial inclusion considerations**

The application of a RBA to CDD may support financial inclusion objectives by providing for a more flexible application of CDD measures to certain categories of financial products or customers who might otherwise struggle to meet banks' CDD requirements. However, financial exclusion in itself is not an indicator of low ML/TF risk and banks have to take an informed decision, based on a holistic assessment of ML/TF risk, whether exemptions or SDD measures may be appropriate.

64. Where banks cannot apply the appropriate level of CDD, Recommendation 10 requires that banks do not enter into the business relationship or terminate the business relationship.

65. The BCBS's guidance on the *Sound management of risk related to money laundering and financing of terrorism* provides detailed guidance to banks on the management of money laundering

35 based on the bank's own risk assessment and taking into account risk factors such as those outlined in the FATF standards, e.g., in INR 10 and Recommendations/INR 12-16.

risk in correspondent banking and in situations where banks rely on third parties to carry out all, or part, of their initial CDD.

ONGOING CDD/MONITORING

66. Ongoing monitoring means the scrutiny of transactions to determine whether those transactions are consistent with the bank's knowledge of the customer and the nature and purpose of the banking product and the business relationship. Monitoring also involves identifying changes to the customer profile (for example, their behaviour, use of products and the amount of money involved), and keeping it up to date, which may require the application of new, or additional, CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious.

67. Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer's activity with that of a peer group. It need not require electronic systems, although for some types of banking activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules, verify their integrity on a regular basis and check that they address the identified ML/TF risks.

68. Banks should adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for higher risk situations, while banks may decide to reduce the frequency and intensity of monitoring where the risks are lower. The adequacy of monitoring systems and the factors leading banks to adjust the level of monitoring should be reviewed regularly for continued relevance to the bank's AML/CFT risk programme.

69. Banks should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be transparent.

Box 5. **Examples of monitoring in high/lower risk situations**

- Monitoring in high risk situations: daily transaction monitoring, manual transaction monitoring, frequent analysis of information, considering the destination of funds, establishment of red flags based on typologies reports, reporting of monitoring results to senior management etc.
- Monitoring in lower risk situations: thresholds, low frequency, automated systems

The BCBS's guidance on the *Sound management of risk related to money laundering and financing of terrorism* sets out in Section II 1 (d) what banks should consider when assessing whether their monitoring system is adequate. It stresses that a bank should have a monitoring system in place that is adequate with respect to its size, its activities and complexity as well as the risks present in the bank. For most banks, especially those which are internationally active, effective monitoring is likely to necessitate the automation of the monitoring process.

70. To this end, banks should properly document, retain and communicate to the relevant personnel the results of their monitoring as well as any queries raised and resolved.

REPORTING

71. Recommendation 20 requires countries to mandate that if a bank suspects, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, it shall report its suspicions promptly to the relevant FIU. Banks should have the ability to flag unusual movement of funds or transactions for further analysis. Banks should have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether the funds or transaction are suspicious.

72. Funds or transactions that are suspicious should be reported promptly to the FIU and in the manner specified by competent authorities. The processes banks put in place to escalate suspicions and, ultimately, report to the FIU, should reflect this. While the policies and processes leading banks to form a suspicion can be applied on a risk-sensitive basis, a bank should report once ML/TF suspicion has formed.

C. INTERNAL CONTROLS, GOVERNANCE AND MONITORING

INTERNAL CONTROLS

73. Adequate internal controls are a prerequisite for the effective implementation of policies and processes to mitigate ML/TF risk. Internal controls include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated, controls to monitor the integrity of staff, in accordance with the applicable local legislation, especially in cross-border situations and the national risk assessment, compliance and controls to test the overall effectiveness of the bank's policies and processes to identify, assess and monitor risk.

74. For larger banking groups, there should be controls in place for a consistent approach to AML/CFT controls across the group. The BCBS's *"Sound management of risk related to money laundering and financing of terrorism"* document[36] provides comprehensive guidance to banks on the effective management of ML/TF risk in a group-wide and cross-border context[37].

---

36 See part III.

37 It explains the rationale behind and principles of consolidated risk management; how group-wide AML/CFT policies and procedures should be consistently applied and supervised across the group, and, where reflecting local business considerations and the requirements of the host jurisdiction, should still be consistent with and supportive of the broader policies and procedures of the group; how banks should address differences in home/host requirements. Importantly, it also provides detail on how banks that are part of a group should share information with members of the same group with a view to informing and strengthening group-wide risk assessment and the implementation of effective group-wide AML/CFT policies and procedures.

GOVERNANCE

75. The successful implementation and effective operation of a RBA to AML/CFT depends on strong senior management leadership and oversight of the development and implementation of the RBA across the bank.

76. Senior management should consider various ways to support AML/CFT initiatives:

- promote compliance as a core value of the bank by sending a clear message that the bank will not enter into, or maintain, business relationships that are associated with excessive ML/TF risks which cannot be mitigated effectively. Senior management, together with the board, are responsible for setting up robust risk management and controls adapted to the bank's stated, sound risk-taking policy;
- implement adequate mechanisms of internal communication related to the actual or potential ML/TF risks faced by the bank. These mechanisms should link the board of directors, the AML/CFT chief officer, any relevant or specialised committee within the bank (e.g., the risks or the ethics/compliance committee)[38], the IT division and each of the business areas;
- decide on the measures needed to mitigate the ML/TF risks identified and on the extent of residual risk the bank is prepared to accept; and
- adequately resource the bank's AML/CFT unit.

Box 6. **Examples of steps taken by banks' senior management to promote compliance:**

- To carry out product development and commercial campaigns in strict compliance with national AML/CFT legislation.
- To involve senior management in AML/CFT training of staff.

77. This implies that senior management should not only know about the ML/TF risks to which the bank is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. This would require that senior management:

- receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the bank is exposed through its activities and individual business relationships;
- receives sufficient and objective information to understand whether the bank's AML/CFT controls are effective (for example information from the Chief Compliance Officer on the effectiveness of control, or audit reports);

38 BCBS(2010a), par. 52 and 53.

- and that processes are in place to escalate important decisions that directly impact the ability of the bank to address and control risks.

78. It is important that responsibility for the consistency and effectiveness of AML/CFT controls be clearly allocated to an individual of sufficient seniority within the bank to signal the importance of ML/TF risk management and compliance, and that ML/TF issues are brought to senior management's attention. This includes, but is not restricted to, the appointment of a skilled compliance officer at management level[39].

ENSURING AND MONITORING COMPLIANCE

79. A bank's internal control environment should be conducive to assuring the integrity, competence and compliance of staff with relevant policies and procedures. The measures relevant to AML/CFT controls should be consistent with the broader set of controls in place to address business, financial and operating risks generally.

VETTING, RECRUITMENT AND REMUNERATION

80. Banks should check that staff they employ have integrity and are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls.

81. The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities. Their remuneration should be in line with principles on the independence of the compliance function in the BCBS paper on principles on compliance and the compliance function in banks[40].

TRAINING AND AWARENESS

82. The effective application of AML/CFT policies and procedures depends on staff within banks understanding not only the processes they are required to follow but also the risks these processes are designed to mitigate, as well as the possible consequences of those risks. It is therefore important that bank staff receive AML/CFT training, which should be:

- Of high quality, relevant to the bank's ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls;
- Obligatory for all relevant staff;
- Tailored to particular lines of business within the bank, equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks;

39 INR 18.

40 BCBS (2005).

- Effective: training should have the desired effect, and this can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the bank's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;
- Ongoing: in line with INR 18, AML/CFT training should be regular, relevant, and not be a one-off exercise when staff are hired;
- Complemented by AML/CFT information and updates that are disseminated to relevant staff as appropriate.

83. Overall, the training should also seek to build up a working behaviour where compliance is embedded in the activities and decisions of all bank's staff.

ASSESSMENT OF CONTROLS

84. Banks should take steps to be satisfied that their AML/CFT policies and controls are adhered to and effective. To this end, their controls should be monitored on an ongoing basis by the bank's compliance officer. In addition, the adequacy of and compliance with banks' AML/CFT controls should be reviewed by an audit function.

85. Recommendation 18 requires countries to require banks to appoint a compliance officer at management level. In addition to advising relevant staff how to meet their obligations, their role should be to monitor and assess ML/TF risks across the bank as well as the adequacy and effectiveness of the measures the bank has put in place to mitigate the risks. The compliance officer should therefore have the necessary independence, authority, seniority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including across lines of business, and foreign branches and subsidiaries).

Box 7. **Examples of internal controls to encourage compliance**

- Facilitate the reporting of suspicious transactions:
  - Set up staff training on mechanisms to adequately detect unusual transactions
  - Establish adequate channels to allow staff to report unusual transactions to the Compliance Officer
  - Ensure confidentiality to staff reporting suspicious transactions
- Allow staff to report areas of policy or controls they find unclear/unhelpful/ineffective:
  - Establish ongoing consultation channels for staff concerning AML/CFT issues
  - Ensure consistency of the answers given to staff questions concerning AML/CFT issues
  - Conduct AML/CFT activities in such a way that they are perceived by all staff as a support to the quality of the banking services provided to clients and the integrity of the bank.

86. Recommendation 18 also requires countries to require banks to have an independent audit function to test the bank's AML/CFT programme with a view to establishing the effectiveness of the bank's overall AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. The findings should inform senior management's view of the design and implementation of the bank's AML/CFT framework. The audit function needs to examine the adequacy of all risk determinations and should therefore not focus exclusively on higher risks.

87. Both the compliance and audit functions should base their assessment on all information relevant to their task including, where relevant and appropriate, information obtained confidentially through relevant internal mechanisms or whistleblowing hotlines. Other sources of information can include training pass rates, compliance failures, and analysis of questions received from staff.

ANNEX 1

EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH TO THE BANKING SECTOR

This annex shares countries' supervisory practices which seek to illustrate the implementation of the RBA. They are presented as examples only. At the time of the publication of this guidance, the individual efforts had not been assessed for compliance with FATF Recommendations as part of the 4th Round of mutual evaluations. Therefore, their presentation here should not be considered as an endorsement by FATF.

Examples of different ways banking supervisors assess ML/TF risks in the banking sector and in individual banks

AUSTRALIA

Australia's AML/CFT regulator and specialist financial intelligence unit, AUSTRAC, applies a risk-based approach to the supervision of the banking sector at a corporate group level. Under this approach, AUSTRAC applies higher amounts of regulatory effort towards supervising entities within corporate groups that provide services and products identified as having a higher exposure and vulnerability to ML/TF risk.

Four factors are taken into account in determining the ML/TF risk profile:

- Whether the reporting entity group (RE Group) operates within an industry type identified as a major or significant channel for money laundering (as set out in Australia's National Threat Assessment on money laundering). RE Groups within these industry types are subject to higher levels of supervision by AUSTRAC.
- The exposure of an RE Group to ML/TF risk. Proxy measures used by AUSTRAC to determine the exposure of an RE Group to ML/TF activities are the size of the entity and/or the volume and value of transaction reports lodged with AUSTRAC. Larger RE Groups generally have more customers and typically provide products which are more complex using multiple distribution channels in multiple jurisdictions. In addition, large RE Groups have a greater impact on the overall integrity of Australia's financial system. Accordingly, large RE Groups, particularly those that lodge significant numbers of transaction reports with AUSTRAC, are subject to higher levels of supervision.

- Specific interest by AUSTRAC's Intelligence operations in relation to particular RE Groups or industry sectors.
- Specific interest by competent authorities (law enforcement, intelligence, revenue or regulatory agencies) in relation to particular RE Groups.

GERMANY

BaFin's risk classification of financial institutions is a combination of:

- The assessment of an individual abstract risk situation, based on 5 essential risk criteria (location, scope of business, product structure, customer structure and distribution structure). Each of the 5 elements is rated. The rating reached on customer structure weights more in the overall rating, as ML is a crime committed by customers. If the financial institution reaches an overall score which is the high limit for low risk institutions, or the low limit for enhanced risk institutions, the supervisor has discretion to decide which risk category the institution will fall in, based on its past AML/CFT history.
- The assessment of the quality of AML/CFT preventive measures (task fulfilment by the AML compliance officer, IT monitoring, Know-Your-Customer measures etc.) implemented by the financial institution, including the group-wide compliance aspects when relevant. The ratings are based on information from the annual audit reports and additional assessments from external auditors. The importance and scope of the deficiencies identified will impact the quality level and the rating of preventive measures.

The end result is a 12 cell-matrix, which will be used to determine the intensity of the AML/CFT supervision required:

		Quality of AML/CFT-prevention			
		A (high)	**B (medium-high)**	**C (medium-low)**	**D (low)**
Potential threat of ML/TF	**3 (high)**	**3A**	**3B**	**3C**	**3D**
	2 (medium)	**2A**	**2B**	**2C**	**2D**
	1 (low)	**1A**	**1B**	**1C**	**1D**

MEXICO

The National Banking and Securities Commission (CNBV), based on the inherent risks identified through the information obtained from financial institutions and other sources, establishes monitoring strategies. The strategy for effective monitoring takes into account which products or services are offered by financial entities, their types of users or customers, their flow of funds, and their geographic area of operation, among others. Considering those factors, CNBV determines which financial institutions represent higher risks in order to decide which financial institutions have to be visited during the year (annual program). Subsequently, a diagnosis for each entity to be visited is performed, where the major significant activities (products with inherent risk) and the correspondent risk mitigating action that the financial institutions have applied are reviewed. As a result of the inspection visit, a risk rating of the entity is determined, which at the same time provides the input necessary to determine the periodicity for further inspection visits on AML/CFT

THE NETHERLANDS

The Dutch Central Bank (DNB) is responsible for AML/CFT supervision and enforcement over banks. DNB applies a risk-based approach to AML/CFT supervision by focusing on institutions which pose the highest risk. For this, a thorough understanding of the risks is required. DNB analyses integrity risks on different levels, namely on a macro, meso and micro level. On a macro-level DNB takes into account country and global developments which are of importance for the Dutch financial sector. On a meso-level, DNB distinguishes between different sectors and the way in which different developments/risks might impact these sectors. On a micro-level DNB takes into account factors of specific institutions which can increase the vulnerability of those institutions.

The first step in the risk-based approach is to identify ML/TF risks through several sources, such as typologies, intelligence, international and national committees and other (foreign) supervisors which are involved in the prevention of ML/TF (i.e. FATF, BCBS, European Supervisory Authorities, IAIS). DNB also takes into account information received from the supervisory visits. DNB sends out a questionnaire to a group of selected institutions to gain insight in the inherent risk level and control measures in place. In addition, DNB has set up a trend analysis function which monitors open sources of information to detect new trends and signals which concern AML/CFT supervision.

When the risks are identified, DNB analyses these risks based on different criteria such as the potential impact on society, the institutions, and the stability of the financial sector. The risk profile of an institution is determined on the basis of two main dimensions, the ML/TF risk level and control level. Factors for the inherent risk score which DNB takes into account are geographical scope, the customer base of the institution, the products and services and the distribution channel of the institution. For the control level DNB look into the governance and control procedures of an institution, the adequacy of the compliance function, the compliance history and incidents and the quality of preventative measures in the institution.

SINGAPORE

The Monetary Authority of Singapore (MAS) adopts a risk-based approach in its supervision of Financial Institutions (FIs). This approach is articulated in the public monograph on MAS' *Framework for Impact and Risk Assessment of Financial Institutions*. At the heart of this framework is the impact and risk model which is used to assess FIs on two aspects annually:

- Impact (relative systemic importance): the impact assessment considers the potential impact that an FI may have on Singapore's financial system, broader economy and reputation, in the event of distress. Related institutions are grouped together for an assessment of their aggregate impact. Generally, the larger the FI's intermediary role in critical financial markets or the economy, or the greater its reach to retail customers, the higher its assessed impact.
- Risk (relative risk profile): the risk assessment examines the inherent risks of the FI's business activities, including ML/TF and proliferation financing risks, its ability to manage and control these risks, the effectiveness of its oversight and governance structure, and the adequacy of its financial resources to absorb losses and remain solvent. The assessment also takes into consideration intra-group linkages, where applicable, between the FI and its related entities, and risks posed by other entities in the group (e.g., for a locally-incorporated banking group, risks posed by significant subsidiaries will be aggregated with the main banking entity and monitored on a consolidated basis). To ensure robustness and consistency, the risk assessments of individual FIs are subjected to a process of peer comparison, challenge and review by other experienced supervisors, or panels of senior and specialist staff for key FIs.

Based on the combined assessments of impact and risk (with the impact component accorded greater weightage), the FI is assigned to one of four categories of supervisory significance, with Bucket 1 FIs supervised most intensely. FIs in Buckets 1 and 2 are supervised more closely with more resources allocated by MAS, subjected to more frequent inspections, and have their risk assessments approved by a more senior level of management.

MAS' risk-based approach encompasses both on-site and off-site supervision. MAS' off-site supervision involves ongoing monitoring of an FI's financial soundness and risk indicators, and developments in its businesses and home country, as well as trends in the financial sector. MAS also reviews the FI's regulatory returns and audit reports, and conducts regular meetings with the FI's management, auditors and home supervisors. Concerns impacting the FI's safety and soundness are followed up expeditiously.

SOUTH AFRICA

Bank Supervision Department of SARB Supervisory processes - Risk-based approach to on-site inspections

Due to limited resources, it is not practically possible to extend the scope of AML/CFT inspections to cover all areas within a bank, nor will it be possible to inspect all banks within a calendar year. Therefore, the AML Review Team, in executing its supervisory duties, has adopted a risk-based approach in scheduling and conducting AML/CFT inspections of the accountable institutions (banks) it supervises.

Risk-based methodology:

- The AML Review team will always request the bank's own AML risk assessment for purposes of inspection and review;
- As one of the contributing elements of the review of the risk assessment of a bank, a list of products and services offered by the bank, aligned with each business unit, should be requested;
- The AML Review team should assess the bank's ML risk assessment process to determine whether the bank has adequately identified the level of risk it has assumed;
- In the absence of an ML risk assessment of a particular bank, the AML Review team should perform its own risk assessment based on the structure provided by the bank and the inherent risk factors of the bank's activities;
- Should the bank's risk assessment be inadequate, the AML Review Team should complete its own risk assessment as stated above;
- The test for adequacy of the bank's risk assessment or completion of the team's own risk assessment on the bank should specifically be done for a particular inspection.
- The factors used for compiling the risk assessment should be benchmarked against the FATF Recommendations, the Basel Core Principles for Effective Banking Supervision, as well as known money laundering and terrorist financing typologies from reputable authorities.
- The banking institutions' activities, products, geographic locations and client types should be segmented between high, medium and low risk.
- Based on the risk assessment (high, medium and low risk), the AML Review Team should, thereafter, develop the scope of the inspection taking into account the identified high risk AML activities from the risk assessment.
- FATF requires countries to take appropriate steps to identify and assess money laundering and terrorist risks for the entire country on an on-going basis and in order to:
- inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and measures;
- assist in allocation and prioritisation of AML/CFT resources by competent authorities; and
- make information available for ML/TF risk assessments conducted by banks.

UNITED KINGDOM

The Financial Conduct Authority (FCA) classifies all firms according to the risk they pose to the FCA's operational and statutory objectives. It also classifies all firms that are subject to the UK's AML legislation according to their money laundering risk. This is because money laundering risk does not necessarily correlate to the size of a firm. As a result, a firm in a lower conduct risk category may receive relatively more supervisory attention from an AML/CFT perspective.

When classifying firms according to money laundering risk, the FCA considers a number of factors. These include the nature of the firm's business, the products and services it offers and the jurisdictions where it is located or operates.

This risk assessment and the criteria the FCA uses to inform it, are reviewed on a regular basis and firms can be reclassified without delay as appropriate.

UNITED STATES

The Federal Banking Agencies (FBAs) supervisory processes assess whether depository institutions have established the appropriate policies, procedures, and processes based on their BSA/AML risk to identify and report suspicious activity and that they provide sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions that are reported. To ensure consistency in the application of the BSA/AML requirements, the FBAs follow the examination procedures contained in the Federal Financial Institutions Examination Council (FFIEC)'s *Bank Secrecy Act/Anti-Money Laundering Examination Manual*. In order to effectively apply resources and ensure compliance with BSA requirements, the Manual is structured to allow examiners to tailor the BSA/AML examination scope and procedures to the specific risk profile of the depository institution. It also provides the private sector with a clear "road map" of FBA supervisory expectations and definition of the procedures that examiners will apply in evaluating compliance program effectiveness. The FBAs communicate their expectations to the private sector informally through on-going dialog with boards of directors and senior management and formally through the FFIEC BSA/AML Exam Manual, guidance and general outreach in workshops and seminars for banks based on size, location, product type and other factors and through speaking engagements sponsored by trade and industry associations. The FFIEC BSA/AML Exam Manual contains sections on identified risks associated with products and services and persons and entities that incorporate law enforcement information from reports such as the U.S. National Money Laundering Strategy and the U.S. Money Laundering Threat Assessment; on-going dialog with law enforcement representatives at the national, state and local levels and risks identified by FBA examiners based on information provided by law enforcement. This information is also used to prepare and issue guidance detailing supervisory expectations for risk management related to vulnerabilities identified in the jurisdiction and scope and plan exams.

Examples of different ways banking supervisors approach on-site and off-site ML/TF supervision in line with the risks identified

AUSTRALIA

AUSTRAC's current phase of supervision includes targeting high-risk entities for supervisory activity, and to test the effectiveness of entities' systems and controls in practice. AUSTRAC has developed data-mining techniques that scan the entire regulated entity population and bring to the surface issues and vulnerabilities that may impede reporting entities' effectiveness. Through these techniques, AUSTRAC is able to identify individual reporting entities whose behavioural characteristics are outliers to that of their peers. AUSTRAC utilises this information to identify entities requiring further supervisory engagement, particularly in lower risk sectors.

After AUSTRAC identifies ML/TF risk and significance, it determines the level and type of engagement required with an RE Group based on an assessment of its compliance risk. (Compliance risk is defined as the risk that an RE Group is non-compliant with its legislative obligations, and is a different measure to the ML/TF risk of an entity. An entity may have a high ML/TF risk but have a strong approach to its regulatory obligations, meaning that its compliance risk score will be low.)

AUSTRAC uses a range of compliance techniques to assess the adequacy of RE Groups' policies, practices, systems and controls to meet the requirements of the AML/CTF Act, including:

- Low intensity or 'engagement' activities such as enrolment processes, mail-outs, e-newsletters, forums, workshops and the development and distribution of guidance materials.
- Moderate intensity or 'heightened' activities such as processes associated with the registration of remitters, behavioural assessments, desk reviews, themed reviews and transaction monitoring directed at specific behaviours of cohorts of reporting entities.
- High intensity or 'escalated' activities such as on-site assessments and a dedicated management approach. AUSTRAC tailors these activities to individual reporting entities. They are designed to have a direct impact on improving compliance outcomes.

GERMANY

On-site inspections contain both:

- Regular annual inspections, carried-out on-site by external auditors, and
- Special/targeted inspections, on a regular basis or with respect to specific circumstances by external auditors (on behalf of the supervisor) or by the supervisor itself.

Employees of the supervisory authority accompany the external auditors in all special/targeted inspections and in some regular annual inspections.

According to the Banking Act, the supervisory authority is able to decree thematic priorities in the course of regular on-site inspections. This is done for example to check the implementation of new provisions in the AML law or when a certain type of deficiency is detected in a multitude of annual reports of different financial institutions.

Off-site supervision:

- The annual report contains an annex where the main results are highlighted in one or two brief sentences, in connection with a mark. Depending on the individual risk classification of a financial institution, in certain cases of low risk only a "quick check" of this annex is done and the whole annual report is only evaluated ("intensive check") in case of bad marks in this annex.
- After the evaluation of reports from on-site inspections and depending on their findings, the follow-up procedure will be conducted with different level of intensity.
- Detailed written information about AML measures applied to specific customer/product groups can be requested, or a consultation with the bank's compliance officer can be organised.
- The presentation of updated internal safeguards which have been put in place can be requested; depending on the importance of the system and the shortcomings that were analysed, an external expert can be mandated to check the proper operability of the system in place.

MEXICO

The AML/CFT supervision in Mexico is composed of the following stages:

- Financial institutions are assigned a risk rating using a RBA model. Information is requested periodically from financial institutions to elaborate a regulatory report and the offsite analysis is performed on the basis of this data. The information collected is consolidated in the same risk matrix used to determine the risk level of the entity. Based on these results, the CNBV determines the frequency with which a financial institution will be visited in order to supervise its compliance with AML/CFT laws and regulations; including the implementation of measures to mitigate AML/CFT risks.
- Based on the risk rating of a given financial institution, a monitoring strategy for onsite supervision is determined focusing on the higher risk factors identified at the previous stage. This is strengthened with a diagnosis that allows pinpointing significant activities (products and services) set as higher risks and the effectiveness of specific mitigants implemented by the financial institution for such activities.

- During the on-site inspections, supervisors request information and documentation in order to confirm if the risk level previously assigned to the financial institution is adequate, and conduct their inspection accordingly. Supervisors enhance their review of those aspects considered of higher risk.
- In accordance with the results of the inspections, various acts of authority can be carried out, including the issuance of observations and recommendations, as well as the implementation of corrective actions and/or sanctions.

Finally, the results of the inspection are taken into account to either confirm a risk level or assign a new one to the supervised entity. This new information is added to the offsite supervisory matrix, which helps determine the best timing for having the entity monitored again (supervision strategy).

HONG KONG, CHINA

The Hong Kong Monetary Authority (HKMA) supervises banks' AML/CFT systems through a combination of on-site examinations and off-site reviews, which is integrated as part of the broader banking supervisory process. AML/CFT supervision is risk-based, and the frequency, intensity and scope of supervisory activities are linked to the ML/TF risk profile of individual banks, which takes into account both impact to the financial system and risk level. On-site examinations comprise risk-focused examinations and thematic examinations, which are part of a cycle, culminating in best practices being provided to banks in training forums, which are conducted on an annual basis.

To illustrate the approach in practice, in 2012, the HKMA conducted thematic reviews for 9 banks over suspicious transaction reporting (STR). As a result of observations made, in Q1 and Q2 2013 a further 107 banks were subject to high-level desk-based reviews over STRs, with a focus on post-reporting risk-mitigation. On the basis of the risks identified, 26 banks were further selected for more intensive desk-based reviews, including policies and procedures and actions taken to mitigate ML/TF risks. Follow-up supervisory actions were determined on the basis of risk, including requiring additional action on the part of banks, external auditor reviews and a further 4 thematic on-site examinations that comprised interviews with key operational staff and reviews of STR related processes. The findings from this supervisory initiative were communicated to banks in training seminars held in October 2012 and April 2013, and were the subject of a guidance paper, developed in collaboration with the Joint Financial Intelligence Unit, issued on 16 December 2013.

ITALY

The Bank of Italy employs a mix of off-site and on-site supervision. Off-site analysis is systematic, carried out at set intervals, and based on analysis of data and information that banks report to the Bank of Italy (BI) (annual report of AML compliance function; reports by control bodies on specific irregularities, post inspection follow-up reports, etc.). Moreover, whenever necessary, BI holds meetings dedicated to AML issues with board members or AML compliance officers to gather relevant information and discuss initiatives.

Based on the off-site analysis results, inspections are planned and carried out. Inspections may be: full scope, targeted (business areas, specific risks, operational profiles, corrective action follow-up) and thematic. Following the entry into force of the Italian AML Law in 2008, Bank of Italy's reviewed its on-site control procedures: AML controls may be conducted in the framework of general on-site inspections or through thematic inspections dedicated to AML compliance.

In 2008, the Bank of Italy inaugurated yearly cycles of targeted on-site AML inspections on banks' branches in high risk areas in order to conduct an assessment on the implementation of AML rules in day-to-day operations. The assessment consists of short on-site visits (3/5 days) in a number of pre-selected branches located in areas of the country where specific criminal activities risks (organised crime, tax evasion, tobacco smuggling, usury, etc.) exist. Visits are conducted using a questionnaire on AML obligations (CDD, registration, reporting and training) to verify compliance with AML Law/regulations and banks' internal regulations by branch's staff; a sample testing of individual customer positions is also performed. Whenever the findings of the visits indicate major deficiencies, corrective actions are requested.

Moreover, the Italian FIU verifies compliance of financial institutions, both off-site and on-site, with regard to suspicious transactions reporting duties and cases of omitted reporting of STRs mainly on a RBA basis. The areas of risk are recognised by information transmitted by law enforcement, financial sector supervisory authorities, professional associations or other FIUs. In case of infringements or major organisational disorder at the financial institution, close coordination with Bank of Italy and other supervisory authorities is ensured by MoUs. Feedback to intermediaries, for corrective actions, is also warranted in cases detection and valuation of STRs result critical.

FRANCE

The French financial supervisor (*Autorité de Contrôle Prudentiel et de Résolution*, ACPR) implements a multi-level approach for the assessment of ML-FT risks, and the AML/CFT supervision of the financial sector:

- *Annual questionnaire on AML-CFT*: the answers to the questionnaire are systematically studied by off-site control services. Several priority levels are defined. The nature and time limit to set out corrective actions depend on the seriousness of the deficiencies revealed by the answers to the questionnaire.

  The questionnaire for credit institutions, investment firms, and life insurance institutions reflects the revised FATF Recommendations, and highlights key issues such as the RBA. It also takes account of the results of the analysis of thematic AML-CFT inspections (e.g., wealth management recently). Specific questions are added for financial groups, as well as targeted sectoral questions for the banking and insurance sectors respectively.

- *Different tools are used for the off-site control:*
  - Internal audit reports
  - On-site inspection reports

- Information collected during meetings (annual meetings, and other relevant meetings)
- Annual internal control reports, with an overview of business conducted and risks incurred by the institution; significant changes made in the internal control system; governance; money laundering and terrorist financing risks.

THE NETHERLANDS

DNB performs both on-site and off-site supervision in a risk based manner. In addition to the ongoing supervisory cycles, DNB performs thematic reviews which are in-depth reviews of a specific risk(area) for a selection of institutions. Thematic reviews allow DNB to benchmark practices, identify outliers and best practices. The process of thematic supervision starts with the selection of themes based on risk analyses, reviews from previous years or incidents/compliance issues that are known from ongoing supervision.

The entities to be visited are selected on the basis of a number of criteria, such as the size of the business, the risk profile, previous experience of compliance weaknesses etc. Prior to onsite visits, information is requested from institutions that are reviewed (such as policy and processes, transactions, suspicious transaction reports, customer information etc.). During the on-site, discussions with management, sampling of customer or transaction files as appropriate and an examination of the institution's risk assessment and risk management procedures are performed and analysed.

UNITED KINGDOM

The Financial Conduct Authority (FCA) allocates specialist supervisory resource according to the level of money laundering risk associated with a firm and *ad hoc*, as risk dictates. This involves both on-site and off-site assessments of the adequacy of firms' AML/CFT systems and controls.

Off-site assessments include the analysis of regulatory returns (which include specific financial crime questions), policies and procedures, audit reports, minutes of meetings, reports of previous supervisory visits and, where relevant, intelligence obtained through external sources.

On-site visits include interviews with key staff, testing the firm's AML/CFT controls and file reviews.

The focus and detail of both on-site and off-site reviews is determined by the reason for the review, e.g., a planned review as part of the FCA's ongoing supervisory programme or suggestions that a risk has crystallised.

Examples of differing frequency of ML/TF supervision in line with the risks identified

AUSTRALIA

The frequency of supervision by AUSTRAC correlates with the compliance risk associated with the RE Group. A key supervisory performance indicator for AUSTRAC is to undertake an assessment of

each high-risk RE Group within a three year period. In parallel, AUSTRAC employs data-mining techniques that scan the entire regulated entity population and bring to the surface issues and vulnerabilities that may impede reporting entities' effectiveness. Through these techniques, AUSTRAC is able to identify individual reporting entities whose behavioural characteristics are outliers to that of their peers. AUSTRAC utilises this information to identify entities requiring further supervisory engagement, particularly in lower-risk sectors.

GERMANY

Frequency aspects for on-site inspection are inter alia:

- Credit institutions with a total balance sheet below a specific threshold only need to be assessed on a biennial basis, except if certain risk factors indicate a higher risk.
- Special inspections are conducted more frequently with regard to "big players" in the financial market, due to the complexity of their business which requires a more frequent update of information for the supervisor.
- Special inspections can be conducted on a regular basis because of the (high) risk classification of a financial institution, regardless of its size.
- Additional or focused special inspections are sometimes conducted if serious deficiencies are evidenced by previous reports
- Special inspections can be conducted on an *ad hoc* basis in case of ML/TF related "bad news" revealed through investigations of law enforcement agencies, newspapers, whistleblowers, internet research etc.

MEXICO

The AML/CFT supervision frequency is determined by taking into account the risk ratings provided to financial institutions, as well as the following factors, among others:

- Unusual increases in the number and threshold of transactions performed by financial entities
- Increases in the STRs or CTRs, among other types of reports
- Change of a financial institution's business line profile
- New financial products or new lines of business
- The level of compliance of financial institutions with their regulatory obligations (submission of AML/CFT program to the authority, and submission of reports in a timely manner, among others).

The AML/CFT supervision frequency is also subject to the follow-up of the corrective measures, including specific plans and timelines.

THE NETHERLANDS

Based on the perceived risks DNB allocates its supervisory resources through ongoing supervision and thematic reviews. This applies to both frequency and intensity of AML/CFT supervision. In the ongoing reviews DNB assigns more resources to institutions which have a higher risk profile (based on their size, activities, compliance history etc.). In the thematic reviews a specific subject/high risk area is examined for a selection of institutions.

UNITED KINGDOM

The UK's Financial Conduct Authority (FCA) categorises firms according to their money laundering risk:

- Firms in the highest band are covered by the Systematic AML Programme. The programme operates on a four-year, rolling cycle and each programme lasts several months.
- Firms in the second band are subject to a regular on-site inspection programme consisting of two or three day on-site visits every two years.
- Firms in the lower risk banks are visited on an events-driven basis or when they are part of a sample of a thematic review.

All firms can be subject to events-driven supervision and form part of thematic reviews.

UNITED STATES

The Federal Banking Agencies (FBAs) are required by law to conduct Bank Secrecy Act (BSA) examinations of insured depository institutions as part of their overall prudential supervisory function. Such reviews are conducted during regular examinations of their depository institutions, on a 12-18 month cycle, which is required by statute (12 U.S.C. §§ 1820(d) and 1784). Supervision and regulation of depository institutions for compliance with the BSA is conducted through a combination of on-site examinations and off-site reviews. FBA BSA examination policies and procedures are established in the Federal Financial Institutions Examination Council (FFIEC)'s *Bank Secrecy Act/Anti-Money Laundering Examination Manual.* FBAs are required to conduct required core examination procedures for assessing compliance with the BSA/AML compliance program, regulatory requirements and related topics. Expanded procedures for products, services, persons and entities are required depending on risk. Transaction testing is required during each examination regardless of the level and nature of risk present in the institution. For larger, more complex institutions, some FBAs maintain resident on-site examiners who provide continuous supervision of the institution and obtain at least quarterly updates on the institution's condition and risk assessment.

Examples of adjustment of the intensity of ML/TF supervision in line with the risks identified

AUSTRALIA

As described above, AUSTRAC uses a range of compliance techniques to assess the adequacy of RE Groups' policies, practices, systems and controls to meet the requirements of the AML/CTF Act, including:

- Low intensity or 'engagement' activities such as enrolment processes, mail-outs, e-newsletters, forums, workshops and the development and distribution of guidance materials.
- Moderate intensity or 'heightened' activities such as processes associated with the registration of remitters, behavioural assessments, desk reviews, themed reviews and transaction monitoring directed at specific behaviours of cohorts of reporting entities.
- High intensity or 'escalated' activities such as on-site assessments and a dedicated management approach. AUSTRAC tailors these activities to individual reporting entities. They are designed to have a direct impact on improving compliance outcomes.

Where an entity with high inherent ML/TF risk is assessed and shown to have inadequate policies, practices, systems and controls in place to address its compliance risk, these entities are prioritised for remediation and/or enforcement action.

Remediation processes are undertaken through issuing a compliance assessment report to an entity, which requires that entity to take specific actions to remedy non-compliance in specific timeframes. AUSTRAC then monitors the entity against those requirements.

GERMANY

BaFin has set up a risk-matrix for credit institutions (see above), and the intensity of supervision follows the risk classification of each institution. The main reasons for this approach are the necessity of concentrating on the highest risk areas and the need to allocate resources where they are most needed.

Differences in the levels of supervisory intensity include:

- On-site inspections always include sample testing. If lots of deficiencies appear in a certain field (e.g., customer identification process), this could lead to a so called "full-size check" (i.e. the identification process of all new customers acquired in the past 6 months is checked)

- Escalation steps can be taken in the follow-up procedure to on-site inspections. Institutions are dealt with individually, when specific events occur.

MEXICO

CNBV applies the methodology set forth in the Institutional Manual of Supervision, which contains a detailed description of all the procedures that must be held in order to assess significant activities (products and services) of higher risk that are determined by the offsite supervisory area, as well as the effectiveness of the mitigating actions implemented by the financial institution.

During the inspections, if the supervisor in charge determines that some risk mitigating actions that are not originally covered in the corresponding supervision program should be reviewed by virtue of having evidence that there is a weakness in their implementation or effectiveness, it has the faculties to conduct a deeper and more comprehensive review. E.g., if, based on a transaction report, a deficiency is detected in the automated system of the bank, the supervisor should proceed to verify the system in order to detect the actual cause of the deficiency.

THE NETHERLANDS

DNB will allocate its supervisory resources through ongoing supervision and thematic reviews. This applies to both frequency and intensity of AML/CFT supervision. DNB's approach to supervision makes a distinction between different regimes, for example low, neutral, high and urgent. Each institution is assigned to a specific supervision regime, based on an assessment of the chance that the identified risks within an institution could harm the supervisory objectives. The risk profile of the institution forms the basis for this. The supervision regimes set the tone for the risk mitigation activities which ranges from no substantial intervention to immediate intervention where all possible measures are used to mitigate the risk.

UNITED KINGDOM

The UK's Financial Conduct Authority (FCA) categorises firms according to their money laundering risk. This categorisation determines the intensity and frequency of AML/CFT supervision.

- Firms in the highest band are covered by the Systematic AML Programme (SAMLP). These firms are subject to the most intensive AML/CFT supervision, which consists of extensive interviews with key staff, including senior management, compliance and front office both in the UK and elsewhere, as well as detailed testing of the firm's AML/CFT systems and controls. A typical SAMLP lasts several months and is repeated every four years.
- Firms in the second band will be subject to a regular inspection programme, consisting of two or three day on-site visits every two years.
- Firms in the lower bands are mainly supervised through thematic reviews and event-driven reactive supervision. Thematic reviews typically involve an off-site assessment of the firm's policies and procedures and detailed

testing and interviews during an on-site visit that lasts between two and three days, depending on the size of the firm and the complexity of its operations. The intensity of event-driven supervision depends on the nature of the suspected breach.

Examples of different approaches to supervisory guidance

AUSTRALIA

An extensive range of guidance information on Australia's AML/CTF reporting obligations is available on the AUSTRAC website (www.austrac.gov.au), including:

Guidance Notes

AUSTRAC's guidance notes contain information regarding legislative provisions to provide assistance to reporting entities in meeting their obligations. Current guidance notes can be found on the AUSTRAC website at www.austrac.gov.au/guidance_notes.html.

Guides

AUSTRAC has released the following AML/CTF Guides, which are available at www.austrac.gov.au/guides.html:

- *AML/CTF compliance guide for pubs and clubs,* to assist hotels and clubs, which are licensed to operate electronic gaming machines, to meet their requirements under the AML/CTF Act and the AML/CTF Rules.
- *AML/CTF compliance guide for independent remittance dealers*, to assist providers of remittance services to determine whether they are required to register as an independent remittance dealer and how to complete the registration process.
- *AML/CTF compliance guide for bookmakers,* to assist bookmakers in understanding and meeting their obligations under the AML/CTF Act.
- *AUSTRAC business profile form explanatory guide,* to assist entities with using the AUSTRAC business profile form.

Guidelines

The AUSTRAC guidelines contain information related to aspects of the *Financial Transaction Reports Act* and cover aspects of the reporting requirements for cash dealers. For example, the *Significant Cash Transaction Reporting Guideline for Solicitors*, available at: www.austrac.gov.au/files/guideline_no6.pdf.

Compliance Guide

The *AUSTRAC Compliance Guide* consolidates a range of AUSTRAC guidance material. The guide outlines and explains the obligations under the AML/CTF Act, Rules and regulations and presents

examples on how they operate and assists reporting entities to design, develop and implement systems and controls necessary to mitigate the risks of money laundering and terrorism financing.

The current guide is at:
www.austrac.gov.au/businesses/obligations-and-compliance/austrac-compliance-guide

CANADA

FINTRAC has published a series of guidelines to ensure that reporting entities understand and comply with their legislative and regulatory AML/CFT obligations. All of FINTRAC's guidelines can be found at the following link: www.fintrac-canafe.gc.ca/publications/guide/guide-eng.asp FINTRAC has recently issued new guidance (Guideline 4) on how to implement a compliance regime, including in respect of the risk-based approach (see www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp).

OSFI, the Office of the Superintendent of Financial Institutions, has also issued guidance to assist reporting entities that are Federally-Regulated Financial Institutions to comply with applicable AML/CFT requirements (www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b8.aspx).

ITALY

The Bank of Italy regularly provides supervised entities with general feedback on controls activities and guidance on AML/CFT risks encountered in the exercise of supervisory tasks, as well as on AML/CFT measures recommended or requested at international level (i.e. FATF black list, UN sanctions). Guidance also contains instructions on the proper procedures for fulfilling anti-money laundering obligations and compliance with the rules.

In addition, the Italian FIU, in order to ease detection of STRs, produces guidance on anomalous conduct patterns of economic or financial behaviour that may be linked to money laundering or terrorist financing (e.g., conduct patterns regarding possible loan sharking issued in 2011, on ML risk of factoring issued in 2012, on gambling and betting issued in 2013). In some cases, the Italian FIU issues "alert notes" in order to foster the awareness of financial institutions on how certain financial instruments may be exploited for ML or TF purposes (e.g., alert note on pre-paid cards in 2012). Often this kind of guidance goes along with roundtables or (in) formal meetings with ML reporting officers in order to reduce wrong interpretation regarding STRs. Such contacts are used by reporting entities for implementing an efficient RBA approach and enhance internal procedures, due to the close relationship between STRs and overall AML and CFT policies.

THE NETHERLANDS

DNB has published several guidance documents to support institutions in implementing the AML/CFT requirements. After the off-site and on-site activities, the results are benchmarked to determine outliers and good practices. Institutions receive individual feedback and potentially enforcement actions follow. The industry also gets more generalized feedback (round table, seminar, (in) formal meetings) and overviews of good practices/guidance. The sectors are kept informed of the thematic examinations through an annual publication on the themes and regular updates through newsletters.

UNITED KINGDOM

Regulatory guidance

The Financial Conduct Authority (FCA) publishes regulatory guidance on a wide range of financial crime issues. This guidance sets out the FCA's expectations of firms' financial crime system and controls. It also includes questions firms can use to test the adequacy of their systems and controls and lists examples of good and poor practice observed during on-site visits to help firms understand how they can meet their financial crime obligations.

This guidance is not binding and the FCA will not presume that a firm's departure from this guidance constitutes a breach of its rules. But firms are expected to take note of what the guidance says and use it in a proportionate and risk-sensitive way to inform their own financial crime systems and controls.

The FCA regularly updates its guidance to take account of new findings and to clarify expectations in areas where weaknesses exist across many firms. All changes are subject to public consultation before being finalised. The FCA's guidance, **Financial crime: a guide for firms** is at http://media.fshandbook.info/Handbook/FC1_FCA_20140401.pdf

Industry guidance

When assessing the adequacy of firms' AML/CFT systems and controls, the FCA also has regard to the **Joint Money Laundering Steering Group (JMLSG)'s guidance**. This is guidance written by a group of UK financial services trade associations and sets out how firms can meet their legal and regulatory AML/CFT obligations. It is formally approved by the UK Government and referred to in the FCA's rulebook and guidance. The FCA liaises closely with the JMLSG during the revision of its guidance.

UNITED STATES

The FBAs issue guidance under their own supervisory authorities and jointly with the FIU (FinCEN) to their regulated financial institutions to communicate and clarify their supervisory expectations with respect to managing ML/TF risks and complying with AML/CFT regulations. As members of the Federal Financial Institutions Examination Council (FFIEC), the FBAs have issued the *Bank Secrecy Act/Anti-Money Laundering Examination Manual* that prescribes the procedures that FBA examiners are required to apply in conducting BSA exams. The procedures contained in BSA/AML Exam Manual address compliance with both FBA supervisory expectations as well as BSA regulatory requirements and ensure transparency in the examination process. It also ensures that exam procedures are comprehensive and applied consistently across all the institutions regulated by the FBAs. The FFIEC updates the Manual regularly to incorporate changes in regulations and supervisory expectations that reflect emerging ML/TF risks and any significant changes to existing ones.

ANNEX 2

BASEL CORE PRINCIPLES DESIGNATED BY THE FATF AS BEING RELEVANT TO AML/CFT SUPERVISION (R. 26)

Basel Core Principle	Element of Supervision
Principle 1	*Responsibilities, objectives and powers:* An effective system of banking supervision has clear responsibilities and objectives for each authority involved in the supervision of banks and banking groups. A suitable legal framework for banking supervision is in place to provide each responsible authority with the necessary legal powers to authorise banks, conduct ongoing supervision, address compliance with laws and undertake timely corrective actions to address safety and soundness concerns.
Principle 2	*Independence, accountability, resourcing and legal protection for supervisors:* The supervisor possesses operational independence, transparent processes, sound governance, budgetary processes that do not undermine autonomy and adequate resources, and is accountable for the discharge of its duties and use of its resources. The legal framework for banking supervision includes legal protection for the supervisor.
Principle 3	*Cooperation and collaboration:* Laws, regulations or other arrangements provide a framework for cooperation and collaboration with relevant domestic authorities and foreign supervisors. These arrangements reflect the need to protect confidential information.
Principle 5	*Licensing criteria:* The licensing authority has the power to set criteria and reject applications for establishments that do not meet the criteria. At a minimum, the licensing process consists of an assessment of the ownership structure and governance (including the fitness and propriety of Board members and senior management) of the bank and its wider group, and its strategic and operating plan, internal controls, risk management and projected financial condition (including capital base). Where the proposed owner or parent organisation is a foreign bank, the prior consent of its home supervisor is obtained.

Basel Core Principle	Element of Supervision
Principle 6	*Transfer of significant ownership:* The supervisor has the power to review, reject and impose prudential conditions on any proposals to transfer significant ownership or controlling interests held directly or indirectly in existing banks to other parties.
Principle 7	*Major acquisitions:* The supervisor has the power to approve or reject (or recommend to the responsible authority the approval or rejection of), and impose prudential conditions on, major acquisitions or investments by a bank, against prescribed criteria, including the establishment of cross-border operations, and to determine that corporate affiliations or structures do not expose the bank to undue risks or hinder effective supervision.
Principle 8	*Supervisory approach:* An effective system of banking supervision requires the supervisor to develop and maintain a forward-looking assessment of the risk profile of individual banks and banking groups, proportionate to their systemic importance; identify, assess and address risks emanating from banks and the banking system as a whole; have a framework in place for early intervention; and have plans in place, in partnership with other relevant authorities, to take action to resolve banks in an orderly manner if they become non-viable.
Principle 9	*Supervisory techniques and tools:* The supervisor uses an appropriate range of techniques and tools to implement the supervisory approach and deploys supervisory resources on a proportionate basis, taking into account the risk profile and systemic importance of banks.
Principle 11	*Corrective and sanctioning powers of supervisors:* The supervisor acts at an early stage to address unsafe and unsound practices or activities that could pose risks to banks or to the banking system. The supervisor has at its disposal an adequate range of supervisory tools to bring about timely corrective actions. This includes the ability to revoke the banking licence or to recommend its revocation.
Principle 12	*Consolidated supervision:* An essential element of banking supervision is that the supervisor supervises the banking group on a consolidated basis, adequately monitoring and, as appropriate, applying prudential standards to all aspects of the business conducted by the banking group worldwide.

Basel Core Principle	Element of Supervision
Principle 13	*Home-host relationships:* Home and host supervisors of cross-border banking groups share information and cooperate for effective supervision of the group and group entities, and effective handling of crisis situations. Supervisors require the local operations of foreign banks to be conducted to the same standards as those required of domestic banks.
Principle 14	*Corporate governance:* The supervisor determines that banks and banking groups have robust corporate governance policies and processes covering, for example, strategic direction, group and organisational structure, control environment, responsibilities of the banks' Boards and senior management, and compensation. These policies and processes are commensurate with the risk profile and systemic importance of the bank.
Principle 15	*Risk management process:* The supervisor determines that banks have a comprehensive risk management process (including effective Board and senior management oversight) to identify, measure, evaluate, monitor, report and control or mitigate all material risks on a timely basis and to assess the adequacy of their capital and liquidity in relation to their risk profile and market and macroeconomic conditions. This extends to development and review of contingency arrangements (including robust and credible recovery plans where warranted) that take into account the specific circumstances of the bank. The risk management process is commensurate with the risk profile and systemic importance of the bank.
Principle 26	*Internal control and audit:* The supervisor determines that banks have adequate internal control frameworks to establish and maintain a properly controlled operating environment for the conduct of their business taking into account their risk profile. These include clear arrangements for delegating authority and responsibility; separation of the functions that involve committing the bank, paying away its funds, and accounting for its assets and liabilities; reconciliation of these processes; safeguarding the bank's assets; and appropriate independent internal audit and compliance functions
Principle 29	*Abuse of financial services:* The supervisor determines that banks have adequate policies and processes, including strict customer due diligence rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities.

BIBLIOGRAPHY

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations*, FATF, Paris, www.fatf-gafi.org/recommendations

FATF (2013a), *FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment*, FATF, Paris, www.fatf-gafi.org/topics/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

FATF (2013b), *FATF Methodology for assessing with the FATF Recommendations and the effectiveness of AML/CFT systems,* FATF, Paris www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

FATF (2013c), *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)*, FATF, Paris www.fatf-gafi.org/topics/fatfrecommendations/documents/peps-r12-r22.html

FATF (2013d), *Revised Guidance on AML/CFT and Financial Inclusion*, FATF, Paris www.fatf-gafi.org/topics/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html

Financial Stability Board (2014), *Guidance on supervisory interaction with financial institutions on risk culture, A Framework for Assessing Risk Culture, Basel, Switzerland,* https://www.financialstabilityboard.org/publications/140407.pdf

BCBS (2005), *Compliance and the compliance function in banks*, BIS, Basel, Switzerland, www.bis.org/publ/bcbs113.pdf

BCBS (2010a), *Principles for enhancing corporate governance,* BIS, Basel, Switzerland, www.bis.org/publ/bcbs176.pdf

BCBS (2010b), *Good Practice Principles on Supervisory Colleges*, BIS, Basel, Switzerland, www.bis.org/publ/bcbs177.pdf

BCBS (2011), *Core Principles for Effective Banking Supervision,* Basel, Switzerland, www.bis.org/publ/bcbs213.pdf

BCBS (2014a), *Sound management of risks related to money laundering and financing of terrorism*, BIS, Basel, Switzerland www.bis.org/publ/bcbs275.pdf

BCBS (2014b) *Revised Good Practice Principles on Supervisory Colleges (Consultative document),* BIS, Basel, *Switzerland,* https://www.bis.org/publ/bcbs276.pdf

ESMA, EBA, EIOPA and Joint Committee of the European Supervisory authorities (2013), *Preliminary report on anti-money laundering and counter financing of terrorism Risk Based Supervision,* www.eba.europa.eu/documents/10180/16145/JC-2013-72+%28Report+on+Risk+Based+Supervision%29.pdf

FATF REPORT

Financial Flows from Human Trafficking

July 2018

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The Asia/Pacific Group on Money Laundering is an inter-governmental organisation, consisting of 41 member jurisdictions, focused on ensuring that its members effectively implement the international standards against money laundering, terrorist financing and proliferation financing related to weapons of mass destruction.

Citing reference:

FATF - APG (2018), *Financial Flows from Human Trafficking,* FATF, Paris, France, www.fatf-gafi.org/publications/methodandtrends/documents/human-trafficking.html

Table of Contents

ACRONYMS

AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorists
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSRB	FATF-style regional body
HTFL	Human Trafficking for the purpose of forced labour or services, slavery or practices similar to slavery, and servitude
HTRO	Human Trafficking for the purpose of removal of organs
HTSE	Human trafficking for the purpose the exploitation of the prostitution of others or other forms of sexual exploitation
ILO	International Labour Organisation
ISIL	Islamic State of Iraq and the Levant
ML	Money Laundering
NPO	Non-profit organisation
NRA	National Risk Assessment
Reporting entities	Private entities with obligations in a jurisdiction's AML/CFT regime
RTMG	FATF's Risks, Trends and Methods Group
STR	Suspicious Transaction Report
TF	Terrorist Financing
The previous FATF report	FATF's 2011 report, Money Laundering Risks Arising from Trafficking in Human Beings and the Smuggling of Migrants
UNODC	United Nations Office on Drugs and Crime

Executive Summary

1. In addition to its enormous human cost, human trafficking is estimated to be one of the most profitable proceeds generating crime in the world, with the International Labour Organisation estimating that forced labour generates USD 150.2 billion per year. While in the past, many aspects of the crime went 'unseen', there is now an increased understanding of the breadth and gravity of human trafficking, particularly with respect to domestic human trafficking and human trafficking for labour exploitation. Human trafficking is also one of the fastest growing forms of international crime. The increased displacement and vulnerability of people in, and around, conflict zones increases instances of human trafficking, including potential involvement by opportunistic terrorist organisations.

2. As we learn more about the way human traffickers operate and exploit vulnerable humans, it is clear that this phenomenon affects nearly every country in the world. The Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering (APG) jointly undertook this study to improve global understanding of the financial flows associated with the crime of human trafficking, both as a money laundering predicate and potential source of terrorist financing. This study updates the FATF's 2011 report. This study has brought granularity to indicators of suspected money laundering of the proceeds of human trafficking by separating human trafficking into three categories in line with the *Palermo Protocol:* human trafficking for forced labour, sexual exploitation or for the removal of organs.

3. The project team found that the proceeds from each of these types of exploitation are realised in a different manner, and required different laundering mechanisms. In addition, each of these three types of exploitation could be better understood and detected through the financial activities of the various actors and/or roles involved to conduct each of the three types of exploitation. Further segmentation based on roles and actors provided a second opportunity to develop a more detailed understanding of the offence. The report also provides a more precise set of global money laundering indicators for use by reporting entities, financial intelligence units and other national authorities.

4. This study also identifies the challenges national authorities frequently face in detecting, investigating and prosecuting money laundering and terrorist financing from human trafficking. The study identifies good practices, and in particular the two primary good practices, to mitigate some of these challenges:

- **Assess the diverse money laundering risks from human trafficking, share with stakeholders and ensure that they're understood**
- **Leverage expertise, capabilities and information through partnerships between the public sector, private sector, civil society and NPO communities.**

5. This study updates the FATF Global Network's understanding of the financial flows from human trafficking, and provides tangible indicators and best practices for national authorities to improve their effectiveness in combatting money laundering and terrorist financing from human trafficking (see Annex B). While our

understanding is improved, it is by no means complete. This study therefore concludes with practical next steps to develop further precision to the financial flows from human trafficking, both at the global level, and at the regional/national level.

Introduction

The previous report and this report

6. In July 2011, FATF published a report titled, *Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants*, which studied the nature and scale of the human trafficking and migrant smuggling problem by looking at: countries of origin, transit and destination, operational responsibilities, challenges, and identified trends, typologies and risk indicators.

7. Since the publication of the 2011 report, global awareness of human trafficking has increased and different countries and international organisations have worked to better understand and address human trafficking. Whilst progress has been made in understanding the scale of the problem, the FATF has not updated its research on financial flows related to human trafficking nor money laundering and terrorist financing associated to human trafficking. This study updates the FATF's knowledge on the topic.

Scope

8. This report aims to provide an updated and more precise understanding of the financial flows related to human trafficking, and the various components of human trafficking that this report will identify, building on the wide body of work which has been completed since the last FATF report on the topic. It is designed to be used by FATF members, national authorities, financial institutions, non-government organisations and any other individuals or bodies with an interest in tackling the financial flows related to human trafficking.

9. For the purposes of this report, human trafficking is defined with reference to the types of exploitation set out in in the *Palermo Protocol*.

Box 1. Human Trafficking Definition from the *Palermo Protocol*

The definition utilised for the term 'human trafficking' is the definition provided in the *The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children*, supplementing the *United Nations Convention against Transnational Organised Crime*. This protocol entered into force on 25 December 2003 and 173 jurisdictions have ratified or acceded to it as of January 2018.

The Protocol defines human trafficking as:

"the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs".

Source: UN (2003)

10. The report deliberately does not cover migrant smuggling[1] (also known as people smuggling). This is because of the three fundamental differences between human trafficking and migrant smuggling:

- **Consent:** The smuggling of migrants - while often undertaken in dangerous or degrading conditions - involves migrants who have consented to their smuggling. Victims of human trafficking, on the other hand, have either never consented or, if they initially consented, that consent has been rendered meaningless by the coercive, deceptive or abusive actions of the traffickers.
- **Exploitation:** Smuggling ends with the arrival of the migrants at their destination, whereas trafficking involves the ongoing exploitation of the victims in some manner to generate illicit profits for the traffickers.
- **Trans-nationality:** Smuggling is always transnational, whereas trafficking need not be. Trafficking can occur regardless of whether victims are taken to another country or subjected to human trafficking in the same country where they reside, even if no movement has taken place.

11. As a result of these differences, the financial flows for human trafficking and migrant smuggling are different, and are best profiled independent of one another to differentiate the two and develop a view of each of the offences. Thus, this study updates the previous report's findings with respect to human trafficking; however, the previous report's findings on migrant smuggling stand.

Objectives and structure

12. The report is designed to provide practitioners with an updated view of the scope and scale of the human trafficking problem globally, and the estimated proceeds from this offence. In addition, this report provides updated, more granular indicators of financial transactions suspected of laundering the proceeds of human trafficking. The report identifies challenges and good practices in detecting, investigating and prosecuting money laundering from human trafficking. These objectives are delivered through three parts:

- **Part One**: Provides an overview of recent developments in the nature/scope of human trafficking, including the financial flows, proceeds derived from human trafficking and the potential of human trafficking to contribute to the financing of terrorist activity.
- **Part Two**: On the basis of case study and literature analysis, this section provides context to the laundering of the proceeds of human trafficking, and develops and delivers more precise money laundering indicators to aid in the detection of transactions which may be indicative of the laundering of the proceeds of human trafficking. To provide further granularity, the indicators

[1] The definition of "smuggling of migrants" for the purposes of this study is the one enunciated in Article 3 (a) of the Protocol against the smuggling of migrants by land, sea and air, which states: "Smuggling of migrants" shall mean the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident.

are grouped by how the perpetrators benefit, the roles and/or actors required to commit the offence, and the types of the offence.

- **Part Three**: Highlights challenges in detecting, investigating and prosecuting human trafficking, and offers good practices in overcoming some of these challenges.

Methodology

13. The Financial Action Task Force (FATF) and the Asia Pacific Group on Money Laundering (APG) jointly oversaw the project, which was co-led by delegations from Canada, Indonesia and the United Kingdom. Delegations from Australia, Belgium, British West Indies, India, Italy, New Zealand, Norway, Portugal, Somalia, South Africa, Spain, Sweden, Russian Federation, Ukraine, and United States participated in the project. Also participating in the project team were: European Union Agency for Law Enforcement Cooperation (Europol), International Criminal Police Organization (Interpol), Inter Governmental Action Group against Money Laundering in West Africa (GIABA), Liechtenstein FIU, MONEYVAL, Organisation for Economic Co-operation and Development (OECD), the United Nations Office on Drugs and Crime (UNODC), the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the Egmont Group of FIUs.

14. The methodology consisted of a review and refinement of existing material on human trafficking. This comprised of:

- A literature review conducted by FATF TREIN to identify recent developments in the nature/scope of human trafficking, and the financial flows associated with human trafficking.
- A request to FATF members and associated delegations to provide relevant material to the project team. This included material on risk (e.g. risk indicators, strategic analysis of suspicious transaction reports or other data, relevant information from national risk assessments) and on actions taken to mitigate the risk (partnerships with the private sector, examples of particular law enforcement operations, and access to different data sets). The project team was particularly interested in the use of case studies that highlighted schemes or trends associated with human trafficking.
- Workshops co-chaired by the co-leads on the financial flows related to human trafficking hosted by the APG and FATF TREIN in the Republic of Korea and MENAFATF/ESAAMLG/GABAC/GIABA in Morocco. Thanks to the numerous cases furnished by the jurisdictions and the presentations made by their representatives in the workshop, the project team gathered substantive material for the purpose of this report. Many members of the project team also provided valuable additional contributions at these typologies meetings.
- Working with financial institutions and NGOs to develop a set of updated risk indicators associated with human trafficking. The work of Standard Chartered Bank, Citibank, Barclays Bank, the Bank of Montreal, HSBC, Western Union, Wolfsberg Group, Banks Alliance Against Human Trafficking (convened by the Thomson-Reuters Foundation), Liberty Asia, Stop the

Traffik, RUSI and the Global Initiative on Transnational Organized Crime helped the project team develop such a precise set of indicators.

Part One: Overview of the scale and scope of human trafficking

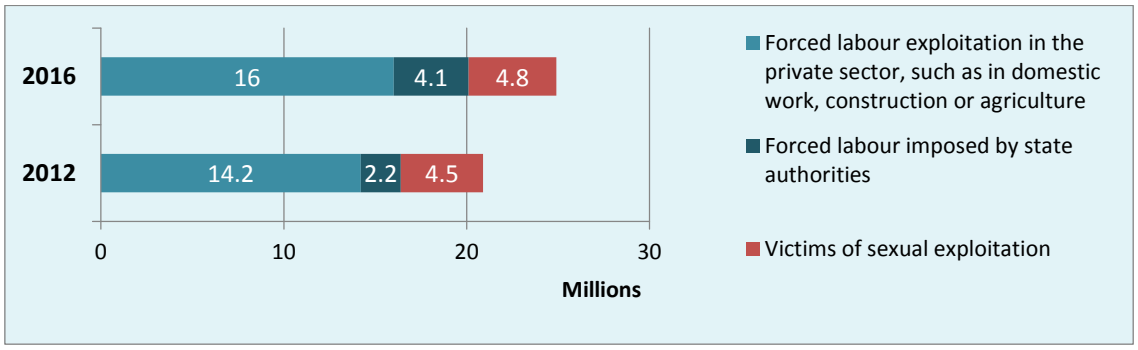
Global estimates

It is challenging to estimate the scale of human trafficking, largely due to the hidden nature of some types of the human trafficking crime and difficulties in identifying victims. There are, however, global estimates on various exploitation types of the internationally recognised definition of human trafficking, which, when aggregated, can provide an estimate of the scale and scope of human trafficking.

15. In September 2017, the International Labour Organisation (ILO) and Walk Free Foundation, in partnership with the International Organisation for Migration, published *The Global Estimates of Modern Slavery*. The report indicates that an estimated **24.9 million**[2] people were in forced labour and sexual exploitation at any moment in time in 2016. Out of the total estimate of 24.9 million:

- 16 million people (64%) were estimated to be in forced labour exploitation in the private sector such as in domestic work, construction or agriculture (compared with 14.2 million in the 2012 ILO estimate)
- 4.1 million people (17%) were estimated to be in forced labour imposed by state authorities[3] (compared with 2.2 million in the 2012 ILO estimate)
- 4.8 million people (19%) were estimated to be subject to sexual exploitation[4] (compared with 4.5 million in the 2012 ILO estimate).

Figure 1. Number of people victim of forced labour or sexual exploitation (2012-2016)



Source: ILO & Walk Free Foundation, 2017 and ILO, 2012.

[2] India has expressed concerns with the methodology used to determine, and the accuracy of, the estimates presented in the ILO/IOM/Walk Free Foundation Global Estimates of Modern Slavery report.

[3] State-imposed forced labour includes forced labour exacted by the military, compulsory participation in public works, and forced prison labour.

[4] This includes 3.8 million adults in forced sexual exploitation and 1.0 million children in commercial sexual exploitation. Where the victim is a child, there is no requirement of any of the means of the trafficking in persons' definition to occur for the child being exploited.

16. There is no such estimate for human trafficking for the removal of organs. In 2007, the World Health Organisation estimated that between 5 and 10 percent of all organ transplants conducted worldwide were conducted 'illegally', which could comprise human trafficking for the purpose of removal of organs, as well as other crimes.[5] Accordingly, there is no such estimate for the number of people affected by human trafficking for the purpose of the removal of organs.

Profile of victims

17. The UNODC's 2016 *Global Report on Trafficking in Persons* study found that in 2014, 28% of detected victims in human trafficking were children and 71% of the detected victims were female. The proportion of men and boys among the detected victims has, however, grown from 16% in 2004 to 29% in 2014. The majority of the male victims (85.7%) were trafficked for forced labour exploitation. For female victims, 72% were trafficked for the purpose of sexual exploitation.

Geographical routes and trafficking flows

18. The geographical human trafficking routes are complex. The previous FATF report considered these routes and found that it affects virtually all countries around the globe. The report considered countries of origin, transit countries and countries of destination.

19. However, the collective understanding of human trafficking has evolved since the time of the previous FATF report. The UNODC *Global Report on Trafficking in Persons 2016* identified more than 500 different trafficking flows, including both domestic and transnational human trafficking. Accordingly, this report takes a modernised approach and considers domestic, regional and trans-regional trafficking flows.

Domestic human trafficking flows

20. Domestic trafficking involves the movement of victims within a country between areas, or within their local area. Where there is movement of victims domestically, this commonly occurs from rural zones to cities or tourist centres, or from villages to industrial or economic hubs[6]

21. Studies show that the majority of forced labourers in economic activities, and almost all those in state-imposed forced labour, have not moved away from their home area. The UNODC found that 43% of victims in the period 2012-2014 were trafficked domestically.[7] The *2017 Global Estimates of Modern Slavery* found that only one in four victims of forced labour were exploited outside their country of residence.[8]

[5] Shimazono, Y., 2007.

[6] UNODC, 2016: p. 40.

[7] *Ibid*.

[8] ILO & Walk Free Foundation, 2017: p.29.

Trafficking within regions

22. Transnational trafficking flows are increasingly complex – victims are exploited within and between regions. While many countries are source and destination countries, most countries tend to be either predominantly a source or predominantly a destination of trafficking victims.[9] The UNODC found most victims detected were trafficked within the same geographical region.[10] For the majority of detected victims of transnational trafficking identified in the UNODC's study, the origin country was in the same geographical region as the destination, which includes domestic trafficking.[11]

23. Common regional trafficking flows include victims trafficked from South-Eastern Europe to Western Europe, from the Andean countries to the Southern Cone in South America, from East Asia to the Pacific, or victims trafficked across a single international border into neighbouring countries.[12]

Trans-regional trafficking

24. In trans-regional trafficking, countries with developed economies remain key destinations, while victims tend to originate from countries with less developed economies. The UNODC found that the Middle East, as well as most countries in Western and Southern Europe and North America, reported being destinations for trans-regional and long-distance trafficking.[13] In particular, they found that the wealthier the country of destination, the greater the number of detected victims from outside the immediate region.

25. In Western and Southern Europe, detected victims held 137 different citizenships, particularly from Central and South-Eastern Europe (47%), Sub-Saharan Africa (16%) and East Asia (7%).[14] Similarly, North American countries detected victims from more than 90 countries of origin. The most prominent trans-regional trafficking flow in the study was from East Asia, as 16% of the detected victims in North America are citizens of East-Asian countries.[15] Trafficking victims from countries in Sub-Saharan Africa and East Asia are trafficked to the widest range of destinations. The UNODC found that 69 countries reported to have detected victims from Sub-Saharan Africa between 2012 and 2014.[16]

[9] *Ibid*.

[10] *Ibid*: p. 41

[11] *Ibid*.

[12] *Ibid*.

[13] *Ibid*: p. 42

[14] *Ibid*: p. 43

[15] *Ibid*.

[16] *Ibid*: p. 5

Human trafficking, irregular migration and conflict

26. The number of persons vulnerable to trafficking in recent years has increased due to an unprecedented rise in irregular migration[17] and the number of displaced persons, often caused by armed conflict or terrorist organisations controlling territory, who are predominantly fleeing the events in an outward direction from the location of the conflict zone. Trafficking flows related to armed conflict can include human trafficking within and into conflict-affected areas for the purposes of sexual exploitation and forced labour,[18] as well as transnational trafficking flows linked to migrant smuggling.[19]

27. There is evidence that criminal networks involved in trafficking in human beings target the most vulnerable, in particular women and children.[20] On irregular migration routes around the globe, migrants who have started out their journeys by willingly placing themselves in the hands of smugglers have become victims of human trafficking along the way.[21] A report by the International Migration Organisation and UNICEF found that children and youth along irregular migration routes are especially vulnerable to trafficking because of their age and status.[22]

28. Once these migrants reach their destination, they remain vulnerable to human trafficking and other forms of exploitation.[23] Migrant workers, in particular irregular migrants, are vulnerable to exploitation due to their economic conditions, language barriers and challenges of social integration.[24]

29. Irregular migration is a macro factor that has changed human trafficking globally. These links between irregular migration and human trafficking are increasing further, particularly with respect to cases of labour exploitation in the countries of destination of the migrants.[25] Moreover, terrorist groups will continue to use human trafficking within and into conflict-affected areas to generate revenue.

Change in the scale and scope of human trafficking

30. The methodologies for determining human trafficking estimates have changed over time, making these figures unsuitable for a direct comparison. They do, however, demonstrate that with our improved understanding of the issue, the estimated scale has increased.

[17] For the purposes of this study, "irregular migration" is meant to denote the movement of people precipitated by events or conditions such as war or drought.

[18] UN University (2016) p. 6

[19] UNODC, 2016: p. 57

[20] European Commission (2016) p. 9

[21] IOM (2017) p. 3

[22] IOM & UNICEF (2017) p. 21

[23] IOM (2017) p.3

[24] ILO & Walk Free Foundation (2017) p. 30

[25] Europol & Interpol (2016) p. 11

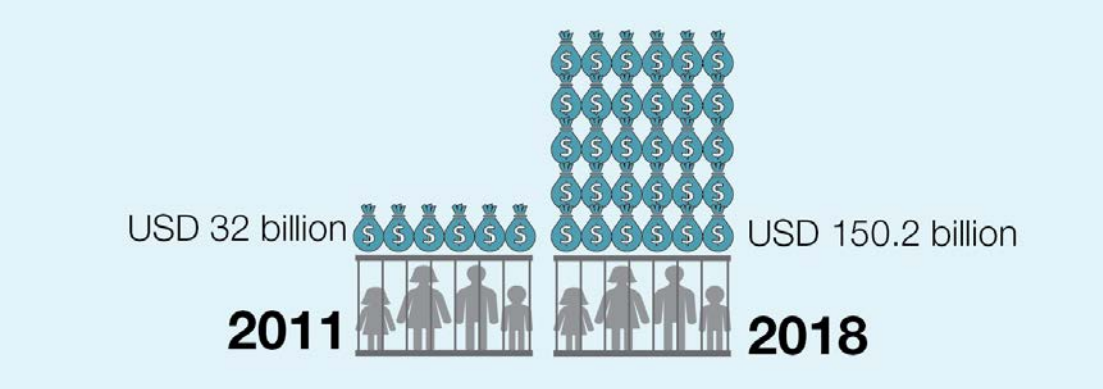
It is unknown how much of this apparent increase is due to a worsening of the issue of human trafficking, or if it is due to an improved awareness in the issue.

31. Since the publication of the previous FATF report, the global community has developed a more precise understanding of human trafficking flows. Demonstrated by findings such as UNODC's identification of 500 different trafficking flows between 2012 and 2014, as well as more information on the profiles of victims and offenders and on the forms of human trafficking. In addition, the international community has further defined and demonstrated the significance of trafficking within jurisdictional borders, and differentiated domestic, regional inter- and intra-trans-regional trafficking.

32. As a result of this apparent increase in the occurrence of human trafficking, the global community's more detailed understanding of the crime, and the macro factor of irregular migration, the global AML/CFT community is, accordingly, responding by updating its understanding of the financial flows from human trafficking, and identifying more granular ways to identify the laundering of these proceeds.

Proceeds derived from human trafficking

Figure 2. Estimated proceeds from Human trafficking



Source: ILO (2014)

33. As a result of the diversity of trafficking and exploitative crimes that produce illicit profits, it is difficult to establish an accurate aggregate figure of the total illicit proceeds from human trafficking. With certain caveats,[26] the ILO estimated that the total illicit proceeds obtained from the use of forced labour, which is inclusive of sexual exploitation, amount to USD 150.2 billion per year based on its 2012 forced labour estimates, published in 2014. This number can be broken down as follows:

- Forced sexual exploitation: USD 99 billion

[26] ILO (2014) p. 13. The estimate is the aggregation of regional profit figures for three forms of forced labour: forced labour exploitation outside of domestic work, forced domestic work and forced sexual exploitation. The estimate does not take into account the profits generated by the 2012 ILO estimate of 2.2 million victims of forced labour imposed by state authorities, nor does it account for the proceeds generated from human trafficking for the purposes of the removal of organs.

- Forced labour exploitation: USD 51.2 billion, of which USD 43.40 billion was generated by non-domestic labour, and USD 7.9 billion by domestic work

34. ILO's estimates of the global average profit per victim of human trafficking varied significantly based on the type of exploitation, ranging from USD 21 800 annually for sexual exploitation and USD 2 300 annually for domestic work. In 2005, the ILO estimated that the annual profits for each forced labourer were USD 13 000 on average. The 2014 figures do not set out a similar average estimate for all forced labourers.

35. According to the ILO, the annual total profits are highest in Asia (USD 51.8 billion) and developed economies (USD 46.9 billion). This is due to the high number of victims in Asia, and the high profit per victim in developed economies.

36. There is no accepted estimated figure for the amount of proceeds from human trafficking for the removal of organs. Figures for the illicit organ trafficking market combine human trafficking with other crimes. These figures place the financial scale at USD 1.2 billion or less, with Global Financial Integrity's[27] estimate of USD 600 million – 1.2 billion being the highest. While these are staggering numbers, even the highest estimate inclusive of other organ-related crimes would represents less than 1% of the combined figure for the other two exploitation groupings. Given that there is no generally accepted estimate, no attribution for the proceeds of human trafficking for the removal of organs will be used for this report; however, even an accepted estimate would not be anticipated to change the final figure in a material way. However, the lack of such an estimate represents a gap in the understanding of the proceeds from human trafficking.

37. The preceding proceeds figures demonstrate that the estimated proceeds from human trafficking in aggregation is approximately USD 150.2 billion, versus the USD 32 billion figure provided in the previous FATF report, which makes it the one of the most significant generators of criminal proceeds in the world. The United Nation's completed *Global Initiative to Fight Human Trafficking*[28] project also indicated that human trafficking is the fastest growing form of international crime.

Terrorist financing from the proceeds of crime derived from human trafficking

38. FATF reports, UN Security Council Resolutions[29] and Reports of the Secretary-General on the threat posed by ISIL (Da'esh) to International Peace and Security,[30] as well as jurisdictions and news media listed below, have highlighted the link between human trafficking and terrorist organisations. Trafficking flows related

[27] Haken, J., 2011.

[28] United Nations Global Initiative to Fight Human Trafficking is an initiative comprised of the International Labour Organisation, the Office of the United Nations High Commissioner for Human Rights, the United Nations Children's Fund, the United Nations Office on Drugs and Crime, the International Organisation for Migration and the Organisation for Security and Cooperation in Europe.

[29] UNSCRs 2331 (2016) and 2388 (2017)

[30] S/2016/92, S/2016/501, S/2017/97, S/2017/467 and S/2018/80

to armed conflict can include human trafficking within and into conflict-affected areas for the purposes of domestic servitude, sexual slavery, forced recruitment, forced labour and forced marriage.

39. These reports also indicate that terrorist organisations who have controlled, or partially controlled territory, have used human trafficking as a way to raise funds and support to their organisations and activities:

- **ISIL:** The UN reported that Yazidi women were being bought and sold by ISIL fighters in 'slave auctions', including via the internet.[31] The 2015 FATF report on ISIL financing noted that the prices paid for ISIL slaves were low (approximately USD 13 each), and have been reported to be transferred between ISIL fighters as commodities. The UN Human Rights Council has stated that some Yazidi women and girls were aware of the amounts paid for them, which ranged between USD 200 and USD 1 500, depending on marital status, age, number of children, and perceived beauty. There were also media reports of payments being made to intermediaries to free Yazidi women from captivity.[32] The UN reports that in January 2016, ISIL received USD 850 000 in payments from Yazidi families for the return of 200 kidnapping victims, and that estimates suggested that in 2014 ISIL earned between USD 35 million to USD 45 million in payments from the Yazidi community.[33] The US State Department has found that in Syria, ISIL used displaced children as forced labour in organised begging rings.[34]
- **Boko Haram:** The UN has noted that Boko Haram uses children as beggars to raise funds.[35] It found that Boko Haram has kidnapped thousands of women and girls to date and some of these women have been subjected to domestic servitude, forced labour, and sex slavery through forced marriages to its militants.
- **Al-Shabaab:** Based on interviews with victims, the Somali Financial Intelligence Unit (FIU) suspects that Al-Shabaab members have been involved in the trafficking of Somalis for profit. The accounts of two victims highlighted that this has occurred both from rural to urban areas within Somalia, and from Somalia to other countries. Typically, women have been promised work opportunities but their salaries have been paid directly to the Al-Shabaab. It is not clear if this has occurred in an organised fashion to raise funds for the group or if the trafficking is for the personal benefit of individual terrorists.

40. There have also been many accounts of numerous terrorist organisations profiting from the exploitation of vulnerable persons in their areas of control, including by forcing young men and boys to fight for the terrorist organisation.

[31] United Nations Human Rights Council, 2016.

[32] White, L., 2015 and Paraszczuk, J., 2015.

[33] United Nations University, 2016.

[34] US Department of State, 2015.

[35] UN University, 2016: p. 8

Fewer reports exist of terrorist organisations profiting off of the facilitation or allowance of human trafficking networks within their territory; however, such a link may be present given the well-reported proclivity of territory-controlling terrorist organisations to tax all activity occurring within their borders.

41. While there are indications that human trafficking may be a source of income for terrorist groups, particularly those that control territory, this appears not to be a key source of revenue for terrorist groups, especially considering the erosion of the territory held by terrorist groups. However, human trafficking is likely used as a tool to exploit and control vulnerable local populations, as a perceived benefit for fighters in conflict, and as an occasion to secure ransom payments. The involvement of terrorists in human trafficking is likely opportunistic and could be for the benefit of individual terrorists or for the terrorist organisation at large.

Links between human trafficking, migrant smuggling and kidnap for ransom

42. Terrorist organisations influence trafficking flows by engaging in armed conflict which causes mass migration and increases the number of displaced persons, thereby increasing the number of persons vulnerable to human trafficking. These individuals may be more susceptible to seeking the services of migrant smuggling networks, or be vulnerable to exploitation through human trafficking networks, which can utilise similar infrastructure or channels.

43. Several jurisdictions have noted that migrant smuggling due to conflict may turn into a human trafficking scenario, particularly if the victim is kept in debt-bondage until the fees for migrant smuggling operation are paid. Similarly, migrant smuggling or human trafficking scenarios can turn into a kidnap for ransom scenario if ransom is demanded from the family members to free the individual. It is not always clear if these payments are for the benefit of terrorist organisations that have territorial control. In one situation, a family member was asked to use a certain money service business provider to make the ransom payment.[36] This suggests that terrorist groups have developed ways to hide and transfer ransom payments made from other countries.

AML/CFT risk assessments

44. Of the 28 national anti-money laundering/countering the financing of terrorism (AML/CFT) risk assessments considered for this report[37], 14 specifically mention human trafficking as a money laundering risk, while none identified human trafficking as a terrorist financing risk.[38] Ten of these 14 countries rated their risk

[36] This information was provided a Somali official. The information was based on personal experience rather than on LEA investigations.

[37] Armenia, Australia, Austria, Bhutan, Canada, Cook Islands, Denmark, Fiji, Ghana, Ireland, Isle of Man, Jersey, Japan, Lithuania, New Zealand, Palau, Panama, Philippines, Portugal, Serbia, Singapore, Sri Lanka, Sweden, Switzerland, Tunisia, Ukraine, United Kingdom and the United States.

[38] It is important to note that there is no standard form for compliance with FATF Recommendation 1: assessing risks and applying a risk-based approach, however, many jurisdictions consider the proceeds of

for money laundering from human trafficking: Four rated it as high, three as medium and three as low. Some of the countries that did not mention human trafficking as a money laundering risk as part of their national AML/CFT risk assessment did have other publications detailing money laundering risks related to human trafficking.

45. National AML/CFT risk assessments that mentioned human trafficking appeared to provide some understanding of trends pertaining to the predicate crime and its links to organised crime; however, they provided little information on the financial flows or the laundering of the proceeds of human trafficking. In addition, many of the national AML/CFT risk assessments acknowledged that there are different money laundering risks for human trafficking for the purpose the exploitation of the prostitution of others or other forms of sexual exploitation (HTSE) or for the purpose of forced labour or services, slavery or practices similar to slavery, and servitude (HTFL), but also recognised that there were gaps in their knowledge related to the latter.

crime derived from specific predicate offences most prevalent in their jurisdiction as a means of understanding their money laundering risk.

Part Two: Analysis of money laundering from human trafficking case studies[39][40]

46. As a predicate crime to money laundering, the financial flows from human trafficking can differ significantly from one case to another. Some examples of this differentiation are in the direction of fund movement, the amount provided to various individuals along a human trafficking crime organisation, and the methods used to transact the funds. This differentiation is due to two primary factors:

- Diverse organisational and financial infrastructure are required depending on recruitment and transportation mechanisms utilised by the crime group; and,
- The exploitive purpose for which the human trafficking is conducted yields different types of material benefit to perpetrators.

47. Different acts can or may take place to start the human trafficking offence. These acts can range from recruitment to the transport, transfer, harbouring or the receipt of persons. Each of these steps can take place across jurisdictional boundaries. They may begin in a lower-income source country and continue in one or more transit countries, and finally end in a higher income country, or, the preliminary acts may occur entirely within a singular jurisdiction. Depending on the exact mechanism of the acts to initiate the human trafficking activity, and the organisational structure of the criminal organisation, the financial flows for the group may take different forms as the offence is carried out. This report does not classify the case studies by source jurisdictions, transit jurisdictions, destination jurisdictions and singular jurisdiction human trafficking, as the bulk of the associated proceeds would be in the destination jurisdiction where the exploitation of the individual reaps the proceeds of the crime.

48. In addition, perpetrators involved in the various types of human trafficking can benefit from it in a variety of ways. This could range from payments to perpetrators in cash to the enrichment of a corporate entity. This part of the study groups the offence into the following three categories and examines case studies based on these groupings. It also allowed for the creation of indicators of money laundering, some of which are known general money laundering indicators, but also others unique to the laundering of the proceeds of the specific type of human trafficking, which have been listed in Annex B:

- Human trafficking for the purpose the exploitation of the prostitution of others or other forms of sexual exploitation (HTSE)

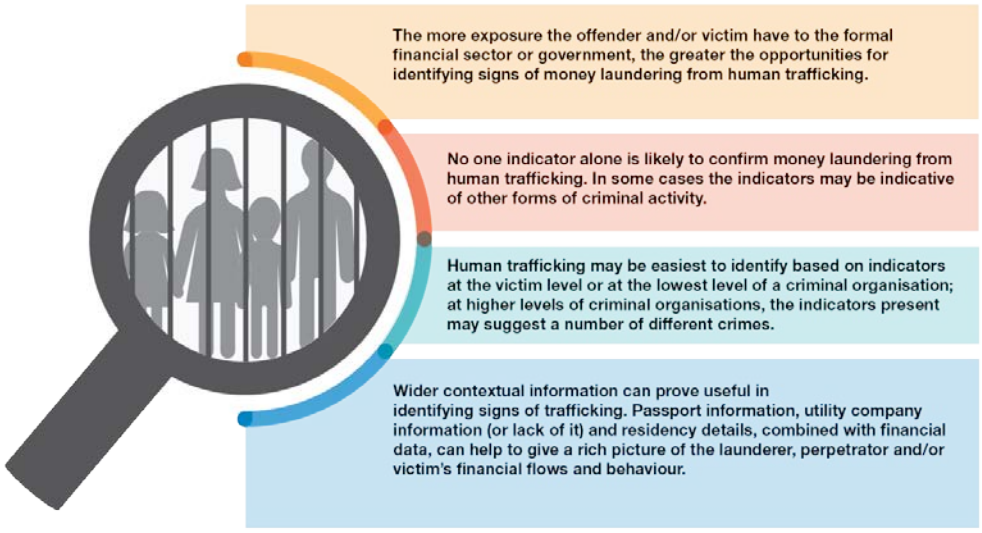
[39] This section of the report provides a selection of case studies, and associated analysis, provided by national authorities, reporting entities, and other entities involved in identifying or combatting the laundering the proceeds of human trafficking. Delegations should carefully consider this section, and also Annex A, which contains relevant case studies not found in the body of this report.

[40] Some of the indicators related to these cases are general money laundering indicators, while others are specific to human trafficking. The indicators are aggregated and segmented by whether they are a general indicator, or an indicator related to HTSE, HTFL or HTRO in Annex B.

- Human Trafficking for the purpose of forced labour or services, slavery or practices similar to slavery, and servitude (HTFL)
- Human Trafficking for the purpose of removal of organs (HTRO)

49. These categories are further segmented, to provide more granularity of the findings based on the roles and/or actors required to commit the offence, and the types of the offence. This will provide a more accurate means of detecting suspicious financial transactions.

Figure 3. Key issues to consider in design efforts to detect financial flows related to human trafficking



50. Additionally, the case studies and indicators highlight four issues which are useful to consider in designing efforts to detect financial flows related to human trafficking:

- **The more exposure the offender and/or victim have to the formal financial sector or government, the greater the opportunities for identifying signs of money laundering from human trafficking**. For example, human trafficking which involves labour via an employment agency or some form of registered business will require some degree of formal interaction with financial institutions, or potentially a government agency. Examples of such formal interaction are opening a bank account, registering for tax purposes or the payment of wages into the victim's account. Conversely, where a victim has no interaction with registered businesses, such as in the case of domestic servitude, it can be much harder to identify the signs of trafficking. In these cases, the physical appearance, such as dress not commensurate with gainful employment, or behaviour, such as deferring to a third party with no apparent relationship for no apparent reason, of the victim may be a greater clue to the likelihood of trafficking.
- **No one indicator alone is likely to confirm money laundering from human trafficking.** In some cases the indicators may be indicative of other forms of criminal activity. But by using a combination of broad primary

indicators, which raise the possibility of money laundering, followed by more specific secondary indicators that may signify money laundering from human trafficking, reporting entities responsible for detecting and combatting this activity can parse out laundering linked to human trafficking and reduce the number of false positives they receive.

- **Wider contextual information can prove useful in identifying signs of trafficking.** Financial institutions may hold passport information, utility company information (or lack of it) and residency details. Combined with financial data, they help to give a rich picture of the launderer, perpetrator and/or victim's financial flows and behaviour.
- **Human trafficking may be easiest to identify based on indicators at the victim level or at the lowest level of a criminal organisation; at higher levels of criminal organisations, the indicators present may suggest a number of different crimes**. This report therefore highlights case studies which demonstrate the financial transactions of victims, and persons at the lower levels of the criminal organisation. These can then be used to 'follow-the-money' to the greater criminal enterprise.

Human trafficking for sexual exploitation

51. This section profiles the two actors involved in human trafficking for sexual exploitation (HTSE) to identify transactions related to this offence:

- Financial transactions of victims; and,
- Financial transactions of perpetrator/launderer.

52. In general, the victims of human trafficking were identified through continued and excessive accommodation, sustenance and movement of types of expenses (e.g., airline tickets, taxi fares, car hire, train tickets). Incurring a number of these expenses is completely normal in circumstances such as vacationing or traveling for business; however, excessive continued incurrence of these expenses may demonstrate that an individual is a victim of HTSE. As demonstrated in the case studies, the identification of victims' transactions has helped reporting entities identify the individuals laundering the proceeds of this crime given their financial interactions with the suspected victim

Identifying suspicious transactions and money laundering from HTSE victim transactions

53. Victims are generally exploited through a variety of means over an extended period of time (i.e., rarely is a victim subject to one instance of sexual exploitation). Therefore, offenders are required to meet the essential needs of the victims throughout the duration of their, generally long-term, exploitation. This care includes basic housing, personal products and nourishment, as well as logistical items so that they may engage in the sexual exploitation such as transportation around a city or larger area, lodging expenses (a flat or hotel) and maintenance of a location for the purpose of commercial sex. The financial transactions for these

expenditures may be conducted directly by the victim or by the perpetrator or launderer involved in the human trafficking offence.

54. Compared to identifying money laundering from human trafficking, which intentionally appears as normal transactions, it is easier to profile a victim's expenses/financial flows. Profiling these expenses is a good first step in identifying the proceeds from HTSE by first identifying the victims of the crime. Further examining the financial transactions of the victim can help identify the individuals laundering the proceeds from the HTSE offence. These transactions can highlight a pattern of activity that can lead to the larger sexual exploitation trafficking network. The following case studies identify indicators of victim-related financial transactions:

Case Study 1.

A financial institution submitted multiple Suspicious Transaction Reports identifying a group of financially connected individuals suspected to be engaging in and/or deriving profit from HTSE. The suspicious transaction reports identified the account of Victim A, who was using excessive taxi and rider sharing services after midnight in various cities across the country where they appeared to be staying only for a few days or weeks at a time. Victim A appeared to not be paying for any accommodations in these various cities, but did incur room service and eatery bills at various motels/hotels. Victim A was also frequenting pharmacies and fast food eateries daily or multiple times a day in a manner inconsistent with normal account activity. Lastly, Victim A's telephone number was connected to multiple advertisements and Backpage postings for escort services. Further review of account activity of Victim A indicates that she was receiving email money transfers (a service in Canada which allows any holder of a bank account to automatically deposit funds into another bank account via email) from email addresses with all male names and that she was repeatedly sending funds to Subject A.

Subject A's accounts were mainly funded by third party cash deposits and frequent email money transfers from various individuals that are deemed to be excessive and do not appear to be in line with the subject's employment income and level of wealth. Subject A appears to use multiple contact email addresses and names. Funds were often depleted rapidly via cash withdrawals, credit card payments, transfers to other individuals and outgoing email money transfers without apparent economic purpose. Further review of Subject A's accounts revealed that individuals transacting with the subject reside in various geographic locations across Canada.

Subject A also received an out-of-province incoming email money transfer from Subject B. Source of funds for this specific transfer was from an email money transfer immediately remitted by another individual and Subject B appears to have used his account to facilitate the pass-through activity. The financial institution also found that Subject B's account activities demonstrate frequent account transfers between the client's bank accounts and credit card, frequent purchases at online gaming sites, Bitcoin exchanges,

payment processors, sports collectable stores, and email money transfers with various individuals with unknown source and purpose.

Subjects A and B are currently under police investigation for their HTSE of Victim A. This investigation was started based on the suspicious transaction reporting from the Canadian financial institution.

Source: Canada

55. The preceding case demonstrated the consistent pattern of activity exhibited by the victims of HTSE, in addition to a newer developing trend of payment to the perpetrator or launderer via new payment technology such as email money transfers and virtual currency. The following case displays such typical victim transactions, as well as a number of behavioural-type indicators that were used by a financial institution to identify members in a criminal organisation conducting HTSE:

Case Study 2.

A local law enforcement agency provided a bank with information about an alleged organised crime network comprising at least six individuals involved in trafficking women from Eastern Europe for the purposes of sexual exploitation in both the UK and the rest of Europe. The group had been observed spending significant funds on adult websites named by UK local law enforcement as used to advertise trafficked women.

In the initial review, the Bank identified that one of the individuals had previously been a customer who had their relationship exited for financial crime concerns and another was an existing retail customer who held an active account. The previous customer had an internal alert raised by branch staff due to staff witnessing in-branch, coercive behaviours. They noted that a customer was regularly visiting to pay in cash, using the branch automated machines and avoiding the counter, even when there were no queues. The customer was accompanied by the same male on a number of visits during the same week. That male appeared to be exerting control over them and was checking deposits and statements; seemingly controlling her actions. The existing customer was also reviewed and it was apparent that this account was being used to pay for a variety of low cost/high volume transportation and logistics-related bookings across Europe. Direct reviews of transactions also highlighted additional indicators, including: a common telephone number to two other customers; regular low level expenditure at local chemist/pharmacy and supermarket; and no evidence of full-time employment despite significant turnover in the account.

The Bank filed two further suspicious activity reports that linked six customers and their transactional activity to unusual behaviour exhibiting indicators of laundering the proceeds of human trafficking for the purpose of sexual exploitation. This extended the law enforcement intelligence picture for their ongoing investigation and also identified previously unknown subjects. Local law enforcement developed the case and arrested members of

the organised crime network who were subsequently convicted of human trafficking, modern slavery and prostitution offences.

Source: Toolkit for Tackling Human Trafficking – Thomson Reuters Foundation and European Banks Alliance

56. Lastly, the following case demonstrates the prosecution of a major facilitator of HTSE activities. This case demonstrates both the financial flows related to the commission of the HTSE offence, and the subsequent money laundering methodologies used:

Case Study 3.

On April 9, 2018 the US Department of Justice seized Backpage.com, the Internet's leading forum for prostitution ads and a place where sex traffickers frequently advertised children and adults. Backpage earned hundreds of millions of dollars from facilitating prostitution and sex trafficking and served as a platform for human traffickers. In addition, seven Backpage executives were indicted for their role in a conspiracy to facilitate prostitution and were charged with 40 counts of money laundering in various forms.

On April 12, 2018, the Justice Department announced that Backpage's co-founder and CEO, Carl Ferrer, 57, of Frisco, Texas, pleaded guilty to conspiracy to facilitate prostitution using a facility in interstate or foreign commerce and to engage in money laundering. Additionally, several Backpage-related corporate entities, including Backpage.com LLC, have entered guilty pleas to conspiracy to engage in money laundering.

In his plea agreement, Ferrer admitted that he conspired with other Backpage principals to engage in various money laundering offenses. Specifically, Ferrer admitted that since 2004, Backpage has earned hundreds of millions of dollars in revenue from publishing "escort" and "adult" ads. Over time, many banks, credit card companies, and other financial institutions refused to do business with Backpage due to the illegal nature of its business. In response, Ferrer admitted that he worked with his co-conspirators to find ways to fool credit card companies into believing that Backpage-associated charges were being incurred on different websites, to route Backpage-related payments and proceeds through bank accounts held in the name of seemingly unconnected entities, and to use cryptocurrency-processing companies for similar purposes.

Backpage advertisers used the proceeds of crime (money earned from pimping/prostitution) to purchase ads on Backpage; additionally, the fees which Backpage collected for posting prostitutions ads also constituted the proceeds of unlawful activity. The investigation revealed that laundering of criminal proceeds was conducted through numerous US-based financial institutions and banks in ten foreign countries. The indictment unsealed by the US District Court for the District of Arizona further alleged that Backpage pursued an array of sophisticated money laundering strategies, including the

following:

a) Instructing advertisers to send checks and money orders to anonymous post office boxes, depositing those payments in bank accounts held in the name of entities with no apparent connection to Backpage, and then giving the advertisers a corresponding "credit" on Backpage to purchase new advertisements;

b) Wiring the proceeds of Backpage's business to bank accounts in foreign countries and then redistributing the funds to Backpage executives (as compensation) or redepositing the funds in bank accounts held in the United States (to conceal the nature of those funds and promote Backpage's ongoing operations); and

c) Converting advertisers' payments, and the proceeds of Backpage's business, into and out of cryptocurrency.

Source: United States

Identifying money laundering and STRs from HTSE perpetrator or launderer transactions

57. HTSE can be a major source of income for individual criminals and organised crime networks operating at local, national and international levels. Given the profitability of the offence, individuals perpetrating the HTSE crime, as well as laundering the proceeds of that crime, may be identifiable by observing financial transactions and information obtained by financial institutions in the course of conducting their customer due diligence and the behaviour of offenders. Many of the typologies and indicators in this subgrouping are common to laundering the proceeds of other cash generating crimes and are generally not unique to laundering the proceeds of HTSE as observed in the following cases. For example, hawala-type systems are used to transfer the proceeds of HTSE to another country.

Case Study 4.

Between 2007 and 2010, several Thai women were sexually exploited in Thai massage parlours in Belgium. These women were lured to Belgium under false pretences of a better life in Europe. Upon arrival, they were forced to work in massage parlours where they had to perform sexual services for payment. Victims were debt-bonded to their traffickers for EUR 10 000 - 15 000 and forced to hand over their earnings to repay this debt and to pay for accommodation. Victims were also forced to hand over their passports until they had paid off the whole debt. In some instances, victims' families in Thailand were threatened to ensure co-operation. Ten defendants were convicted of human smuggling, human trafficking for the purpose of sexual exploitation, criminal organisation, and facilitation of illegal immigration.

A human trafficking for the purpose of sexual exploitation case was opened on the basis of checks and searches in massage parlours by the inspection services. In a Mechelen-based massage parlour, they discovered complete

accounts showing amounts and names. The police noted that the same company managed different massage parlours. Through the analysis of the phone contacts, the main defendant (Defendant 1) and his travel agency were identified. The police also checked advertisements in newspapers and various websites for further information on massage parlours engaging in human trafficking for the purposes of sexual exploitation. These massage parlours were put under surveillance.

The financial investigation revealed three types of transactions:

- money transfers to different recipients in Thailand through the defendants;
- cash payments; and
- the purchase of a house in Thailand.

Various suspicious transfers of funds totalling EUR 48 838 were made through a company to different people in Thailand. Funds totalling approximately EUR 50 000 were also regularly sent through an MS. Defendant 1's wife wired funds totalling EUR 20 598 to beneficiaries in Thailand. The economic justifications for the transfer of funds were not known however, investigators suspected funds were proceeds from human trafficking and/or exploitation of prostitution. The case was prosecuted and the court concluded that the defendants' cash payments and large value transfer of funds to Thailand compared to their income was inconsistent with the commercial turnover usual for a business of that size or type.

Source: Belgium; MYRIA: Trafficking and Smuggling of Human Beings Annual Report 2016

Case Study 5.

A recent major ongoing investigation uncovered tens of millions of dollars in illicit proceeds derived from sex trafficking which were laundered and smuggled by a criminal organisation. Twenty-one members of an international sex trafficking ring were identified as having various roles in the organisation including traffickers, house bosses, money launderers, and facilitators. This sophisticated criminal organisation, which operated for approximately eight years, facilitated the transportation of women from Southeast Asia to cities across the United States and forced them into prostitution. During the coordinated takedown, law enforcement seized hundreds of thousands of dollars in cash, cell phones, and multiple weapons.

This criminal organisation engaged in widespread visa fraud to facilitate the international travel by the victims. Human traffickers assisted the victims in obtaining fraudulent visas and travel documents by funding nominee bank accounts, creating fictitious backgrounds and occupations, and instructing the victims to enter into fraudulent marriages to increase the likelihood that their visa applications would be approved.

Members of the criminal organisation held more than one role, over time or

simultaneously, in order to maximise profits. Some individuals held the bondage debt of a victim until it was fully repaid or, in some instances, a victim's bondage debt was sold from one human trafficker to another. The "house bosses" owned the commercial sex houses and ran the day-to-day operations. The money launderers supported the continued operation of the criminal enterprise by making bank accounts available, coordinating deposits and withdrawals of cash, and moving money to and from Southeast Asia. The organisation's facilitators assisted with the logistics of renting the commercial sex houses, facilitating the transport of victims, assisting with money laundering, and entering into fraudulent marriages with members of the criminal organisation so those criminals could gain immigration status in the United States.

The criminal organisation dealt primarily in cash and engaged in rampant and sophisticated money laundering in order to promote, distribute, and conceal illegal profits. The organisation used funnel accounts to launder and route cash from cities across the United States to the money launderers on the West Coast. Upon entry to the United States, trafficking victims were often escorted by a member of the organisation to a bank and instructed to open an account in their own name; once the account was opened, a member of the organisation took control of it and then provided the account information to other criminal associates to coordinate deposits throughout the United States.

The organisation also engaged in bulk cash smuggling by physically transporting and mailing illegal proceeds from sex trafficking to Southeast Asia. The money launderers recruited money mules to carry large volumes of cash on their persons when traveling overseas as well as to hide cash in items such as clothing and dolls. Finally, the organisation used a hawala system to transfer money to Southeast Asia and elsewhere outside the United States.

Source: United States

Human trafficking for forced labour

58. HTFL involves work that is performed involuntarily and under the menace of a penalty. It refers to trafficking situations in which persons are coerced to work through the use of violence or intimidation or by more subtle means such as manipulated debt, retention of identity papers or threats of denunciation to immigration authorities. Forced labour can take many forms but at its heart is the exploitation of another individual's labour for profit.

59. According to the *ILO Forced Labour Convention, 1930* (No. 29), forced or compulsory labour is "all work or service which is exacted from any person under the threat of a penalty and for which the person has not offered himself or herself voluntarily." This definition encompasses the following three elements:

1. Work or service refers to all types of work occurring in any activity, industry or sector including in the informal economy.

2. Menace of a penalty refers to a wide range of penalties used to compel someone to work.
3. Involuntariness: The term "offered voluntarily" refers to the free and informed consent of a worker to take a job and his or her freedom to leave at any time. This is not the case for example when an employer or recruiter makes false promises so that a worker take a job he or she would not otherwise have accepted.

Types and characteristics of forced labour

60. Forced labour can take various guises depending on the method of recruitment, coercion, control and exploitation of the individual involved. Individual cases may often involve a combination of different types of forced labour. Types of forced labour include:

Types and characteristics of forced labour

Type	Characteristics
Exploitation in the workplace	
Victims exploited for multiple purposes in isolated environment	Victims who are often highly vulnerable are exploited for labour in multiple ways in isolated rural locations. Victims live on offenders' property in squalid conditions, are subject to repeated abuse and are very rarely paid.
Victims work for offenders	Victims are forced to work directly for offenders in businesses or sites that they own or control (some offenders may be gangmasters). The main method of exploitation is not paying or illegally underpaying victims.
Victims work for someone other than offenders	Victims are employed in a legitimate and often low-skilled job, with legal working conditions, by an employer unrelated to the offenders. Most or all wages are taken by offenders often through control of the victims' bank accounts.
Exploitation in the home (domestic servitude)	
Exploited by partner	Victims are forced to undertake household chores for their partner and often their partner's relatives. If married, the marriage may have been arranged or forced and the servitude often occurs alongside domestic abuse and sexual exploitation
Exploited by relatives	Victims live with and exploited for household chores and childcare by family members, usually extended family. Many victims are children
Exploiters not related to victims	Victims live with offenders who are often strangers. Victims are forced to undertake household chores and are mostly confined to the house.
Forced gang-related criminality	Victims are forced to undertake gang related criminal activities, most commonly relating to drug networks. Victims are often children who are forced by gangs to transport drugs and money.
Forced labour in illegal activities	Victims are forced to provide labour to offenders for illegal purposes e.g. victims being forced to cultivate cannabis in private residences
Forced acquisitive crime	Victims are forced by offenders to carry out acquisitive crimes such as shoplifting and pickpocketing. Offenders may provide food and accommodation to victims but rarely pay them
Forced begging	Victims are transported by offenders to locations to beg on the streets for money, which is then taken by offenders. Victims are often children vulnerable adults.
Trafficking for forced sham marriage	Traffickers will transport victims to a host country in which the individual has a legal immigration or citizenship status and sell them victims to an exploiter in a one-off transaction. Exploiters then marry victims to gain immigration advantages and often sexually abuse them.

Source: A Typology of Modern Slavery in the UK

Identifying suspicious transactions and money laundering from the types of HTFL

61. As with human trafficking for the purposes of sexual exploitation, HTFL can take many forms, meaning that the proceeds, and associated laundering of the proceeds, are realised in different ways depending on the type of HTFL. Most forms of forced labour involve some form of initial recruitment of the victim. This is often under the pretence of a better job overseas, at a significantly higher wage. In cases where the victim is forced to work in legal employment, the employer (who themselves are often unaware that they are employing trafficked individuals) can make a form of payment into either the traffickers' or victims' bank account. Where financial institutions with reporting obligations observe financial activity such as multiple employees being paid into a single account or where wage receipt is followed by rapid withdrawal or onward transfer into single accounts, they should consider assessing the situation to determine if there is a suspicion of laundering the proceeds of human trafficking.

62. In addition to the financial footprint, the victim or their trafficker will often have to interact with a government agency or reporting entity staff in person, providing further opportunities to pick up on any suspicious behaviour. Where an individual claims to act on behalf of another employee, demonstrating signs of control of the person or their documents, this may be indicative of forced labour. Unusual in-branch behaviour, such as individuals avoiding cashiers, even when there are no queues, may also indicate the presence of trafficking.

63. In the following case, the initial suspicious activity of two occupants at the same address led to the identification of other individuals at the same address working for the same company. Traffickers will often house their victims in substandard accommodation, with many victims sleeping in a single bedroom. Further similarities in the documentation used to open the victims accounts led the bank to conclude that HTFL was involved:

Case Study 6.

The retail team in a major high street bank identified a potential trend which resulted in a referral to the FIU for investigation. Two customers were living at the same address with funds received followed by multiple cash withdrawals. The purpose of the referral was to identify if any additional customers had similar account activity. A review of these two customers raised concerns due to possible Labour Exploitation in the construction sector.

After the initial referral, the investigation identified at the same address three additional customers who were of concern, making five customers in total. A profile review identified four customers showing the same pattern of account activity and one customer with different account activity.

Analysis of the four customers showing the same pattern of activity identified

the following:

- The accounts were receiving Faster Payments Inwards (FPI) from the same entity followed by ATM withdrawals and larger cash withdrawals in branch and in the same locations.
- The accounts were showing a lack of living expenses such as food, petrol, utilities and rent.

Further analysis of these four customers identified the following:

- all of the profiles identified registered the same mobile number
- Two of the 4 profiles identified registered the same email address
- All profiles had the same nationality
- The Passports used to open 4 the accounts were temporary and issued in the same month. The same home town was stated on all passports
- Income was received and immediately withdrawn in cash

Deeper analysis into these four customers identified the fifth customer residing at the address that had introduced the four customers to the Bank when opening the account. Bank records advise this fifth customer was an interpreter as the applicants could not speak English very well. The mobile number and email address registered on the profiles of the four victims linked to the fifth customers at the address.

The bank identified four customers receiving funds from the same employer. Further analysis was completed into other accounts which had received funds from this employer to identify if the network was larger than the 4 customers identified to date. Based on the foregoing indicators, the FIU suspected that the four individuals might be victims of HTFL and the fifth may have been involved in the offences.

The FIU's analysis revealed that there were further customers of concern. The case was referred to law enforcement who, following a subsequent investigation, confirmed that the customers were subject to forced labour exploitation and began enforcement action.

Source: United Kingdom

64. The following case demonstrates some of the manners in which the victims of HTFL can be also forced to be involved with providing the proceeds to perpetrators, and also used in the laundering mechanisms for the proceeds:

Case Study 7.

In 2013, Italian police started an investigation concerning a major informal strike by immigrant workmen, which led them to discover a HTFL scheme involving Bangladeshi and Indian immigrants, trafficked by three gangmasters, one Bangladeshi (Mr A) and two Italian nationals (Mr B and Mr C). The investigation was concerning Alpha, an Italian logistics firm run by

Mr A. This investigation was commenced through suspicious transaction reporting to the financial intelligence unit based on a number of factors:

- News media reports of a major informal strike by immigrant workmen;
- Rumours about unfair business practices/competition by Alpha;
- Anomalous management and ownership structure of logistics companies associated to Alpha (run and owned by foreign workmen only recently immigrated to Italy, also known to work as employees for similar firms);
- Nearly simultaneous ATM cash withdrawals through payment cards belonging to several immigrants working for the same firm at a singular location.

The investigation uncovered that Mr A had selected the workmen in their home countries, offering them temporary jobs at Alpha in exchange for a sum they would pay him through their future work in the cooperative. This arrangement would also grant them temporary work visas to Italy, so that both their residence and employment in Italy would be completely legal.

On such legal ground, once arrived in Italy, Mr A forced each immigrant workman first to address banks through him in order to get current accounts and payment cards (debit cards and reloadable cards), to which Alpha would credit the wages. The immigrant workmen then had to hand the passwords to Mr B, enabling him to take back half the wages through ATM cash withdrawals. The immigrants were forced to provide a portion of their wages to Mr A to pay back their debt, as well as payment for basic goods, such as accommodation and food etc. In spite of the HTFL, Alpha's accounting and financial records appeared compliant with the law, because each workman's weekly working time and wages were formally consistent with legal thresholds, though actually each workman worked for nearly twice as many hours for half the salary.

Alpha's profits were withdrawn through the immigrants' cards, and in some instances sent to shell companies made to look like logistics companies through a false invoicing scheme with the an apparent ownership structure owned and operated by the victims. The actual beneficial owner of the shell companies to which the funds were sent was Mr C, who was found to also be the beneficial owner of other such shell companies during the course of the investigation. These corporate vehicles provided Mr. C with a sort of multi-purpose "money laundering machine" ultimately founded on immigrants' vulnerability to threats about their dismissal from their work, which would have resulted in being sent back to their home countries.

This scheme enabled the laundering of an estimated EUR 2.5 million in two and a half years.

Source: Italy

65. The following case revealed suspicious behaviours around ATM withdrawals. A victim's ATM usage could occur at the same machine at the same time, suggesting that a third party was in control of their cards. Further use of open source tools like Google StreetView revealed inconsistencies between the number of victims living at a particular property, and the actual size of the house:

Case Study 8.

Two brothers trafficked 18 men from Poland to the United Kingdom to work in a major sports clothing warehouse. The brothers employed 'spotters' in Poland to identify vulnerable men and approach them with an offer of work and accommodation overseas. The men received coach tickets to the destination country. Once the victims had arrived, they had to hand in their passports. They were forced to live in an overcrowded house in squalid conditions. The offenders helped the victims to open bank accounts, and then seized their bank cards to control these accounts. The brothers used physical and verbal threats as a means of control. The victims found employment at the warehouse through an employment agency. The offenders took the majority of the victims' GBP 265 weekly wage, leaving each victim with just GBP 90 a week. The offenders reportedly made GBP 35 000 throughout the exploitation period.

Following work with the police the bank analysed the information it held on the address and found that there were up to 15 customers registered at that address.

They reviewed each of these customers and identified the following suspicious activity:

- The property, when looked at on Google StreetView, could only comfortably accommodate 2 or 3 people at the most
- The customers living there received weekly incomes from an agency
- A high percentage of that income was withdrawn quickly after receipt in to the accounts
- Analysis of ATM activity for these customers shows that their ATM usage often occurred at the same machine at the same time suggesting that a third party is in control of their cards.

Following a police raid on the house and arrest of the brothers, both offenders pleaded guilty to human trafficking offences, and were sentenced to six years each.

Source: United Kingdom

66. Lastly, the following case demonstrates some of the methods and techniques which have been commonly used to transfer the proceeds of HTFL to another destination, namely the use of hawala-type systems and physical transportation of cash. Such techniques can be designed to frustrate financial investigation:

Case Study 9.

In September 2016, a jury in the High Court at Auckland found 46-year-old Faroz ALI – also known as Feroz ALI – guilty of 15 counts of trafficking Fijians to New Zealand on false promises of NZD 900 weekly wages for fruit-picking. He charged the workers exorbitant fees and then exploited them upon arrival by forcing them to work illegally and live in overcrowded conditions, underpaying them and threatening them with deportation if they complained. ALI was found to be receiving large payments from legitimate New Zealand companies, for the provision of services by his construction firm, for which the Fijians forcibly worked. With the illicit proceeds of the HTFL offence, ALI was utilising a hawala-type system to return funds to Fiji, as well as the physical transportation of cash for the purposes of personal enrichment in Fiji.

ALI was also found guilty on 16 counts of aiding and abetting people to enter or remain in the country unlawfully. He pleaded guilty to charges of exploitation, including failing to pay workers minimum wage or holiday pay, as well as aiding and abetting workers to breach the conditions of their visas.

Approximately NZD130 000 was calculated to be the total loss of wages, holiday pay and the like for identified victims (noting that the number of victims and period of offending was ring fenced)

ALI, the first person to be convicted of people trafficking in New Zealand, was jailed for nine and a half years.

Source: New Zealand

Human trafficking for the removal of organs

67. Human trafficking for the purpose of the removal of organs renders significant harm to the victim, for potentially little reward, if any. This crime, significant in its impact to the victim, represents the vast minority of human trafficking cases.

This is exemplified in that this study received no viable case studies of HTRO, but did receive a few cases of organ trafficking, which is outside of the scope of this report.

Box 2. Human Trafficking for the Purpose of the Removal of Organs Versus Organ Trafficking[41]

Trafficking in organs and trafficking in persons for the removal of organs are different crimes, though frequently confused in public debate and among the

[41] Quoted excerpt from UNODC's Assessment Toolkit for the Trafficking of Persons for Organ Removal, 2015 https://www.unodc.org/documents/human-trafficking/2015/UNODC_Assessment_Toolkit_TIP_for_the_Purpose_of_Organ_Removal.pdf

legal and scientific communities. In the case of trafficking in organs, the object of the crime is the organ, whereas in the case of human trafficking for organ removal, the object of the crime is the person. Trafficking in organs may have its origin in cases of human trafficking for organ removal, but organ trafficking will also frequently occur with no link to a case of human trafficking. The mixing up of these two phenomena could hinder efforts to combat both phenomena and provide comprehensive victim protection and assistance.

68. While this study did not receive any viable cases on HTRO, UNODC's *Assessment Toolkit for the Trafficking in Persons for Organ Removal* provides detailed information on the offence which leads to two potential opportunities to detect the offence via financial flows: 1) financing the infrastructure required to effect the offence, and 2) payment to the various individuals required to effect the offence.

69. Unlike HTSE and HTFL, there is a much shorter period of caring for a victim to profit off their exploitation for HTRO, which takes away one opportunity to detect the crime via its associated financial flows. However, HTRO does require more significant infrastructure in comparison to the other classifications, such as medical facilities and equipment. There may be an ability to detect the HTRO offence through the procurement of medical equipment outside of the context of an official medical care facility.

70. The HTRO offence also provides the perpetrators with a more significant one time financial gain than HTSE and HTFL. The UNODC report provides case studies which indicate that, for example, kidney procedures can cost as high as USD 100 000 – USD 200 000 on the black market. This significant inflow provides the second opportunity to detect HTRO. The payment itself may be provided to one individual coordinating the HTRO, or to a network of individuals each contributing to conducting the offence, in the form of a payment that is not in line with what would be reasonably expected of their employment.

Box 3. Human Trafficking for the Purpose of the Removal of Organs Actors[42]

Recruiters (other terms used include brokers, organizers, connectors, coordinators, middlemen, kidney hunters, etc.);

Medical professionals (including specialist doctors such as surgeons and nephrologists [medical doctors who specialize in kidney care and treating diseases of the kidneys], as well as nursing staff and other medical staff);

Other private and public sector facilitators (such as hospitals, transplant centres, laboratories and other medical facilities, as well as their staff, insurance companies, travel agencies, airlines and their staff, as well as

[42] Quoted excerpt from UNODC's Assessment Toolkit for the Trafficking of Persons for Organ Removal, 2015 https://www.unodc.org/documents/human-trafficking/2015/UNODC_Assessment_Toolkit_TIP_for_the_Purpose_of_Organ_Removal.pdf

guards, drivers, service providers, law enforcement officials, translators, etc.);

Although **organ recipients** ('patients', 'buyers') have largely not been found to be perpetrators of trafficking in persons for organ removal, they may have been knowingly or unknowingly involved as recipients of organs that come from trafficking victims.

Victims of trafficking in persons for organ removal (also 'donors', 'victim-donors', 'sellers', 'organ suppliers') are not to be considered actors within the trafficking schemes. They may, however, take on active roles, e.g. by approaching brokers, offering their kidney for sale.

71. It should be noted that both opportunities to identify HTRO via financial flows may point to both HTRO and organ trafficking and other means will be required to distinguish the two once the situation is detected.

Indicators of money laundering from human trafficking

72. Indicators of money laundering from human trafficking derived from the above noted cases studies and information from this section, as well as the other cases provided in this report (provided in full in Annex A) are listed, in full, in Annex B. These indicators will assist obliged entities and national authorities in detecting transactions where there is a suspicion of the laundering of the proceeds of human trafficking.

Part Three: Challenges and good practices in combatting ML/TF from human trafficking

Challenges identified in the 2011 FATF Report

73. The previous FATF report identified a number of challenges in detecting, investigating and prosecuting money laundering from the trafficking in human beings and the smuggling of migrants. The top three challenges include:

1. **Limited international co-operation**: The previous FATF report identified international co-operation as the single biggest challenge in combatting ML/TF from human trafficking/smuggling of migrants. More specific challenges mentioned under this theme include, time delays in obtaining information, incomplete responses to information requests, restrictive conditions attached to the sharing of information and ineffectiveness of the mutual legal assistance process.
2. **Lack of awareness or concern from law enforcement/prosecution authorities**: The previous FATF report cited a culture of investigation and prosecution focusing on the predicate offence and not the associated laundering offence, and a lack of effective training of authorities in financial investigations.
3. **The difficulty to detect funds**: The previous FATF report identifies human trafficking and the smuggling of migrants as being crimes where there are high volumes of cash and comingling of funds as primary money laundering methodologies thereby posing problems for financial investigators in 'following the money'.

74. The previous FATF report also identified other challenges, such as the lack of investigative resources, the lack of witness co-operation, corruption, and time delays in national co-operation. The previous FATF report also notes low levels of STR submission by reporting entities on ML/TF from human trafficking and the smuggling of migrants.

Challenges identified in the current study

75. This section summarises the main challenges identified through the course of the study. Some of the challenges enunciated in the previous FATF report remained common themes throughout the project; however, a number of significant, incremental challenges have been identified.

76. **Addressing the challenges of the previous FATF study:** The challenges identified in the previous FATF report, were also identified as challenges in effectively detecting, investigating and prosecuting ML/TF from human trafficking during the current study, seven years later. Some of these challenges were structural, due to the nature of the predicate offence, some due to a lack of granular understanding of the predicate offence and associated financial flows, and some demonstrating effectiveness issues by authorities. While it is impossible to quantify

the difference in the level of effectiveness of authorities in combatting ML/TF from human trafficking between 2011 and 2018, estimated proceeds derived from human trafficking has increased substantially.

77. **Money laundering risk from proceeds of human trafficking not adequately detailed in risk assessments and understood**: Human trafficking, in many respects, remains a 'hidden crime'. From victims that do not understand that they are victims, victims who are not incentivised to declare the nature of the crime that they have been the victim of, difficulty in detecting forced labour exploitation, national authorities focusing largely on international human trafficking and human trafficking being hidden within other crimes such as prostitution (in some countries) or illegal immigration. In addition, there are incremental challenges when it comes to understanding the money laundering risk related to human trafficking. For example, assets acquired in HTFL are difficult to identify, and a significant amount of the proceeds are in cash.

78. Due to the unseen nature of some aspects of the predicate offence and the difficulty in identifying the laundering of the proceeds of human trafficking, it is hard for national authorities to gather statistics to properly assess the ML risk from human trafficking in their jurisdiction. The review of available risk assessments demonstrates this. On aggregate, the risk assessments do not identify ML from human trafficking with the gravity commensurate with the estimated aggregate global proceeds derived from the human trafficking; this places human trafficking among the most significant illicit revenue generators in the world. If the ML risks remain under-represented globally, then appropriate risk mitigation measures will not be put into place to curb this crime.

79. **Incomplete domestic information sharing**: Many stakeholders – including competent authorities, and stakeholders in the private sector, civil society and NPO sector – are working to combat human trafficking, and money laundering from human trafficking. Each of the stakeholders can have information relevant to combating ML/TF from human trafficking. Some of the stakeholders form part of a country's AML/CFT regime, others are partners of the regime, while others still have limited to no interaction historically with the AML/CFT regimes. This diversity of partnerships, some national authorities' inability to share with all partners and the associated diversity of information offered by stakeholders combatting human trafficking, and ML/TF from human trafficking, can lead to incomplete and/or misunderstood domestic information sharing which could be better co-ordinated and more complete.

80. **Detecting, reporting and analysing suspicious transaction reports**: Members of the private sector have reported issues in effectively detecting transactions where there is a suspicion that the proceeds from human trafficking are being laundered or contribute to the financing of terrorist activity. Specifically, the private sector has indicated that national authorities have provided some information on the national threat environment with respect to human trafficking. However, the information is not complete and does not allow the private sector to best identify such transactions. In addition, reporting entities have indicated that they require more precise indicators of money laundering/terrorist financing, which are responsive to the national threat environment of human trafficking. These issues may result in part from the lack of consideration or weight given to human

trafficking in national risk assessment exercises, or inadequate communication of the risk.

81. As a result of the reporting entities' difficulties in identifying transactions where there is a suspicion that the proceeds from human trafficking are being laundered or contribute to the financing of terrorist activities, financial intelligence units have reported difficulty in appropriately prioritising suspicious transaction reports related to human trafficking. In many respects, reporting entities are not equipped with sufficiently granular information to appropriately identify these transactions, or differentiate such transactions from other reported suspicious transactions. In turn, the FIU is not able to attribute the suspicious transaction report to suspected laundering of the proceeds of human trafficking and forward these transactions to the appropriate authority.

82. **Identifying proceeds in forced labour exploitation type human trafficking cases**: Competent authorities indicated significant issues in identifying the proceeds of forced labour exploitation type human trafficking cases. By nature, these types of cases provide material benefit for the individuals/entities for whom the victims are forced to work, but also for the perpetrators who trafficked the victims, who may or may not be the same individual. In some instances, the material benefit can be readily identified as the direct output of an individual over time or when an entire entity's business model is based around forced labour. In other instances, the individuals merely contributed to a gradual enrichment of individuals or entities over time. Such 'balance sheet' improvements are difficult to trace back to the specific predicate crime that have been committed. The following case exemplifies a HTFL situation where the benefit derived from the offence is difficult to quantify and identify:

Case Study 12. Domestic Servitude by a Stranger

A Tanzanian woman scientist living in London trafficked a 21-year-old woman from Tanzania to work as a slave in her home. The offender offered the victim 250 000 Tanzanian shillings (~£120 at the time) a month to work as her housekeeper. The offender's family paid for the victim's visa and arranged her flights from Tanzania to the UK. Once in the UK, the victim was taken to the offender's two-bedroom flat. The offender and her three children all lived in one room and the second bedroom was rented out. The victim was made to share a bed with the offender's 12-year-old son. The victim was forced to work for up to 19 hours a day cooking and cleaning, as well as looking after the three children. She was never paid for her work, but was given £20 on one occasion by the lodger. Her passport was taken from her and she was banned from contacting family or friends. She was regularly verbally, physically and psychologically abused. This exploitation lasted seven months. The victim was encouraged by a friend to report her exploitation to the police, leading to the offender's arrest. The offender was sentenced and ordered to pay £3 000 in compensation to the victim.

This case highlights the difficulty in determining the material benefit gained through certain types of HTFL where the proceeds are indirect, gradual

enrichment, or enrichment of an individual's lifestyle, but are not realised in a singular material good.

Source: United Kingdom

83. **Victims as sources of information and potential witnesses**: Depending on the circumstances, victims of human trafficking may provide useful insight into the financial operations of the individuals who have trafficked them. However, victims of human trafficking are frequently subject to physical and mental horrors as part of their experience in being trafficked. As a result, many victims are reluctant or unable to provide information to authorities for fear that they or their family/friends may be targeted by the perpetrators. In addition, some jurisdictions have reported problems in keeping victims in the country and motivated to providing information/testimony throughout a potentially lengthy investigative proceeding.

84. **Lack of convictions or confirmed intelligence regarding proceeds of human trafficking contributing to terrorist financing**: A number of studies, reports, press reports and victim testimonials have highlighted the link between human trafficking and terrorist financing. These reports indicate that terrorist organisations such as ISIL, Boko Haram and Al Shabaab have used human trafficking as a way to raise funds and to provide material support to their organisations and activities. Such activity has, to date, been generally confined to areas which are controlled, or partially controlled, by terrorist groups.

85. Despite these reports, there have been no specific law enforcement cases studies that confirmed the proceeds of human trafficking contributing to the financing of a terrorist group. There are many reasons why this may be the case:

- Authorities, appropriately, prioritise victim safety above evidence or intelligence gathering; their focus is thus not on gathering evidence to secure a terrorist financing conviction.
- Evidence and intelligence collection in a given geography which is controlled, or partially controlled, by terrorist groups is very challenging, even after the conclusion of a conflict. The admissibility of such information to court proceeds would also be challenging.
- Seeking a conviction for or specific intelligence on the financing of terrorist activities from the proceeds of human trafficking is simply a lower priority for national authorities combatting terrorist groups than other outcomes which could range from kinetic action to victim extraction.
- Prosecutors may opt to pursue other charges – and not terrorism finance-related charges – because the evidence is more readily available and the penalties are similar.

Good practices in combatting ML/TF from human trafficking

86. This section summarises the good practices identified through the course of this study in project team meetings, the case studies, the analysis of the literature and the workshops in Busan in November 2017 and Marrakesh in January 2018.

These good practices are focused on improving the effectiveness of regimes to combat ML/TF from human trafficking.

87. **Assess the diverse money laundering risks from human trafficking, share with stakeholders and ensure that they're understood**: Countries can benefit from the development of a comprehensive understanding of the risk they face from the laundering of proceeds from human trafficking, which may largely be an 'unseen' crime which has led to problems in assessing its significance. Detailed research and analysis into the predicate crime – and the financial flows associated with the predicate crime – can help to further this understanding. This understanding can benefit from the development and maintenance of national and regional statistics, and other contextual information such as:

- The estimated number of victims of human trafficking, broken down by type of exploitation
- The provenance, facilitation and transit arrangements of the victims for each type of exploitation occurring in the jurisdiction
- The estimated average proceeds earned, and how they are earned, for each victim for each type of exploitation
- The organised crime groups conducting the human trafficking offences
- Prosecutions and charges for perpetrators of both human trafficking and money laundering, as well as aggregated profile information
- Typical financial flows related to each type of human trafficking in the jurisdiction's context
- Methods and indicators of laundering utilised by crime groups, and typical assets (i.e. cash, real estate, cars etc.) utilised to launder
- Whether profits stay in the jurisdiction, or are moved elsewhere

88. A review of the above can benefit from the involvement of all relevant stakeholders combatting human trafficking, as well as money laundering from human trafficking. This group of stakeholders can leverage their varied expertise and data holdings, such as case information, suspicious transaction reports and open-source information, to provide an updated view on the risk posed by human trafficking, and the proceeds of human trafficking to the country. This process can also open channels to enable more effective domestic information sharing on both the strategic and tactical levels.

89. With appropriately identified criticality to the money laundering risks from the proceeds of human trafficking, and granular knowledge of the offense and associated laundering, national authorities will be able to appropriately design mitigation measures for the risks. The below provides an example of such a comprehensive understanding of risk related to human trafficking:

Box 4. Project Tsireledzani!

Tsireledzani! means 'Protect!' in Tshi-Venda (one of the 11 South African official languages) and is the name of the Government's initiative to combat Trafficking in Persons. The programme is headed by the National Prosecuting Authority and involves government departments, international organisations and civil society partners.

This coalition of goodwill has led to the establishment of a National Action Plan on trafficking in persons and to the launch of the Tsireledzani! campaign, whose primary aim is to provide a blueprint for all those working to prevent trafficking and protect the people of South Africa and other nations from human trafficking. The program's action plan is based on three pillars: prevention, victim support and response, which provide a multi-pronged response to human trafficking, including (1) research, and (2) capacity building, which provide insight into combatting human trafficking through risk assessment and anti-money laundering measures. Project Tsireledzani!:

1. Research provides a stronger knowledge base relating to human trafficking trends and responses in South Africa upon which the Government and other stakeholders can develop national frameworks, structures, policies and processes to address human trafficking.
2. Capacity building provides support in identifying trafficked persons, improving the standard of physical protection and direct assistance offered to victims of trafficking in the country, and increases the number of trafficking cases investigated and prosecuted by law enforcement and justice officials.

Source: South Africa

90. The predicate offence of human trafficking is incredibly diverse in how it is carried out. The acts required to commit each of the types of exploitation, and the methods perpetrators use to transact differ between and within the types of exploitation. In understanding these differences, and translating them into typologies, there could be more specific opportunities to identify the criminal organisation committing these crimes and the associated laundering of the proceeds. This paper provides such a segmentation and specificity, and can act as a foundation for national authorities, reporting entities, civil society and non-profit organisations.

91. **Leverage expertise, capabilities and information through partnerships between the public sector, private sector, civil society and NPO communities:** The community of participants, working to effectively combat human trafficking, and ML/TF from human trafficking, is large and incredibly diverse, and holds significant information. This community includes a variety of stakeholders from the public sector, private sector, civil society and non-profit organisations, If participants are properly coordinated, and information is appropriately shared amongst the community of participants, some of which are not traditional partners

for FIU/law enforcement, such as labour, employment and work safety agencies, then the community's size, diversity and the information it holds offer an ability to improve effectiveness in efforts to combat ML/TF from human trafficking. It is important to consider implementing adequate mechanisms for these participants to report to FIUs, while maintaining the confidentiality of the information provided as is normally the case for reporting entities.

92. The creation of a national co-ordination and information-sharing mechanism for relevant participants working to combat human trafficking and ML/TF from human trafficking may be beneficial. Such venues are successful when they:

- Ensure there is understanding between constituents of each participant's mandate/role and capabilities;
- Understand the information each organisation holds, informational needs, and when such information can be shared;
- Ensure that there is a permanent contact point for each participant to enable information sharing across the group;
- Work collaboratively on developing the national threat and risk environment for ML/TF from human trafficking; and,
- Collaboratively develop precise, suspicious transaction report indicators and risk-based assessment guidance responsive to the national threat and risk environment.

93. Such a mechanism could be part of an existing co-ordination and information-sharing channel such as the national AML/CFT risk assessment or conducted as a continuous stand-alone process. Various 'public/private partnership' models are gaining prominence and showing tangible results worldwide, despite different national AML/CFT frameworks and information-sharing legislation in the countries enacting them. Two such models for consideration, which are operationalised under separate AML/CFT frameworks and information-sharing legislation, are Canada's Project PROTECT, and the United Kingdom's Joint Money Laundering Intelligence Task Force:

Box 5. Project PROTECT

Project PROTECT is a minimal or 'no cost' initiative between several Canadian financial institutions, FINTRAC (FIU Canada), regulators, law enforcement agencies at the municipal, provincial and federal level, as well as non-profit organisations and technology companies. The project has two twin goals: Firstly, to increase the awareness of sexual exploitation-type human trafficking amongst project constituents and secondly, to increase the quantity and quality of suspicious transaction reporting to FINTRAC when there are suspicions of money laundering from human trafficking.

Project partners utilise their unique abilities and information to fulfil the needs of other project participants through ongoing dialogue and the sharing of experience in combatting human trafficking. Tangibly, the *Project Protect* partners collectively developed indicators of suspicious transactions of money laundering from human trafficking involving sexual exploitation.

These indicators were used as sourced material for the Operational Alert to all Canadian reporting entities on human trafficking involving sexual exploitation. This Operational Alert provided granular indicators for use by reporting entities and specific instructions to submit all suspicious transaction reports for the project with the label *Project Protect* for ease of identification. The resulting suspicious transaction reports are being forwarded to project participants in law enforcement, who are then able to appropriately and expeditiously address this potential money laundering.

Since its inception, *Project Protect* has been able to make all participants, individually and jointly, more effective at combatting money laundering from human trafficking through this partnership. This is demonstrated by a nine-fold increase in suspicious transaction reports on human trafficking submitted to FINTRAC, and an eight-fold increase in disclosures sent from FINTRAC to competent law enforcement authorities resulting from the submission of these suspicious transaction reports. In addition, project participants have agreed that such a model of partnership has led to such success that it should be continued in efforts to build capabilities in combatting other serious money laundering risks.

Source: Canada

Box 6. Joint Money Laundering Intelligence Taskforce

The JMLIT model

The Joint Money Laundering Intelligence Taskforce was established in 2015 to enable both tactical and strategic intelligence sharing between law enforcement agencies and leading financial institutions in the UK.

The JMLIT brings together law enforcement, the regulator, and over 30 UK and international financial institutions to exchange and analyse information and intelligence. By using the National Crime Agency's legal gateway, the JMLIT enables private sector institutions to share information with law enforcement partners and other private sector partners on a multilateral basis.

The overall aim is to identify priorities and focus the mutual effort deployed against financial crime by the public and private sectors.

How it works

The taskforce shares information through an Operational Working Group and several Expert Working Groups.

The **Operations Group** is dedicated to assisting ongoing money laundering and terrorist financing investigations. It exchanges live tactical intelligence using the Section 7 gateway of the Crime and Courts Act 2013, strengthened and safeguarded by an information sharing agreement which all members must sign. Vetted members of 17 major financial institutions are briefed every week on UK law enforcement subjects of interest, and requests are

made for specific information to fill intelligence gaps. Information is shared for intelligence purposes only, and so all information must be parallel-evidenced by law enforcement should they wish to use it evidentially. This is an entirely voluntary arrangement which complements the UK's existing Suspicious Activity Report regime.

The bank-led **Expert Working Groups** provide a platform for members to discuss current or emerging threats, and to identify innovative ways of collectively combating these threats. These groups are attended by relevant experts from across the public and private sectors. The Experts groups are aligned to the following JMLIT priority areas:

- Organised Immigration Crime /Human Trafficking
- Bribery and Corruption
- Trade Based Money Laundering
- Money Laundering Through Markets
- Terrorist Financing
- Future Threats

Source: United Kingdom

94. Such co-ordination and information-sharing mechanisms can also be conducted with international stakeholders, including the national authorities of other countries where such co-ordination and information sharing would be beneficial.

95. These venues can also provide for the sharing of best practices through co-ordinated and sustainable, technical-assistance solutions for jurisdictions in need of assistance in improving their effectiveness in combatting money laundering from human trafficking. Some such solutions could include: the provision of assistance in conducting a national risk assessment through workshops and models, assistance in co-ordinating a public/private partnership venue, the development of specialist/generalist training programmes and the facilitation of joint investigative teams. The Bali Process provides a model for such international co-ordination, information sharing and technical assistance coordination mechanism:

Box 7. Bali Process

The Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime (Bali Process) was established in 2002 and is a voluntary and non-binding forum for regional dialogue and co-operation on people smuggling and human trafficking. It is co-chaired by the Governments of Australia and Indonesia and comprises 45 member countries from across the Asia Pacific region. Its membership also includes the United National High Commissioner for Refugees (UNHCR), the International Organisation for Migration (IOM) and the United Nations Office of Drugs and Crime (UNODC).

Under the Bali Process, the officials-level Working Group on Trafficking in

Persons (TIPWG) aims to promote more effective and co-ordinated law and justice responses to combat human trafficking in Asia Pacific by sharing information and best practices, and delivering capacity-building activities in member countries. In May 2016, the TIPWG held a Bali Process forum, *Following the Money Forum,* followed by its second annual meeting where the TIPWG agreed to progress a suite of work to promote the use of anti-money laundering and asset recovery tools to support prevention, investigation and prosecution of trafficking in persons (TIP). A key priority was the development of a new Bali Process policy guide and training module on following the money in trafficking in persons cases by a Bali Process drafting committee co-chaired by the Indonesian Attorney-General's Office and the Australian Attorney-General's Department (now the Department of Home Affairs). The guide and training module were formally endorsed at the Ad Hoc Group Senior Officials Meeting in October 2017. They will be translated into regional languages, distributed both online and in person to members, and used in training workshops for interested Bali Process countries.

The Australian Attorney-General's Department also commissioned the development of the report '*Financial Footprints: An Analysis of Financial Investigations to Combat Trafficking in Persons in the Asia Pacific Region*' to provide an overview of key global literature on the financial flows associated with trafficking in persons, and recent global experiences in using financial tools in combating trafficking in persons. Together with the Bali Process policy guide and training module on following the money, the report provides an important tool to target capacity-building activities and ensure a comprehensive and harmonised approach to using anti-money laundering and asset recovery tools in TIP cases.

Sources: Australia and Indonesia

96. **Appropriately identifying suspicious transactions linked to human trafficking and creating useful STRs**: Reporting entities and financial intelligence units may be better able to identify and report transactions where there is a suspicion of laundering the proceeds of human trafficking by considering the following:

- The financial intelligence unit can ensure that reporting entities understand the national money laundering risk associated with human trafficking and receive specific, granular indicators of the laundering of the proceeds of human trafficking
- The financial intelligence unit can guide reporting entities that reporting suspicious transactions on suspected victims are of low value. They can, in these circumstances, instead, identify victims via profiled financial transactions, and submit suspicious transaction reports on those individuals and entities to whom the victims are sending funds/assets.
- FIUs could encourage reporting entities to flag the transaction(s) with possible links to human trafficking with a specific word/phrase, tick box or

other marker when they submit their suspicious transaction report to their financial intelligence unit.

- FIUs and reporting entities could consider ways to mine open source information which provides address, phone numbers and email addresses associated with human trafficking.

97. **Raise awareness of human trafficking as a means to potentially support terrorist organisations**: Convictions for and the use of proceeds of human trafficking to materially support terrorist activity are difficult to secure for the reasons which have been enunciated in the previous section of the report, and information and credible intelligence on the issue may be difficult or impossible to collect. As a result, authorities could raise awareness about this issue to:

- Study how terrorist organisations are realizing the proceeds of human trafficking to materially support their activities. Such an understanding could include number of victims, the nature of their exploitation and the estimated material benefit derived from their exploitation. It may require a victim-based study for each territory controlled by terrorists.
- Study the financial component of human trafficking for the provision of material support to a terrorist organisation, and specifically, how the material benefit from such exploitation is used. At the time of writing this report, it is unknown if such proceeds ever leave the controlled territory of these terrorist groups, and if the proceeds are used for anything more than the sustenance and benefit of the singular terrorist engaging in such activity.

98. This information could help foster the development of appropriate AML/CFT policy and operational responses.

99. **Development of specialist and generalist training**: Authorities may wish to create and deliver training programs for individuals tasked with detecting, investigating and prosecuting ML/TF from human trafficking. Such programs will inform professionals on the use and availability of financial intelligence. Professionals can learn best practices in obtaining evidence from a variety of sources. These sources include the victims' financial documents and online sources. They will learn how to present relevant information in court and strengthen the working relationship between constituents of the regime combatting human trafficking and the ML/TF from human trafficking.

100. In addition, a leaner curriculum on financial intelligence and human trafficking can be delivered to non-specialists to ensure that national authorities can more effectively identify human trafficking and ML/TF from human trafficking, so that they can recommend and conduct appropriate actions.

101. **Other good practices**: Other good practices were identified through the course of the study (but they have also been identified through numerous other global AML/CFT regime studies on other subject matter so are not detailed in depth for the purpose of this report). These include:

- Creation of multi-agency task forces

- Focus relevant investigations on hawala-type systems and their use by facilitators in order to ensure that there is greater traceability of the financial flows of the HT
- Utilising both informal and formal international co-operation mechanisms, such as are available through asset recovery networks
- Ensuring that ML investigations operate in parallel to predicate crime investigations

Conclusion and Potential Next Steps

102. This study aimed to update our understanding of the financial flows from human trafficking. It also aimed to provide actionable ways forward for national authorities in improving their effectiveness in combatting ML/TF from the proceeds of human trafficking. While the goals of this study have been fulfilled, the study has also identified other opportunities for the global network to improve its effectiveness in the future, once time has passed and more information is available, on the following areas of work:

- Developing a better grasp of the proceeds derived from human trafficking for forced labour cases when assets are immediately identifiable;
- Developing a global estimate of proceeds derived from human trafficking for the removal of organs;
- Mapping and profiling the actors/roles involved in human trafficking for the purpose of the removal of organs, and identifying how their unique financial flows can aid in the detection of HTRO; and,
- Identifying cases of the proceeds of human trafficking contributing to terrorist activity financing to determine how proceeds are realized and used.

103. As seen in this paper, human trafficking is an offence with diverse financial flows, and where proceeds are realised differently across the world, and across the various types of human trafficking. Because of these significant differences, the findings of the international community are one aspect of what is required by national authorities to improve their effectiveness in combatting ML/TF from human trafficking. The FATF encourages all jurisdictions to better understand their ML/TF risk, share the results with relevant stakeholders, and consider implementing some the good practices identified in this report, where relevant. In addition, jurisdictions should work to better understand the challenges they have in effectively detecting, investigating and prosecuting ML/TF from human trafficking, and implement practices to overcome these challenges.

References

FATF (2011), *Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants*, FATF, Paris.

Haken, J. (2011), *Transnational Crime in the Developing World,* Global Financial Integrity, Washington DC, United States, www.gfintegrity.org/storage/gfip/documents/reports/transcrime/gfi_transnational_crime_web.pdf

Home Office, UK, *A Typology of Modern Slavery Offences in the UK*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652652/typology-modern-slavery-offences-horr93.pdf

ILO & Walk Free Foundation (2017), *The Global Estimates of Modern Slavery*, ILO, Geneva, Switzerland

ILO (2012), 2012 *Global Estimate of Forced Labour*, ILO, Geneva, Switzerland.

International Organisation for Migration, https://www.iom.int

Liberty Asia, www.libertyasia.org

MYRIA, Belgian Federal Migration Centre, 2*016, Annual Report trafficking and smuggling of human beings: Beggars in the hands of traffickers*, www.myria.be/en/publications/2016-annual-report-trafficking-and-smuggling-of-human-beings

Paraszczuk, J. (2015), 'No Other Way:' GoFundMe Effort Aims To Rescue Yazidi Women From IS, RadioFreeEurope, Radio Liberty, 18 August 2015, https://www.rferl.org/a/islamic-state-yazidi-women-rescue-effort/27195741.html;

Shimazono, Y. (2007), "Mapping Transplant Tourism," in *World Health Organizations Second Global Consultation on Human Transplantation*, Geneva 28-30 March 2007.

Thomson Reuters Foundation and European Banks Alliance, *Toolkit for Tackling Human Trafficking*, http://www.trust.org/contentAsset/raw-data/4a50dde4-0a6c-49f9-9ba4-92a8b10d3243/document

UN (2003), *United Nations Convention against Transnational Organized Crime and the Protocols Thereto (Palermo Convention)*, https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

United Nations Human Rights Council (2016), *"They came to destroy": ISIS Crimes Against the Yazidis*,Human Rights Council, A/HRC/32/CRP.S, 15 June 2016, https://www.ohchr.org/Documents/HRBodies/HRCouncil/CoISyria/A_HRC_32_CRP.2_en.pdf

United Nations University (2016), *Fighting Human Trafficking in Conflict: 10 Ideas for Action by the United Nations Security Council*, https://unu.edu/fighting-human-trafficking-in-conflict

UNODC (2016), *Global Report on Trafficking in Persons 2016*, UNODC, Vienna, Austria, https://www.unodc.org/documents/data-and-analysis/glotip/2016_Global_Report_on_Trafficking_in_Persons.pdf

US Department of State, 2015, *2015 Trafficking in Persons Report,* https://www.state.gov/j/tip/rls/tiprpt/countries/2015/243543.htm

White, L. (2015), *Isis: Yazidi families pay $20,000 ransoms to free their loved ones from Daesh slavery,* International Business Times, 18 December 2015, https://www.ibtimes.co.uk/isis-yazidi-families-pay-20000-ransoms-free-their-loved-ones-daesh-slavery-1533829

Annex A. Additional Case Studies

Human Trafficking for Sexual Exploitation

Case Study 13.

A financial institution submitted a STR on Subject A regarding financial activity occurring in Subject A's account related to possible HTSE. Subject A received an email money transfer from Subject B, who was previously reported for movement of funds and account activity indicating HTSE. Subject A's account was primarily funded by transfers from linked accounts, direct deposits, and email money transfers. Incoming email money transfers were primarily from men and outgoing email money transfers were to individuals previously unknown to the financial institution. Funds were utilised for point-of-sale transactions and included local transportation purchases and accommodation transactions.

Through the analysis of the transactions by the previously unknown individuals above, it was uncovered that they were withdrawing the funds from their personal accounts and depositing them into the accounts of 3 cash-intensive businesses to launder the proceeds of the HTSE offence.

Source: Canada

Case Study 14.

Person A was the head of a HTSE syndicate which was trafficking female victims from County X to Country Y, both located in Asia. Person A was from Country X but living in Country Y, and sought and recruited young female victims from Country X and promised them a high salary to work in Country Y. When the girls arrived in Country Y, Person A sold them to traffickers and earned USD 4,376 per Person.

To launder the proceeds of HTSE, Person A sent money to his father's bank account in Country X. To launder the proceeds from HTSE, Person A's father opened and operated a small clothing shop that had a very small customer base.

Source: Financial Footprints: An Analysis of Financial Investigations to Combat Trafficking in Persons in the Asia Pacific Region

Case Study 15.

A criminal group used legitimate business activities such as bars/night club services to cater to the needs of their clientele wanting to engage in adult entertainment. Suspects were arrested and charged after promoting and hosting what was referred to as a 'vice party' for which an entrance fee of TTD 200 (USD 30) per person was requested from patrons to contribute to forced sexual activity. The suspects were also found to be involved in promoting brothels (prostitution), child prostitution and other HT related offences.

The proceeds derived from the predicate of HT were laundered using 'legitimate' cash intensive business entities such as restaurants & bars. In some instances STR's were received indicating high value cash deposits into the accounts of the suspects. In one case an analysis of accounts held by a suspect revealed that there was an increase of cash deposits by as much as 485% over a two-year period. Funds were laundered through the accounts of third parties, payments of credit facilities and for personal expenses.

Source: Trinidad and Tobago

Case Study 16.

Investigators were asked by a local-level government to investigate possible sex trafficking in residential areas. Investigators used account tracking warrants and warrants for search and seizure of property as part of the investigation. The suspects used mobile phones registered under other people's names and changed the phones regularly. The suspects concealed the proceeds of crime by keeping the money in a bank account under a third party's name. The suspects also bought gold bars with the proceeds.

Source: Financial Footprints: An Analysis of Financial Investigations to Combat Trafficking in Persons in the Asia Pacific Region

Case Study 17.

A police investigation was conducted on an organised group profiting from sexual exploitation of foreign women in Spain. The police investigation was focused on a number of members of the organised criminal group. The different roles of the members of the criminal organisation were identified through the law enforcement investigation which acquired evidence that some members were involved in activities centred around controlling the victims, others on ensuring that they obtained money and work as required, and others focused entirely on the proceeds derived from their criminal activity.

The proceeds of HTSE were mainly in cash and operations of this network were detected through money remittance companies, highlighting the

following financial activities:

- Small amounts of money were sent abroad through money remitters by victims to their countries of origin.
- Some of the addresses in the country of destination were identical across multiple conductors.

Small amounts of money were sent at domestic level by the members of the criminal organisation and by the victims, who both reported an identical address.

Source: Spain

Case Study 18.

Young women from rural villages in West Africa are recruited to travel to Europe for a better life and to escape the economic and political hardship in their homeland. Recruiters or 'madams' use various coercion and deception tactics to consolidate the exploitative relationships. Once victims arrive at their destination in Europe, they are often bought and sold to criminal groups for sexual exploitation. Victims are also debt bonded to their traffickers for up to EUR 70 000.

Indicators for this typology include:

- Victims and 'madams' are known to use intermediaries with legitimate identification documents to facilitate the electronic transferal of funds via a money service business to Nigeria.
- Using intermediaries to allow for smurfing of funds.
- Perpetrators unable to suitably provide evidence of any legitimate income and/or struggle to prove that the money has a legal source.

Source: Nigeria

Case Study 19.

An investigation was initiated into the activities of a Romanian organised crime group who is suspected to be engaged in the trafficking of human beings into Ireland for the purposes of sexual exploitation, property crime and blackmail. Victims initially engaged with the NGO sector who reported it to An Garda Síochána through an established framework.

It is suspected that the group is engaged in using family networks and financial institutions and in some cases the victims of human trafficking for sexual exploitation are being used to traffic proceeds of crime out of the jurisdiction. At an early stage, financial investigations supported the identification and the movement of people and monies associated with this crime.

Source: Ireland

Case Study 20.

An operation was established by the An Garda Síochána to conduct an investigation into trafficking in human beings from Nigeria into Ireland for the purposes of sexual exploitation. The group is comprised of suspected offenders residing in both Ireland and the United Kingdom who engaged in the trafficking of young females from Nigeria into Ireland. Victims initially engaged with the NGO sector who reported it to An Garda Síochána through an established framework.

It is suspected that the group engaged in using family networks, financial institutions in numerous jurisdictions to move proceeds and in some cases the victims of human trafficking for sexual exploitation are being used to traffic proceeds of crime out of the jurisdiction. At an early stage, financial investigations identified and established money flows in a number of jurisdictions by submitting financial enquiries.

Source: Ireland

Case Study 21.

The Spanish police started an investigation into an organised criminal group in Spain trafficking women for sexual exploitation from Eastern Europe and South America.

The criminal organisation owned several nightclubs in the South of Spain and incorporated more than thirteen front companies to launder the proceeds obtained from human trafficking. During the police investigation the FIU received several STRs related to one of the front companies of the organisation. The suspicious transactions were mainly cash deposits below the customer identification threshold in the bank accounts of those companies. The bank accounts of the nightclubs showed mainly credit cards payments in exact amounts and a low volume of cash operations. Afterwards the money was withdrawn in cash in other regions of Spain and the operations were supported with false invoices linked to construction activities.

The exchange of information between the FIU and the investigative police unit fostered collaboration at an early stage. This resulted in the police unit leveraging FIU-disclosed information to uncover new operations and new branches of the organised criminal group conducting HTSE.

Source: Spain

Case Study 22.

In 2015, a federal jury convicted Hortencia Medeles-Arguello (aka "Tencha") of conspiracy to commit sex trafficking, conspiracy to harbour aliens, aiding and abetting money laundering, and conspiracy to commit money laundering.

The convicted defendants in this sex trafficking scheme owned, controlled, participated in, and operated bar/brothels where they charged entrance fees and sold drinks to customers. However, the conspirators mainly profited by offering young, undocumented Mexican women and girls for commercial sex at these establishments. The typical bar/brothel operated by the defendants would consist of a bar on the first floor and rooms on upper floors for customers to engage in commercial sex with the victims. The amount of money charged for a commercial sex act would vary from USD 65 for fifteen minutes to up to USD 500 per hour for illegal sex acts with minors.

The criminal organisation relied on pimps known as "padrotes" to recruit, smuggle, and supply the young women and girls, coerce them into engaging in commercial sex thereby generating proceeds for their illegal enterprise. Padrotes also rented out the bar/brothels, which generated additional income for Tencha.

The undocumented Mexican nationals "employed" at the defendants' establishments were compelled into commercial sex acts through the use of force, fraud and coercion. For example, the women and girls were placed in locked rooms to main control over them, and the defendants used violence to punish and control them.

Tencha recruited or directed family members, friends, and others to serve as employees at the bar/brothels. There were a number of co-defendants who managed the bars and had a role in moving and disguising the proceeds. Other managers provided false/fraudulent identifications (e.g., social security cards and Texas identification cards) to employees, including the females working at Las Palmas II. The bar managers paid Tencha USD 20 000 each week out of the money received from the operation of the Las Palmas I and kept all the monies received in excess of that amount.

To conceal the illegal proceeds derived from the sex trafficking enterprise, Tencha and others, including her family members, would obtain cashier's checks in amounts less than USD 10 000 (in order to avoid bank reporting requirements). One of Tencha's daughters who worked as a bartender assisted in counting the proceeds obtained from Las Palmas II. She also negotiated cashier's checks. The money used to obtain the cashier's checks came from the sex trafficking violations occurring at Las Palmas II. Tencha also held the physical property in the name of a nominee (her daughter), in order to conceal the true ownership and nature of the premises.

Tencha was sentenced to life in federal prison on 20 January 2016. A total of 13 additional defendants pleaded guilty to similar offences, including money laundering, for helping Tencha keep track of her profits, including by

investing proceeds in properties purchased by Tencha in the Houston area.

As part of the sentence, 15 real properties and other assets (valued at USD 2.5 million) were forfeited to the United States because they were acquired with the proceeds of sex trafficking. The forfeited assets have been used to make restitution to the victims of this crime. Tencha was also ordered to pay approximately USD 840 000 in restitution. Additional co-defendants were ordered to pay restitution amounts of USD 530 000, USD 570 000, USD 530 000, and USD 160 000, respectively.

Source: United States

Case Study 23.

In May 2015, Eric Omuro was sentenced to 13 months in prison following his conviction for the use of a facility of interstate commerce to facilitate prostitution. Omuro was the operator of the website myredbook.com. According to information available on that website as of the date of its seizure by the FBI, myredbook.com purported to provide "Escort, Massage, and Strip Club Reviews". Instead, however, the website hosted advertisements for sex workers, complete with explicit photos, lewd physical descriptions, menus of sexual services, hourly and nightly rates, and customer reviews of the sex workers' services.

Although the website could be accessed for free, myredbook.com charged fees for premier placement of prostitution advertisements and for "VIP Membership," which purportedly allowed customers access to "private forums" and to search reviews of the prostitution services. According to an affidavit submitted in connection with the sentencing hearing, the FBI identified more than 50 juveniles who were also advertised on myredbook.com for the purpose of prostitution. Co-defendant Annmarie Lanoce pleaded guilty to assisting Omuro with the operation of the myredbook site pursuant to a diversion program that ran into 2016. At sentencing, Omuro was ordered to forfeit more than USD 1.28 million in proceeds from his operation of the site.

Source: United States

Case Study 24.

In April 2016, law enforcement agents from Homeland Security Investigations (HSI) in El Paso, Texas, responded to a call made to local police regarding a woman who was being forcibly held by an individual identified as "Tae" at a motel. Two adult victims were discovered by officers who searched the motel room. Police located and stopped a suspect vehicle in the area and identified the driver as William "Tae" Harris. Police searched Harris and found a semi-automatic firearm. Harris was traveling with an associate, Dean Hall, and police determined that both subjects were

members of the West Side City Crips gang from Phoenix, Arizona.

The subsequent HSI investigation revealed that the victims came from Arizona with Harris and Hall. The victims were forced into prostitution and beaten and suffered threats of violence. HSI determined that at least three other West Side City Crips were operating a prostitution scheme in El Paso on the same weekend that Harris was stopped. During a forensic extraction of Harris' mobile phone, HSI discovered Bitcoin transaction data was able to exploit Harris' Bitcoin wallet information. Evidence revealed that the group's illicit activity revolved around the purchase of Vanilla Visa pre-paid credit cards, which were then used to purchase Bitcoin on the Paxful virtual currency exchange. Those Bitcoin were used to purchase prostitution ads on Backpage.com. Furthermore, during Harris' prosecution, HSI uncovered and disrupted an attempted murder-for-hire in which Harris planned to have a key witness and her sister murdered.

In January 2018, Hall and Harris were convicted and sentenced for violating several anti-trafficking statutes, including interstate transportation for prostitution, sex trafficking, felony in possession of a firearm and murder for hire.

Source: United States

Human Trafficking for Labour Exploitation

Case Study 25.

A case concerning Polish and Romanian bogus self-employed workers was opened following the findings of the Belgium's Financial Intelligence Processing Unit concerning a company's suspicious transactions. The main defendant managed a company specialising in building works. He had set up two British companies which, in turn, set up two other companies. Romanians were then employed as limited partners or associates in the structure of these last two companies. They worked mainly as subcontractors for the main company.

The Romanian workers were unaware of their roles as managers-partners of the company and were therefore employed as self-employed workers, earning EUR 8 per hour. Through this wage, the Romanian workers were required to pay social and tax contributions, as well as rent for accommodation.

Investigators used money tracking techniques to identify the perpetrators, criminal organisation elements, and to analyse the network. Over the course of this case's financial investigation, investigators queried banks and money transfer agencies, conducted wiretaps to track the defendants' investment and identify local hawala bankers and analysed the role of construction companies and accountants.

The defendants of the case were prosecuted for human trafficking for the

purpose of labour exploitation (conditions contrary to human dignity), with aggravating circumstances. The defendants were also prosecuted for participation in a criminal organisation, forgery and the use of forgeries, breaches of the income tax code, money laundering and fraud.

Source: Belgium; MYRIA: Trafficking and Smuggling of Human Beings Annual Report 2016

Case Study 26.

Three Romanian nationals, two males and one female, trafficked 22 male Romanian nationals into Europe for labour exploitation. The female offender was the partner of the male primary offender, and sister of the other offender. Economically vulnerable victims were recruited in a rural area in Romania, and were promised EUR 400 per week, to work eight hours a day, with food and accommodation provided. Upon arrival all victims had their passports taken, were required to sign a waiver to the EU working time directive, and sign transfer forms for their wages to be transferred into the primary offender's bank account. Fifteen of the victims were housed in a 3-bedroom property, sharing a single toilet and shower. They slept on mattresses on the floor. The male primary offender provided minimal food (such as a salami and two loaves between 15 people), and told the victims to eat stones if they were still hungry. He controlled them primarily through threats of violence and debt bondage. The primary offender acted as an unlicensed gangmaster, booking agricultural work for the victims at legitimate recruitment agencies for minimum wage, but then forcing them to work for over 12 hours a day for multiple agricultural businesses. These businesses were not aware of any exploitation having taken place. One victim worked for 68 hours a week and another for 18 days in a row. Frequent use of cheques was made to pay offenders and withdrawals were made rapidly after payments had been received, often from the same location. The primary offender made over EUR 1 000 a week in this way. The other male offender lived with the victims and assisted in monitoring and controlling them. As a result, he was allowed to keep his entire wage.

The exploitation was identified when four victims reported it at a police station, and identified the primary offender. The primary male offender was convicted of trafficking people and conspiracy to traffic people, and was sentenced to 2.5 years in prison. The other was convicted of conspiracy to traffic people. The female offender was given a suspended sentence of 2 years for acquiring and converting criminal property in the form of the victims' wages.

Source: United Kingdom

Case Example 27.

This case relates to slavery in Asia-Pacific waters by foreign charter vessels and is a combination of observed typologies which demonstrates the number of potential entities in multiple jurisdictions involved HTFL in the fishing industry.

To fish a particular region, fishing companies must go through a standard process to secure the appropriate licenses, vessels, crew, and quota. If a Northeast Asian based fishery wishes to fish in South Pacific waters, they contact a South Pacific local corporate to help arrange a quota and chartering agreement. In this arrangement, the local South Pacific corporate holds the quota allotment for the country's EEZ. They also own boats locally that are available for charter. In this case, the Northeast Asian based fishery contracts with the local South Pacific corporate for part of its quota and management of its fleets.

The boats and above deck crew are supplied by the local South Pacific corporate, often the same nationality of the true boat owner. However, the Northeast Asian based fishery contracts with a recruitment agency to find the below-deck crew. This agency may be legitimate, but others lie to jobseekers, deceive them, or steal their money. These crew members are often of a different nationality from the boat owner and above deck crew.

While on board, men who have lost their basic freedom suffer a series of indignities and abuse. The fish caught by these men are sent to market; processed at a fish processing factory; sold to food distributors; and moved to restaurants and grocery stores worldwide. Revenue from the sales of the slave-caught fish makes its way back to the Northeast Asian based fishing company, often in USD, processed through the international finance system.

The various parties involved all have been complicit in either directly facilitating or indirectly financially benefiting from this incidence of HTFL.

The following issues were identified:

1. **Direct -** Those financial institutions banking the entities that are directly facilitating HTFL may be at risk from handling and facilitating the proceeds of human trafficking.
2. **Indirect -** Entities indirectly involved i.e. involved in the global supply chain in purchasing/importing/exporting/using/selling goods produced from forced labour.
3. **Correspondent Banking -** Facilitating payments on behalf of financial institutions that may be directly or indirectly involved (payments between 1 and 2).
4. **US Clearing -** Handling USD clearing payments; facilitating trade payments in global supply chain for products from slavery.
5. **Exposed Industries/Players -** Fishing companies, fish processing companies, quota holders, vessel owners, vessel operators, vessel charterers, recruitment agencies, seafood markets, seafood distributors, grocery stores, restaurants.
6. **Trade Based Money Laundering -** Often, in association with incidences of HTFL,

in order to hide the use of slaves, company staff will maintain false ledgers of time sheets, take production logs (in this case catch logs), falsify shipping documents to show compliance with local laws and tariffs. Closer inspection will reveal that often the information on the documents does not match with other sources of information.

Source: Liberty Asia

Case Study 28.

The case started in 2014 after a labour union reported its concern of labour exploitation to the police. The union represents workers with little or no education. They were concerned because they suspected that several companies in the cleaning and transport industries in the Oslo area were using legal corporate structures for criminal activities and labour exploitation.

The Financial Intelligence Unit started a preliminary investigation and found that the companies and people mentioned in the report had a history of bankruptcies, and the FIU had received several reports of suspicious transactions from the bank system regarding a large amount of cash withdrawals from bank accounts. There were also several concerns about possible labour exploitation registered in the police intelligence system. An investigation team was put together with investigators from the National Criminal Investigation Service (NCIS), the National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) and the tax authorities.

An organised criminal group (OCG) operated businesses in the cleaning and transport industries. They also controlled other companies that they set up in other people's names. These companies were fronts with no actual business operations. They were created to send invoices for fictional services and to have fictional employees. The cash flows through the companies' bank accounts were controlled by the OCG. The people doing the actual work were not registered workers. They were vulnerable people whose labour was exploited, and some of them stayed in Norway only for a short period. They knew very little about how the Norwegian system works and they were followed around and "helped" by the OCG whenever they were in contact with Norwegian authorities and the banks.

Over the course of the investigation, it was revealed that the organised criminal group (OCG) was also involved in obtaining around NOK 30 million in bank loans on false premises. People in a vulnerable situation were exploited to apply for loans and the OCG falsified work contracts and pay slips that made it possible for them to be granted loans. The borrowers were not aware of how many loans were taken in their names. The funds were laundered by transferring the money back and forth between many different bank accounts before they were withdrawn in cash. While there was insufficient evidence found to pursue human trafficking for labour exploitation charge, the members of the OCG were prosecuted for tax fraud,

welfare fraud and bank fraud.

Risk indicators identified include:

- Small companies that go bankrupt within one to two years.
- Large amounts of cash being withdrawn from the companies' bank accounts or being transferred from the companies to private persons. Money received into private bank accounts is then immediately withdrawn in cash.
- Companies registered in the names of EU citizens that live outside of Norway. These EU citizens had origins from outside the EU.
- Employees who work for short periods before becoming ill and receiving welfare.
- Abuse of identities. In some cases we suspect that individuals were forced into signing applications for and taking up bank loans. In other cases people were sent from other European countries to start up a company and open bank accounts; these then sold their identities.

Source: Norway

Case Study 29.

In 2016, a major case involving labour-market crime in grocery stores brought forth charges including aggravated human trafficking, social dumping, money laundering, bank fraud, social welfare fraud, tax evasion and threats. The defendants were investigated for excessive profit from running grocery shops, which normally would not have been as profitable if the business was run legally. Financial investigation revealed that the exploitation of labour in combination with unreported profit to IRS led to considerable illegal profits which were being used to reinvest in businesses.

The prosecutor has submitted confiscation claims totalling NOK 103 million and restraining orders amounting to about NOK 100 million on various properties to secure the confiscation claims against the defendants. As this is a very complex case, a judgement from the district court is expected in 2018.

Source: Norway

Case Study 30.

A male Vietnamese national trafficked at least three other Vietnamese nationals (two adult women and a 16 year-old boy) to work at his nail bar in Europe. The child had been transported to Europe from Vietnam through a long series of different transportation methods which were paid for by the trafficker, and had no idea what country he was in. The victims were housed in the offender's residence in a private housing estate. By opening bank accounts for the victims the trafficker acted as custodian, despite the fact that he was not related to any of the victims. Some of the victims were controlled

through debt bondage, and were paid only small or irregular amounts for their work for the offender in the nail bar; they were also forced to undertake domestic work for him. None of the victims' accounts showed evidence of payment of taxes or of other payments to a regulatory body typically associated with legitimate full-time employment of workers. They relied on the offender for their basic accommodation and food. Some victims had been in this situation for over a year. The child only received 'pocket money' for being a 'trainee' at the bar. As part of a larger operation, the police visited the offender's nail bar, and recovered the child victim, as well as gaining evidence of exploitation. They obtained a search warrant for the nail bar and the offender's residence, recovered the two female adult victims and arrested the offender. The offender was found guilty of Human Trafficking.

Source: United Kingdom

Case Study 31.

A man kept his wife in domestic servitude for two years. The victim was well-educated and from a relatively affluent family. The arranged marriage took place in Pakistan. When the victim arrived in the host country her husband reportedly told her that her only purpose was to look after him and his mother, who had ill health. The victim cooked, cleaned and did household chores for her husband and mother-in-law. She often worked 19 hour days and was unpaid, only being given £10 a month to top up her mobile phone. Her husband controlled her through a combination of fear, mental abuse and repeated physical violence. She was not allowed to leave the house unaccompanied or to make friends. In February 2014, the offender was taken into police custody after he was spotted pulling the victim back into the house by her hair. She was found to have a black eye and a broken nose, requiring surgery. The victim then signed a document asking for the offender's release, stating that she was not acting under pressure. The exploitation continued for 18 months, until the victim attempted suicide by taking an overdose of painkillers. She was taken to her brother-in-law's house for safe-keeping, and there notified the police of her exploitation by calling 999. This led to an 18-month investigation, which culminated in the offender being sentenced to two years.

This case highlights the difficulty in determining the material benefit gained through certain types of HTFL where the proceeds are indirect, gradual enrichment, or enrichment of an individual's lifestyle, but are not are realised in a singular material good.

Source: United Kingdom

Case Study 32.

A 13 year-old Romanian girl was trafficked to Western Europe by an organised crime group to undertake forced begging. Her father paid the gang 200 euros for this. She was driven to Spain and then flown to other Western European capitals, accompanied by one male offender. The victim used her own Romanian identity card to travel, but her flights were paid for by the offenders using a stolen USA credit card. The victim was placed with a male and female offender, and was instructed to call them 'aunt' and 'uncle'. The victim was driven by one offender 40 miles to another town, 5 days a week, where she was made to beg and sell unofficial copies of a charity magazine outside the entrance to a Post Office for over 7 hours a day. She was beaten and searched at the end of each day, and was not allowed to keep any of the money she had made. The offenders, who had no legitimate explanation for the repeated low value deposits, wired the money to Romania as soon as it was in their account.

The victim was poorly fed and clothed, and this was noticed by members of the public. She was also exploited for domestic servitude by the offenders, looking after their children. The victim was identified by the police during a raid following a large-scale investigation by the police into the trafficking of Romanian nationals to other European countries by an organised crime group for the purposes of forced criminality. She was placed into social services, and then returned to her mother in Romania. The victim gave evidence against her father and three other offenders who were convicted for trafficking a child for forced criminal exploitation. The father was sentenced to four years, served two, and then returned to his family (including the victim) in Romania.

Source: United Kingdom

Case Study 33.

Between October 2015 and January 2017, two Bulgarian men brought at least nine other Bulgarian individuals to Sweden with promises of construction or other jobs. The organisers' *modus operandi* was to target economically vulnerable individuals in Bulgaria, paying for their transportation to Sweden in order to put them in their debt. However, once the latter had arrived, it became clear that there were no jobs, and they were forced to beg on the streets (in Sweden, begging is not illegal). The two organisers made the nine individuals pay for transportation, food, housing (in dilapidated property) and for the "right" to beg in particular spots, collecting and keeping detailed accounts of the money from each person by the end of each day. The two men were apprehended in January 2017 and were later charged with trafficking and aggravated money laundering offences.

On a typical day, a beggar would earn about SEK 300 (~ EUR 30). The two organisers would collect the money, keeping detailed records of the beggars' earnings and of how much remained of their debt. The organisers would keep half of the earnings for themselves as payment for the "right" to beg in a particular spot, and deduct expenses as well as debt payments from the other half. During 2016 alone, the bank account of one of the organisers received cash deposits of about SEK 135 000. Funds from that account were transferred to other accounts or sent to relatives of the organisers (but not of the beggars) in Bulgaria via money transfer services.

In the prosecutor's estimation, 38 persons in total, over different periods in time, could have been forced to beg. The seized bookkeeping belonging to the two organisers, combined with other forms of evidence, suggest a grand total of about SEK 1 270 000 collected through begging during 2016.

In November 2017, the two men were convicted of the trafficking offence and were sentenced to 4 years and 2 months in prison followed by deportation. Just under SEK 120 000, an amount roughly equivalent to the recorded earnings of the beggars who were parties in this case, was confiscated in order to be returned to the beggars. A further SEK 340 000 SEK was awarded to the beggars in damages. The verdict has been appealed.

Source: Sweden

Case Study 34.

On December 18, 2017, two defendants plead guilty to an alien harbouring scheme involving labour exploitation at a Nebraska motel. According to documents filed in court, the defendants admitted to conspiring to harbour the victim, an Indian national who lacked immigration status, at a Motel in Kimball, Nebraska, between October 2011 and February 2013. During that time, the defendants required the victim to work long hours, seven days a week at the motel, performing manual labour, including cleaning rooms, shovelling snow, and doing laundry. Although the defendants promised to pay the victim, they never did, but rather claimed to apply that amount to a debt the victim owed. The defendants further restricted the victim's movement, isolated him, and verbally abused him.

The defendants face a possible sentence of up to 18 months in prison according to their plea agreements, and they are expected to be removed from the United States at the completion of their sentences. The defendants also paid the victim USD 40 000 in restitution at the change of plea hearing as a condition of their guilty pleas.

Source: United States

Case Study 35.

In 2015, two Ukrainian nationals were found guilty of conspiracy to participate in a racketeering enterprise in connection with a human trafficking scheme. The defendants, who were brothers, operated a human-trafficking organisation, the Botsvynyuk Organisation, for seven years which smuggled young Ukrainians into the United States and then forced them to work for little or no pay. The defendants promised the victims that they would earn USD 500 per month with free room and board by working for their organisation. In reality, they smuggled the migrant workers into the United States and put them to work as cleaners in retail stores, private homes, and office buildings—but did not pay them. The defendants used physical force, threats of force, sexual assault, and debt bondage to keep the victims in involuntary servitude. Even after some of the victims escaped, the defendants continued with their extortionist activities in order to recoup the organization's investment in the workers.

The Botsvynyuk Organisation also engaged in visa fraud by bringing the victims to the United States legally using tourist visas to travel first to Mexico and then coaching the workers on how to enter the United States illegally. While some of the victims successfully gained entry into the United States, others were taken into custody by US immigration officials, where they remained in detention for almost two months. Once the victims were released from US custody, with immigration documents and summonses to appear for immigration hearings, the Botsvynyuk Organisation transported them to Philadelphia, Pennsylvania, either by bus or by plane. The brothers then confiscated the immigration documents and summonses from the workers and put them to work cleaning large chain stores at night. Other members of the organisation would wire money to smugglers in Mexico and the United States to finance the journeys of the victims.

Omelyan Botsvynyuk was sentenced to life in prison plus twenty years and was ordered to pay restitution in the amount of USD 288 272.29; Stepan Botsvynyuk was sentenced to twenty years in prison and was ordered to pay restitution in the amount of USD 288 272.28.

Source: United States

Annex B. Indicators of Laundering the Proceeds of Human Trafficking

There are four considerations to note with respect to the indicators of laundering the proceeds of human trafficking identified in this study:

1. The indicators have been positioned to best identify those who are laundering the proceeds of human trafficking. From the cases that have been identified, the most unique and identifiable indicators of money laundering occur at the level of the victim, or at the lower level of criminality or individual criminals levels of the criminal organisation. The money laundering mechanisms utilised at the higher levels of the criminal organisation are already well identified in other, more general, money laundering typologies documents. This may make the indicators case studies have identified solely 'small time', lower value or local human trafficking networks. However, they are positioned deliberately in this manner to prioritise the ability to identify money laundering uniquely from human trafficking.
2. This study organises the indicators according to the three types of exploitation identified earlier in this study. These three classifications have identified unique indicators, and the granular ability to identify each will be helpful to reporting entities and operational authorities.
3. The identification of victims is one of the most reliable ways, when there is interaction with the financial system, to identify laundering the proceeds of human trafficking. This is particularly prescient for HTSE and HTFL when victims endure an extended period of exploitation under which perpetrators profit, whereas HTRO allows comparatively little opportunity to identify victims given that their exploitation, albeit horrible, is relegated to a singular experience. Reporting entities must take care that when identifying victims, they must either use the transactions of the victims to identify the perpetrators and launderers related to human trafficking, or to clearly identify to national authorities when they are reporting on suspected human trafficking victims.
4. Some indicators identified in the cases submitted to the study, and other material that was used to create this paper, are indicators that can be utilised to detect money laundering specifically from human trafficking. Other indicators demonstrated in the materials, which are indicators of general money laundering, have been identified by the global AML/CFT community previous to this study. These common money laundering indicators have been provided in a separate section below to be used in conjunction with the unique indicators of laundering the proceeds of human trafficking to provide reporting entities with national authorities with an enhanced ability to detect, using them in conjunction with each other.

Indicators of money laundering related to human trafficking

Indicators of money laundering of the proceeds of all types of human trafficking

- Common mobile number, address and employment reference being used to open multiple bank accounts in different names
- Customer makes deposits/withdrawals or otherwise generally operates an account accompanied by an escort, handler or translator (who may hold the customer's ID)
- High and/or frequent expenditure at airports, ports, other transport hubs or overseas, inconsistent with customer's personal use or stated business activity
- Income received and immediately withdrawn in cash
- Newly-opened customer account appears to be controlled by a third party, including forms completed in different handwriting and/or the customer reads their address from a form
- Payments to logistics, airlines, coach companies, car rental or travel agents inconsistent with customer's personal use or stated business activity
- Relatively high or recurrent expenditure on items inconsistent with customer's personal use or stated business activity, such as food, necessities, or accommodation for workers

Indicators of money laundering related to human trafficking for sexual exploitation

Indicators of money laundering unique to human trafficking for sexual exploitation

- Account holder contact information linked via open sources to advertising related to escort services
- Account is funded primarily via cash deposits and funds transfers from other individuals
- Addition of an unusual number of unrelated individuals as joint account holders, or authorised users of products such as credit cards
- Cash deposits conducted at different cities across the country
- Client makes deposits accompanied or watched by a third party who may, on separate occasions, accompany or watch clients who are making deposits: the third party may be handing over to the client what is subsequently confirmed to be the client's identification
- Credit card payments for purchases made after the establishments' normal hours of business (e.g. strip clubs, massage parlours, beauty salons, model agencies)
- Deposits conducted in one city followed by same-day or next-day withdrawal and/or purchases conducted in another city

- Frequent cash deposits made via an ATM rather than with a cashier, sometimes followed by ATM withdrawals in a different location
- Frequent low-value payments to advertisers, classified services involved in the sex industry or to escort agencies
- Frequent purchases in multiples of small amounts of Bitcoin or virtual currencies, directly by the client or through exchanges
- Funds transfers involving third parties with alternative names provided in brackets
- Hotel transactions by the same individual for two separate rooms for the same dates
- Identical address reported by numerous, seemingly unrelated, individuals
- Media coverage of account holder's activities relating to human trafficking in the sex trade and/or prostitution rings
- Multiple accounts making repeated transfers to the same third party, or multiple individuals reporting similar information (i.e. address, phone number etc.)
- Multiple low value remittances to jurisdictions known to be of a higher risk for HTSE
- Outbound international funds transfers directed to countries at higher risk for human trafficking or between two countries/areas on a known trafficking route
- Outbound international wire transfer in an amount commonly associated with a subscription or payment fee (i.e. 9.99 or 29.95) to a jurisdiction of concern for human trafficking, to a company with a name denoting its involvement in the provision of sexual services, or to a company with a name denoting involvement in the video industry between the hours of 10pm – 4am local time
- Payments to hotels, serviced apartments and other accommodation inconsistent with customer's personal use or stated business activity
- Personal account activity inconsistent with expectations involving frequent deposits and payments through an online payment service in small amounts typically under USD 100; account funds may then be used for virtual currency deposits/redemptions, or payment of bills, such as personal or third-party credit cards
- Recurring payment for transportation or logistics services in the late night or early morning
- Significant payment for transportation or logistics (car rental, taxi, and/or ride sharing service transactions)
- The use of cash intensive legitimate businesses (bars, restaurants, guest houses, etc.) for apparent daily sustenance

- Transactions conducted in an area suspected to be a sex trafficking location (possible 'hot spot')
- Transactions with classified advertising services involved in the sex industry or to escort agencies
- Use of a third party to execute transactions (for example, under the pretext of requiring an interpreter)
- Use of addresses where prostitution is reported to occur by media, law enforcement, or classified ads
- Use of aliases for the purpose of opening multiple accounts in different banks, or in different branches of the same bank
- Use of someone else's identification, or opening an account in the name of an unqualified minor

Indicators of money laundering related to human trafficking for forced labour

Indicators of money laundering unique to human trafficking for forced labour

- A high percentage of income withdrawn quickly after receipt in the accounts
- A property, when looked at on Google Street View, could only comfortably accommodate two or three people at the most, but seems to have more people living there
- Analysis of ATM activity shows that their ATM usage often occurred at the same machine at the same time suggesting that a third party is in control of their cards
- Customer displaying a poor standard of dress and personal hygiene
- Lack of living expenses such as food, petrol, utilities and rent (one utility may be set up for the purposes of confirming ID for account opening)
- No evidence of payment of taxes or of other payments to a tax authority or other government or regulatory body typically associated with legitimate full-time employment of workers
- One-way flight purchase from high-risk country by non-family member
- Payment for visa by non-family member
- Payments to labour agencies, recruiters or employment websites, especially if those entities are based overseas
- Personnel numbers and costs, if known through the provision of information by the entity, is not in line with wages paid out, or what you know of the entity
- Repeated (at least weekly) transfers of funds to the same third party (where known), often in round amounts
- Reports or indication of cheap labour or unfair business practices towards an entity

- Signs of bruising or other physical abuse on customer
- The customers receive weekly incomes from an agency
- Use of an interpreter at account opening or for conducting transactions

Indicators of money laundering identified in suspected human trafficking cases which common across different predicate crimes

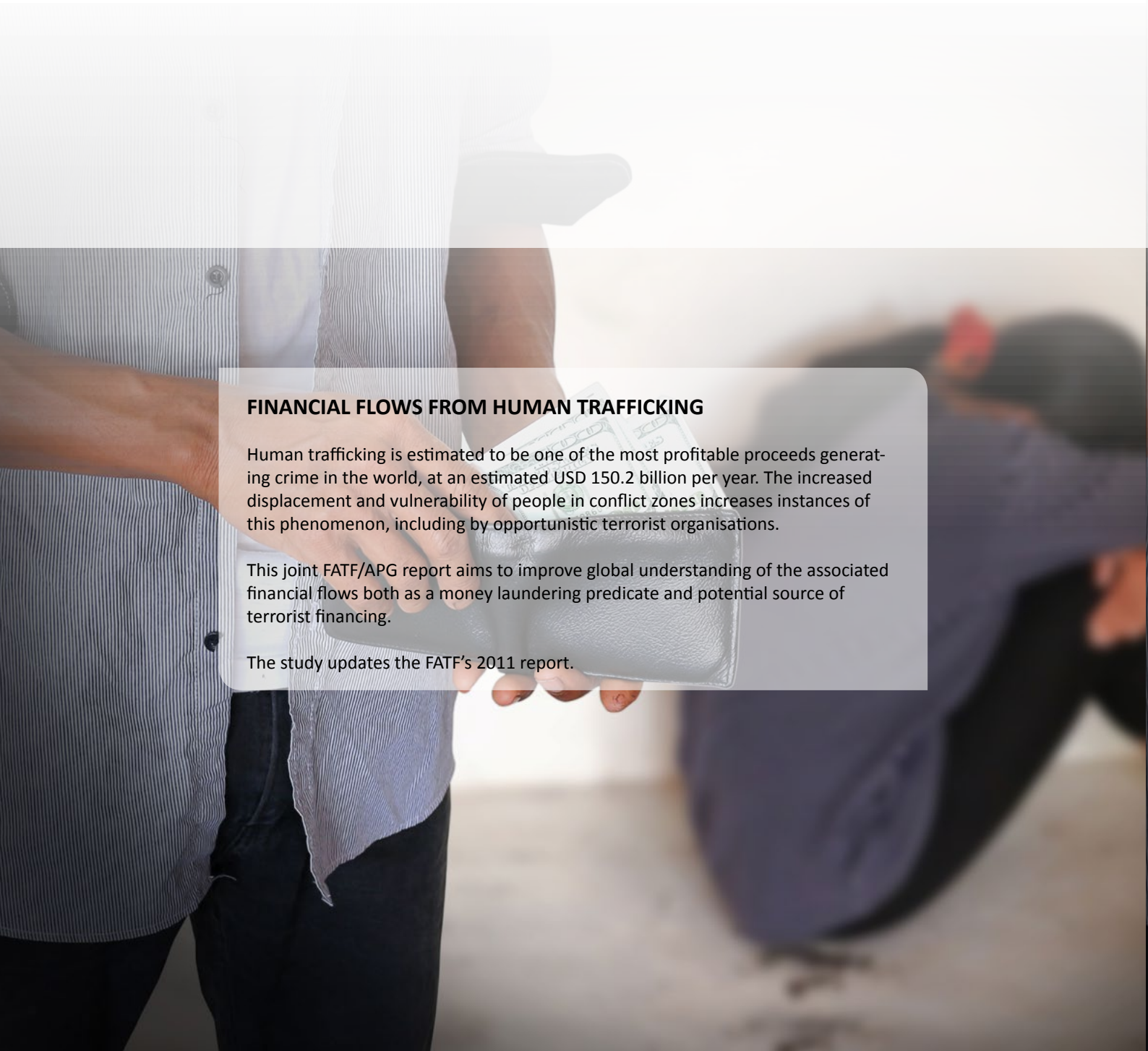
- Account appears to function as a funnel account
- Cash-intensive business with unclear source of cash or capital
- Commercial entity's capital consists of no-term deposits
- Cross-border transfers of funds to the same individual, financial institution or to an overseas location that are inconsistent with customers' personal profile or stated business activity
- Customer accounts which display unusual withdrawal patterns, such as lump sum withdrawals
- Customer requesting direct payment in a branch, as they have not been receiving their wages
- Customer's accounts display unusual deposit or withdrawal patterns, in other regions and overseas
- Deposits and/or other transactions inconsistent with what could be reasonably expected for the customer's personal profile and/or stated occupation
- Deposits much larger than are usual or reasonably expected for the customer's personal profile and/or stated occupation
- Frequent low-value/below threshold cash deposits in low-denomination bank notes
- Funds transfers received from or to the benefit of unrelated third parties
- Inability to contact client at their reported phone number, or the phone number changes very frequently
- Income received and immediately withdrawn in cash
- Incurring and payment of credit facilities or credit card charges not commensurate with the client's confirmed wealth
- Large cash deposits into an account quickly followed by electronic funds transfers, bank draft purchases and/or the issuance of cheques
- Large cash or cheque deposits followed by domestic wire transfers or cash withdrawals
- Loans provided by a shareholder to the related legal person and subsequent transfer back of funds
- Media or other reliable sources suggest that a client may be linked to criminal activity which could generate proceeds of crime

- Multiple deposits from varying geographies and apparent different individuals, consistent with smurfing
- Numerous personal cheques deposited into business accounts for no apparent purpose
- Numerous transfers into business accounts from personal accounts
- Profits or deposits much larger than are usual or reasonably expected for the customer's size or type of business, or where financial turnover is incommensurate with the commercial turnover usual for a business of that size or type
- Purchase of commodities in manners inconsistent with normal business practice
- Rapid transfers of funds through accounts
- Small irregular payments from the same account
- Source of funds used for transactions is unknown
- Structuring via commercial entities and transfer of money using loan contracts
- Transactions with apparent front, shell or shelf companies
- Use of a third party, with no apparent relationship to client, to conduct financial transactions
- Use of third-party accounts

Annex C. National actions to consider to ensure an effective system in combatting money laundering/terrorist financing from human trafficking

The following is an abridged version of the good practices identified in the FATF's 2018 *Financial Flows from Human Trafficking* report. National authorities may wish to consider adopting some of these practices to improve the effectiveness of their efforts to combat money laundering and terrorist financing from human trafficking.

Develop Understanding of Risks of ML/TF from Human Trafficking	• National regime creates an inclusive partnership with the private sector and civil society to ensure that all threat and risk information is available to those that need it, within the bounds of national privacy laws. • National regime conducts a granular assessment of the risks of ML/TF from human trafficking, reflecting the diverse types of human trafficking exploitation.
National Coordination to Combat ML/TF from Human Trafficking	• A national action plan to combat the identified ML/TF risks from human trafficking sets out responsibilities and commitments of public stakeholders, and private sector/civil society actors (where relevant). • Training is provided to specialists combatting ML/TF from HT – abridged training available for generalists who may be implicated.
Information is Shared Across all Relevant Stakeholders Combatting ML/TF from Human Trafficking	• Strategic perspective of human trafficking in national context and assessment of ML/TF risks shared with all relevant stakeholders. • Country-specific indicators of ML/TF from human trafficking developed and shared among public/private/civil society sectors. • Open source information is used to identify potential cases of ML/TF from human trafficking in a coordinated manner. • National authorities share information across the regime.
Information is Readily Identifiable to Authorities Combatting ML/TF from Human Trafficking	• The private sector submits STRs on those laundering the proceeds of human trafficking, even when the victims of human trafficking may display the financial flows most unique to human trafficking. • Suspicious transaction reports identifying potential ML/TF from human trafficking are appropriately identified via tick box or textual indicator.
Law Enforcement Authorities Working in a Coordinated Manner	• Law enforcement conducts a parallel money laundering investigation to human trafficking investigations. • Multi-agency task forces are used to coordinate enforcement and intelligence resources to combat ML/TF from human trafficking.
Leverage International Information and Good Practices	• Informal assistance channels are used early in investigations, and responses are provided to formal and informal assistance requests with expediency. • Good practices from counterparts and international organisations are considered for implementation into national regime. • Technical assistance is provided in a coordinated and sustainable manner.



FINANCIAL FLOWS FROM HUMAN TRAFFICKING

Human trafficking is estimated to be one of the most profitable proceeds generating crime in the world, at an estimated USD 150.2 billion per year. The increased displacement and vulnerability of people in conflict zones increases instances of this phenomenon, including by opportunistic terrorist organisations.

This joint FATF/APG report aims to improve global understanding of the associated financial flows both as a money laundering predicate and potential source of terrorist financing.

The study updates the FATF's 2011 report.

Appendix LL:

FATF, *FATF Report: Money Laundering Through the Physical Transportation of Cash* (Paris: FATF, 2015)

FATF

MENAFATF
مينافاتف
GAFIMOAN

FATF REPORT

Money Laundering Through the Physical Transportation of Cash

October 2015

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

For more information about the Middle East & North Africa Financial Action Task Force (MENAFATF), please visit **www.menafatf.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF and MENAFATF (2015), *Money Laundering through the Physical Transportation of Cash* , FATF, Paris, France and MENAFATF, Manama, Bahrain,
www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html

TABLE OF CONTENTS

ACRONYMS

AML	Anti-money laundering
BCS	Bulk cash smuggling
BNI	Bearer negotiable instruments
CDD	Customer due diligence
CFT	Countering the financing of terrorism
CVIT	Cash/Valuables in Transit
EC	European Commission
ECB	European Central Bank
FSRBs	FATF-Style Regional Bodies
GAFILAT	Financial Action Task Force of Latin America
IMF	International Monetary Fund
MENAFATF	Middle East and North Africa Financial Action Task Force
MSB	Money service business
UNODC	United Nations Office on Drugs and Crime
UPU	Universal Postal Union
WCO	World Customs Organization

EXECUTIVE SUMMARY

Despite the increasing prevalence of non-cash payment methods in developed economies, cash remains an important means of settlement across the globe, with an estimated USD 4 trillion in circulation and between 46% and 82% of all transactions in all countries being conducted in cash.

Similarly, cash is still widely used in the criminal economy and it remains the raw material of most criminal activity. In many cases, even when the proceeds of a crime are initially generated in electronic form (such as the theft of funds from a bank account), criminals choose to withdraw the funds from a bank account in cash, transport it to another country, and pay it into another account in order to break an audit trail. The physical transportation of cash across an international border is one of the oldest and most basic forms of money laundering[1], but this report shows that it is still widespread today. There are no fully reliable estimates for the amount of cash laundered in this way, but the figure would seem to be between hundreds of billions and a trillion US dollars per year. The majority of countries surveyed during the compilation of this report were of the opinion that cash smuggling is an increasing problem.

Physical transportation of cash as a method of money laundering is not restricted to a particular type of crime. Although many jurisdictions report the use of this typology by drug trafficking organisations, it is also linked to the illegal trafficking of other commodities, such as alcohol and tobacco, and it is also used widely by criminals involved in other activity including tax fraud, weapons and arms smuggling, organised immigration crime and the financing of terrorism. There are no cash smuggling methods more associated to one form of criminality than another, and no guarantee that criminals committing the same type of crime will move their proceeds in the same way and by the same route.

Instead, the methods used to physically transport criminal cash are dependent on a decision making process undertaken by the criminal. This process begins with the criminal deciding what the purpose of the cash movement is (for example, to break the audit trail, to pay a supplier, to bank it in another jurisdiction etc.). This will dictate the ultimate destination, which will in turn inform the method used, and ultimately the route chosen. At all stages, influences such as risk, familiarity, simplicity and the demands of partners will affect the decisions made. Understanding the decision making process can assist in developing control techniques by authorities tasked with combatting the problem.

Once the cash has been moved to its destination and used for its intended purpose it will eventually enter the legitimate financial system and will be recycled by banks and other financial institutions. Countries that use their own unique currency have the opportunity to monitor the repatriation of their currency from overseas, and while this is by no means straightforward, proper analysis can in some cases identify high risk routes, money laundering networks and drive national programs to raise awareness of risk.

[1] Techniques which can be used for money laundering, can also be used for terrorist financing (see Box 31), so the report is also of interest for combating terrorist financing.

Key findings:

Notwithstanding the influence of criminal decision making on the methods used, some common features and trends emerge from the study of the information gathered during the compilation of this report.

- The use of physical transportation of cash distances the criminal proceeds from the predicate offence that generated them, and breaks audit trails.
- The amounts of cash being concealed in cargo and adapted freight being far in excess of what can be carried by a natural person.
- The currencies most frequently encountered in consignments of criminal cash – the US dollar, the euro, the British pound, the Swiss franc, etc. – are the most stable, widely used and readily traded in the world
- Although by no means universally seen, high-denomination notes are often used to reduce the bulk and weight of criminal cash when concealment of the cash is a prerequisite to smuggling it
- Criminals exploit mechanisms of cash declaration systems, particularly as a method of lending a veneer of legitimacy to criminal cash introduced into the legitimate financial system
- Because of the legitimate demand for cash, it is moved in huge quantities on a daily basis across the world, by natural persons (whether carried on their person, in their personal effects, or in a vehicle), in cargo and mail. However it appears that although most countries have a reasonable knowledge and understanding of transportation of cash by natural persons and have comprehensive measures in place to monitor and control this issue, substantially less have any appreciation of the legitimate movement of cash in cargo and mail, and pay little attention to this phenomenon despite the amounts moved in cargo being much larger than those being moved by natural persons. A possible reason for this lack of knowledge is that although FATF Recommendation 32 sets standards for the control of physical cross-border transportation of cash by natural persons, cargo and mail, its focus on 'natural persons' may help explain why many jurisdictions seem to consider that their obligations under this recommendation to be limited to having in place a disclosure or a declaration system for transportation of cash by natural persons only.

  When transported in cargo, cash is treated as a form of goods and in most cases only a basic customs declaration is required – most countries do not require a specific cash declaration in addition to the normal customs declaration. The amount of detail required on this declaration is minimal – not even the actual value of the cash is required – which means that, in most cases, there will be insufficient information available to customs to form a view on whether the shipment is suspicious or not. Some countries noted that this absence of ability to form a suspicion restricted the ability of their

customs authorities to open and inspect shipments, require the provision of further information and exercise effective control of cash in cargo.

These factors can significantly hamper efforts to identify consignments of criminally derived cash. There are indications from research carried out by some countries that criminal groups have become aware of this and seek to infiltrate large amounts of cash into the legitimate system used by banks and other financial institutions to transport cash traded between themselves, effectively hiding it in plain sight.

Every physical transportation of cash across international borders involves at least two countries, and most of those surveyed raised the importance of effective international co-operation in controlling the phenomenon. Countries need to make every effort to share information and intelligence and facilitate the gathering of evidence by international partners in order to ensure that efforts to combat money laundering are not hampered unnecessarily. Similarly, in many countries several agencies need to work together to control borders and it is of paramount importance that these agencies are not hindered by issues such as poor communication and co-ordination of resources.

1. THE SCOPE AND EXTENT OF THE PROJECT

1.1 THE BACKGROUND TO THE PROJECT

Cash remains a significant raw material for criminal groups and is used by choice as an anonymous financial instrument by a wide range of criminals, even in complex money laundering systems.

Physical transportation of cash (i.e. bulk cash smuggling (BCS) and cash couriers) as a means of money laundering continues to be a problem in many countries worldwide. It is an issue that concerns both developing countries with cash based economies as well as countries with developed and sophisticated financial systems. Despite there being an incomplete understanding of the issue globally, responses to the questionnaires imply that the increasing robustness of Anti Money Laundering (AML) regimes in the financial sector has led to the increasing prevalence of physical transportation of cash as an alternative method to move the proceeds of crime and ensure its security by keeping it away from the traditional financial system. Criminals who need to make use of their ill-gotten gains are looking for options as more preventive measures are implemented by the traditional financial sector.

Having adequate measures in place to detect and prevent illicit cross-border transportation of cash and bearer negotiable instruments (BNIs) is a requirement of all countries. It is covered by Recommendation 32 of the FATF standards[2], and the associated interpretive note, which defines physical cross-border transportation as '… any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation:

- physical transportation by a natural person, or in that person's accompanying luggage or vehicle;
- shipment of currency or BNIs through containerised cargo or
- the mailing of currency or BNIs by a natural or legal person.'

To date, there has been no global study and typology report issued by FATF dedicated to BCS and cash couriers. However, the issue of BCS and cash couriers has been referred to in a number of FATF typologies reports in addition to the FATF international best practices paper *Detecting and Preventing the Illicit Cross-border Transportation of Cash and Bearer Negotiable Instruments*, published in February 2010. The issue of physical transportation of cash has also been referred to in some studies conducted by FATF-style regional bodies (FSRBs) and the Egmont Group. This paper is intended to complement, not replace, the 2010 FATF best practices paper. While the 2010 paper sets out a range of policy responses, this paper is intended to develop the knowledge base about the methods and trends used by criminals to smuggle cash to further inform policy work in this area.

[2] The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

The project was proposed by the Middle East and North Africa Financial Action Task Force (MENAFATF) secretariat and the Netherlands authorities and adopted by the FATF in October 2013. The UK volunteered to co-chair with Tunisia. The project was the subject of discussion at the joint experts meeting in Doha, Qatar in December 2013. The project team meetings were very well attended, with as many as 70 delegates attending and contributing and presentations were delivered by the Financial Action Task Force of Latin America[3] (GAFILAT), the Kingdom of Saudi Arabia, Lebanon, MENAFATF, the Netherlands, the State of Qatar, the World Customs Organization (WCO), the UK and the USA.

Interest in, and collaboration with the project remained strong throughout 2014 with in excess of 60 countries contributing information and case examples in response to a questionnaire devised by the co-chairs and issued by the FATF secretariat in March 2014. As recently as October 2014 the UAE requested to join the project team, and the typology was further discussed, and additional presentations and case examples presented over two days at the Typology Workshop jointly held by MENAFATF and EAG in Doha in December 2014.

1.2 THE OBJECTIVES OF THE PROJECT

The main aim of the project is to fill the knowledge gap identified by the FATF in course of the review of the work done , and to explore and understand the extent, scope and operating models of using physical transportation of cash in ML schemes[4] to provide a basis for identification of policy implications that may ultimately help in the effort to improve its prevention, detection and disruption.

- In order to achieve that goal, the key objectives of this project are the following:
- To develop an understanding of the scope and extent of the problem of the physical transportation of cash on a global and regional level through data collection and reviewing of existing literature.
- To identify trends, methods and techniques used for ML through physical transportation of cash and provide a compilation of case examples.
- To identify the main challenges and problems faced in the detection and disruption of physical transportation of cash.
- To compile a set of red flags and/or indicators and any other information that might be used later for developing best practices on preventing, detecting and disrupting ML through physical transportation of cash.

1.3 THE PREVALENCE OF THE USE OF CASH

The definition of ‘cash’ in the Oxford English Dictionary is ‘money in coins or notes, as distinct from cheques, money orders or credit’. The Oxford American Dictionary further qualifies the definition as

[3] Formerly known as the *Financial Action Task Force of South America (GAFISUD).*

[4] And also terrorism financing (TF) schemes.

'money in any form especially that which is immediately available'. Dictionaries in other widely spoken languages, such as Spanish, Mandarin and Arabic, give very similar definitions.

The concept of cash has existed for millennia. It was the original type of money which was in existence long before the advent of the modern banks and other financial institutions which have become an integral and indispensable part of modern life. Yet despite the proliferation of such financial institutions, cash is still the preferred method of settlement for goods and services for billions of people in the world today. There are many reasons for this. Not the least of these is the fact that there are still 2 billion adults in the world today who do not have access to banking services[5]. For these people, cash is still the only thing that they can use to procure the goods and services that they need to live their lives day to day. It is no coincidence that many of the poorest and least developed countries of the world have economies that are predominantly cash based.

However cash is still prevalent as a method of payment in many of the world's biggest economies. This infers that there are factors other than ease of access to financial services that influence the preference to use cash rather than more advanced instruments, such as cheques, credit and debit cards to settle transactions.

These factors include;

- **Cultural issues.** In some countries, the bulk of the population are inherently mistrustful of any form of officialdom, such as governments and large financial institutions. They feel the need to conduct their day-to-day activities, including financial activities, with a minimum of official scrutiny. They may also wish to hide the value and location of their assets from the government, perhaps for tax purposes. In these countries cash is seen as an anonymous instrument which facilitates these needs.
- **Cash is widely accepted**. Numerous studies[6] have demonstrated that, in most countries, even those with highly developed financial systems, cash is the preferred method of payment for low value transactions. Very few retail outlets in the world that sell day to day items such as food or clothing will refuse to accept cash, and most AML regimes recognise this when dictating *de-minimis* levels for suspicious transaction reporting.
- **Cash is quicker**. A cash transaction is conducted in real time and payment is received immediately. Transactions through the banking system can take days, weeks or months depending on a host of variables such as delays in clearance, non-banking days, credit terms etc.
- **Cash reduces spending**. Academic studies[7] suggest that persons purchasing goods and services with cash tend to spend less money overall as they are more 'connected' with the transactions they are undertaking. These studies find that the use of debit and credit cards has the effect of

5 World Bank (2015).

6 Bagnal, J., Bounie, D. et al (2014)

7 For example: Knouse, K.C. (1996).

making a transaction feel less 'real', meaning that the holder of the card is less likely to budget effectively.

- **Cash reduces indebtedness**. Persons who transact only in cash can only spend money that they actually possess, as opposed to persons who use debit and credit cards, which can result bank overdrafts and credit card bills.
- **Discounted Goods**. In many countries it is possible to negotiate a lower price when paying for goods and services in cash, as some banks charge a fee for processing credit and debit card and cheque transactions. Some businesses may also be selling goods 'off record', thus evading sales or value added tax, meaning they can afford to sell goods at a lower price.
- **Interest and fees**. Persons buying and selling goods for cash are not charged interest on credit balances or fees for operating a bank account, meaning that for small businesses overheads can be reduced and profits increased.
- **Cash is dependable in a crisis**. Large-scale natural disasters, such as floods or earthquakes, can cause widespread disruption to critical infrastructure such as transport links, buildings and power supplies, which in turn affects the operation of financial institutions. In these circumstances, cash can often be the only method of conducting any form of financial transaction.
- **Store of value**. In volatile economies, or in jurisdictions threatened by war or natural disasters, cash is often used to store wealth in a way that is considered safer than a financial institution. In some areas, the use of a foreign currency that is perceived to be more stable or secure than the local one (such as the US dollar or the euro) is used for this purpose.

Yet there are numerous disadvantages to using cash to fund anything other than very small transactions;

- **Large amounts of cash are heavy and bulky.** In countries where high denomination banknotes in the local currency are not printed, or not widely available, the amount of cash required to make a major purchase, such as a car, is invariably physically big and heavy. In the UK, GBP 10 000 in a mixture of used GBP 5, GBP 10 and GBP 20 notes weighs in excess of 1 kg and is a pile of banknotes 13 cm high.[8] This has obvious drawbacks in terms of storage and transport to where they are needed.
- **Large amounts of cash are vulnerable to theft.** If a person or business chooses to keep their wealth in cash in a non-secure location such as their house or business premises, or to carry it about their person, then they are much more vulnerable to opportunist or planned theft. Such thefts are often

[8] Source: Bank of England data sourced by UK authorities.

carried out using the threat of, or actual violence. Large amounts of cash stored or carried in this way are unlikely to be covered by home or personal insurance, meaning that the owner has no recourse in the event of a loss.

- **Cash hoarding restricts wealth.** Storing using and cash outside financial institutions restricts access to currency markets, meaning that the cash cannot be used for investment purposes, and cannot therefore generate interest and additional income for the beneficial owner. This is all the more important as money declines in value through inflation; in volatile economies this decline can be extremely rapid.
- **The use of cash restricts purchasing options.** Cash cannot be used to purchase goods in certain circumstances, for example using online portals, and in some countries governments have placed restrictions on the maximum value of cash transactions, or have imposed strict AML regulatory requirements on businesses accepting large amounts of cash in payment for goods and services[9].
- **Making remote payments requires the cash to be transported.** Purchasing goods and services from persons or businesses situated a long way from the purchaser generally requires that the cash for the purchase be transported to the vendor (assuming that neither the purchaser nor the vendor wish to have the cash paid into a bank account). This obviously presents security and logistical problems and results in additional costs. Similar problems are faced by persons wishing to gift money to relatives and/or friends.
- **Cash is costly to count and process.** For businesses, counting and processing cash efficiently requires additional investment in security, distribution, staff recruitment, training and equipment. For businesses and financial institutions; these costs cannot always be passed on to the customer. Large banks and other financial institutions often find it more economical to outsource cash handling systems to specialist companies, which may be cheaper but which creates additional requirements in respect of contract arrangements etc.
- **Restricted access to other financial services.** Deliberately choosing to conduct transactions in cash rather than through a bank means that a person builds up less of a financial 'profile', which can be a hindrance when that person wishes to save or invest their earnings, or to apply for another financial produce such as an emergency loan, or insurance on their house or car.

[9] See section 2.5

1.4 LEGITIMATE CASH USAGE

The total value of cash in circulation in the world was estimated in 2009 to exceed USD 4 trillion[10]. Figures from the European Central Bank (ECB) and the US Federal Reserve point in the same direction, although they only give an indication for an order of magnitude of the legal circulation of banknotes, as they represent only two currencies out of the top 5 currencies in the world[11].

In 2014, there were around 17.5 billion euro banknotes in circulation with a total value of EUR 1.02 trillion.[12] 20-25% of the banknotes were held by people outside of the euro area.[13]

In 2014, there were about 3.4 billion US dollar banknotes in circulation with a total value of USD 1.3 trillion[14] (partly held outside of the US as well).[15]

The use of euro banknotes outside of the euro area cannot be estimated with exact precision, but the ECB estimated around EUR 143 billion worth of euro banknotes to have been in circulation outside the euro area at the end of 2013. This was around 16% of the total euro currency in circulation in that month in the euro area.[16]

This estimate is regarded as a clear lower bound, given that the banking channel is just one of the several channels through which euro banknotes leave and re-enter the euro-area. According to the ECB, anecdotal evidence suggests that the outflows of euro banknotes via non-mainstream financial institution channels (*e.g. via tourism or workers' remittances*) are, for most countries, greater than the inflows via such channels.[17] Therefore, the net shipments by banks offer an incomplete picture of true net flows of banknotes. Other estimates suggest that around 25% of euro currency in circulation (potentially slightly higher) were circulating outside the euro area at the end of 2013.

Movements of currency across US borders cannot be precisely measured for several reasons[18] There is no legal requirement to monitor movements of USD10 000 or less, and many tourists and migrants carry amounts considerably less than this across US borders on a daily basis. In addition, even when there is a legal requirement to report currency flows, mechanisms are not always in place to capture the data; also some reporters might not comply with requirements.

The Federal Reserve provides currency on demand to numerous international customers from within the USA. This banknote shipping business is highly concentrated and data available from this process currently captures the vast majority of banknote shipments that cross US borders through

10 Hewit, Mike (2009)

11 According to Swift, the 3 other top 5 currencies are the Japanese Yen, British Pound and Chinese Yuan (Swift, 2015).

12 ECB (nd a and nd b).

13 ECB (nd a).

14 Federal Reserve (2015a and 2015b)

15 "The Federal Reserve estimates that the majority of the cash in circulation today is outside the United States" (Federal Reserve Bank of New York, 2013)

16 ECB (2014), p. 23.

17 ECB (2014), p. 23.

18 Judson, R. (2012), p.4.

commercial banking channels.[19] However the data does not cover US banknote flows among other countries, which can be substantial.[20]

Moreover, in countries with underdeveloped banking sectors, US dollar banknotes are used to settle transactions of all magnitudes and even in some countries with developed banking sectors and stable currencies, US dollars are the preferred currency for travelers, cross-border trade, settlement of large cash transactions and for transactions in the informal sector.[21]Nonetheless, the Federal Reserve has developed several statistical models for estimating the stocks and flows of US currency abroad. These models suggest that around USD 751 billion was in circulation outside of the US in 2003.[22]

A recent study published by the ECB[23], found that throughout seven major developed economies around the world, including Australia, Canada and the USA, cash was still used extensively, particularly for low-value transactions. The number of cash transactions differed widely between the jurisdictions but were between 46% and 82% of the total number of transactions. The value of such transactions as a percentage of the total was in excess of 50% in Austria and Germany, whereas in Canada, France and the USA it was only about 25%. Moreover, this study found that the use of cash decreases with transaction size; in all countries examined cash was predominant for the smallest 50% of transactions. The study also found a direct correlation between the use of cash and acceptance of credit and debit cards at the point of sale.

Therefore, even in countries with sophisticated financial systems and a wide range of payment options, banks and other financial institutions need cash on a day-to-day basis in order to conduct their normal business activities and to service their customers. Cash will be required for loading into ATMs, for passing across the counter and for foreign exchange purposes, such as for sale to holidaymakers visiting a foreign country, amongst other reasons. Financial institutions receive cash on a day-to-day basis, for example from private or business customers depositing it into their bank accounts.

In recognition of this, the project team agreed that, in order to identify physical cross-border transportation of criminally derived cash and to understand the drivers behind this activity, it was necessary to study the legitimate cash market. By doing so, not only would it become possible to define 'red flags' for identifying criminal cash movements, but it would also aid in the identification of vulnerabilities in the legitimate systems that could be exploited by criminals.

In order to facilitate this, section 2 of the questionnaire was entirely focussed on gathering data regarding the scope and extent of legitimate cash movements. Countries were asked about the following subjects:

- methods used to move legitimate consignments of cash;

19 Judson, R. (2012), p.4-5.

20 Judson, R. (2012), p.5.

21 US Treasury (2006).

22 J. Botta (2003), p. 155.

23 Bagnal, J., Bounie, D. et al (2014).

- the extent of the legitimate cash movements into, transiting and out of their country;
- the types of legitimate cash movements;
- the way in which movements of cash are recorded at their borders.

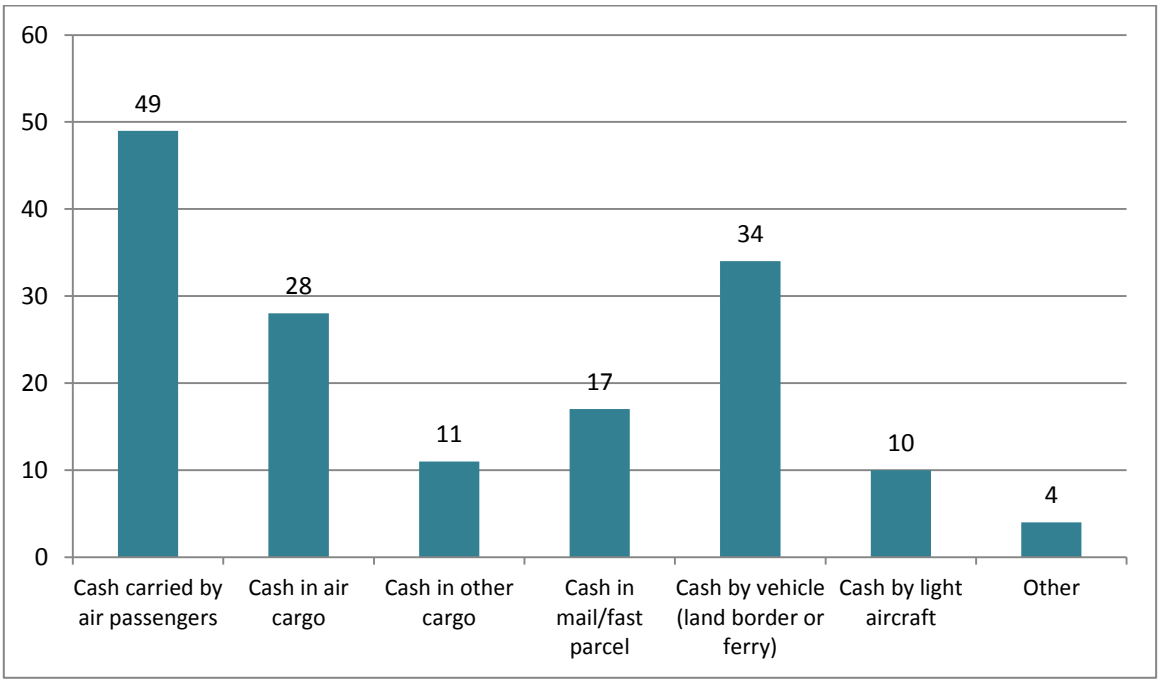
1.5 LEGITIMATE CROSS BORDER CASH TRANSPORTATION

Every day, around the world, businesses and persons transport cash according to their own particular needs, perhaps for the purposes of spending money whilst on holiday, or to pay for goods and services purchased in another country. In the EU for example, where there is a common currency, many countries sharing land borders and a right for any EU citizen to live and work in any EU country, cross-border cash movements take place for legitimate purposes extremely frequently.

In addition, banks and other financial institutions need cash for their day to day operations, in the currency of the country where they operate, and also in numerous other currencies according to the demands of their business, and also that of their customers. This legitimate demand for cash from financial institutions cannot always be serviced from the local market and the reserves of the country in which the bank or branch is physically located, either because the reserve does not have sufficient stocks of the required currency at a particular time, or because the relevant financial institution does not have an agreement with the local reserve to supply it. Accordingly, banks and other financial institutions buy and sell banknotes on global markets, both to meet their demands for cash, and also to enhance their profits by taking advantage of exchange rate fluctuations. The result of this is that cash is physically transported in huge volumes across international borders on a daily basis.

It was apparent from the questionnaire responses that this phenomenon of legitimate cross-border cash transportation was not well understood generally. In the questionnaire, countries were asked to state which methods, in their experience, were most frequently used to transport legitimate consignments of cash across their borders. A summary of the responses are shown in the chart below. The responses showed that most countries were aware that air passengers and persons in cars carry cash legitimately across borders. However, substantially fewer had any experience of cash moving in cargo and mail for legitimate purposes, and yet huge amounts of cash (the equivalent of tens, and sometimes hundreds of millions of US dollars in a single shipment) are transported between major financial institutions by air cargo every day, shipments that are generally subject to very little scrutiny by customs authorities.

Chart 1. **Methods used to move <u>legitimate</u> consignments of cash out of and into a country**



Graphic showing the methods that are used to move legitimate consignments of cash into and out of countries.

Respondents to the questionnaire were also asked if they knew how much cash was moved legitimately across their borders. Again, the majority (60%) said that they knew how much was transported legitimately by air passengers, but substantially less had any knowledge about the value of cash movements in cargo (32%) and mail (21%).

This general lack of knowledge and/or understanding is significant. Without a thorough understanding of the methods and techniques of legitimate crossborder cash transportation, the customs procedures and documentation applicable and the mechanisms that drive these methods and techniques, it can be very difficult for the authorities in a country to be able to tell if a shipment of cash is legitimate or not. Moreover, without this understanding, countries will not be able to assess whether their legislative processes are sufficient to allow their customs and border authorities to control cross-border cash transportation effectively. However, any regulated financial institution involved, e.g., in the case of a (real) bank-to-bank transaction, falls under AML/CFT legislation so that to this extent cash transportation is already regulated (implying compliance management and specific rules defined by supervisory authorities). National authorities can take this into account to identify priorities and operational procedures, including the role of Customs and supervisory authorities. Furthermore, an objective assessment requires specialised expertise which is primarily available in the financial sector and their supervisory authorities.

In line with FATF Recommendation 32, most countries now have in place some form of cash declaration system, a legal requirement for natural persons entering and leaving the country to declare cash in excess of a certain value. However only a few countries have such a system in place for cash in cargo and mail; most rely on the customs procedures applicable to general movements of goods.

1.5.1 CONTROL OF LEGITIMATE CASH MOVEMENTS - NATURAL PERSONS

Specific cash declaration systems (as opposed to general customs declarations) are used by most countries in the world for natural persons (passengers). In some countries, the central bank places restrictions on the amount of currency that can legally be exported, and who can export it, and also what can be done with it once it has been exported. For example, Pakistan prohibits the export of in excess of PKR 3000 (Pakistani Rupees) by natural persons, and stipulates that this currency can only be exported by natural persons who intend to keep it for use when they next return to Pakistan. The exchange of Pakistani Rupees for another currency is prohibited.[24] Similarly, in Tunisia, only the Central Bank has the authority to conduct cross-border transportations of cash in cargo[25].

It is not surprising that most countries that responded to the questionnaire said they had some idea of the value of cash shipped by passengers as most have some form of cash declaration or disclosure system in place, in accordance with FATF Recommendation 32. However, these systems only record amounts above the declaration threshold level – anyone carrying less than this amount need not make a declaration and so those details will not be recorded.

Cash declaration systems are covered by the interpretive note to Recommendation 32, which states that, *inter alia*, all countries should implement a system requiring either all travellers to declare or disclose any currency they are taking in out of a country, either orally or in writing, or only those carrying in excess of a certain value (the interpretative note states this should be USD or EUR 15 000 or equivalent, but many jurisdictions specify a lower amount). In addition the interpretive note states that travellers should be required to make truthful declarations, that penalties should apply for false or non-declaration, and that the relevant authorities should have powers to detain cash and conduct enquiries in such cases.

The questionnaire distributed for this research included questions in relation to the cash declaration systems in effect in the responding country. The responses indicate that the methods by which this recommendation is implemented vary considerably from one country to another, with some countries saying, for example, that all cash declarations by natural persons are checked for accuracy (by counting the cash), whilst others say this is only done occasionally[26]. The responses also reveal that some countries keep detailed statistics on the amount (value) of cash that is transported into, out of or through their country by legitimate financial institutions (as opposed to natural persons), whereas others keep no such records and effectively have little oversight of the matter.

The responses also reveal that there is little collaboration between neighbouring countries when establishing cash declaration systems, resulting in significant incongruences. For example, Guatemala's system requires the declaration of any amount of cash being taken into or out of the country, whereas Mexico and Honduras, with whom it shares lengthy land borders, only requires the declaration of amounts in excess of USD 10 000. Likewise, Brazil's entry and exit declaration

[24] State Bank of Pakistan (2014).

[25] Source: Tunisian authorities.

[26] Recommendation 32 makes no reference to extent to which verifications of cash declarations should be carried out

threshold is BRL 10 000 (Brazilian real), (about USD 3 900), whereas those in its neighbours Colombia, Peru etc. are USD 10 000.

Perhaps inevitably, case examples reported by a number of countries show that criminal groups have learned that they can exploit cash declaration systems for criminal purposes by various means, including:

- using the fact that cash has been declared on entry as a way of legitimising criminal cash paid into a bank account,
- re-using cash declarations several times for the same purpose, or
- over-declaring cash on entry (where there is no confirmatory count) to cover the receipt of criminally derived cash in the country of import.

These issues are examined in more detail in Section 3.

1.5.2 CONTROL OF LEGITIMATE CASH MOVEMENTS - CARGO

A significant percentage (21%) of countries who responded to the questionnaire stated that import and export of cash consignments in cargo and mail are not declared at customs at all. A possible explanation for this may relate to the interpretation of customs legislation – some countries do not acknowledge cash as a type of goods, and consequently they do not require customs declarations (or, for that matter, any other types of declarations) for cash in cargo and mail.

For customs purposes, including import, transit and export, cash (banknotes) are a type of goods and subject to the same procedures as other goods; a customs declaration is required. In the international "Harmonized System", developed by the WCO, cash (banknotes) is given a unique goods nomenclature code: 4907 ("Unused postage, revenue or similar stamps of current or new issue in the country in which they have, or will have, a recognised face value; stamp-impressed paper; banknotes; cheque forms; stock, share or bond certificates and similar documents of title[27]").

"The Harmonized Commodity Description and Coding System (generally referred to as "Harmonized System" or simply "HS") is a multipurpose international product nomenclature developed by the WCO. It comprises about 5 000 commodity groups; each identified by a six digit code, arranged in a legal and logical structure and is supported by well-defined rules to achieve uniform classification. The system is used by more than 200 countries and economies as a basis for their customs tariffs and for the collection of international trade statistics. The HS contributes to the harmonisation of customs and trade procedures, and the non-documentary trade data interchange in connection with such procedures, thus reducing the costs related to international trade. It is also extensively used by governments, international organisations and the private sector for many other purposes such as

- internal taxes,
- trade policies,
- monitoring of controlled goods,

[27] World Customs Organisation (nd)

- rules of origin,
- freight tariffs,
- transport statistics,
- price monitoring,
- quota controls,
- compilation of national accounts, and
- economic research and analysis.

The HS is thus a universal economic language and code for goods, and an indispensable tool for international trade. The HS is governed by "The International Convention on the Harmonized Commodity Description and Coding System"[28].

As cash is a normal cargo consignment a custom declaration has to be lodged. These declarations are always recorded in customs systems. However, neither the denomination or currency need to be specified in the declaration. The customs declaration requires only the weight of a shipment and a proper description of the goods. Opinions between countries differ when it comes to the need to state the value in the customs declaration. Some countries think it is not necessary, as the commodity code for banknotes has no VAT or duty implications so a value would not be required.

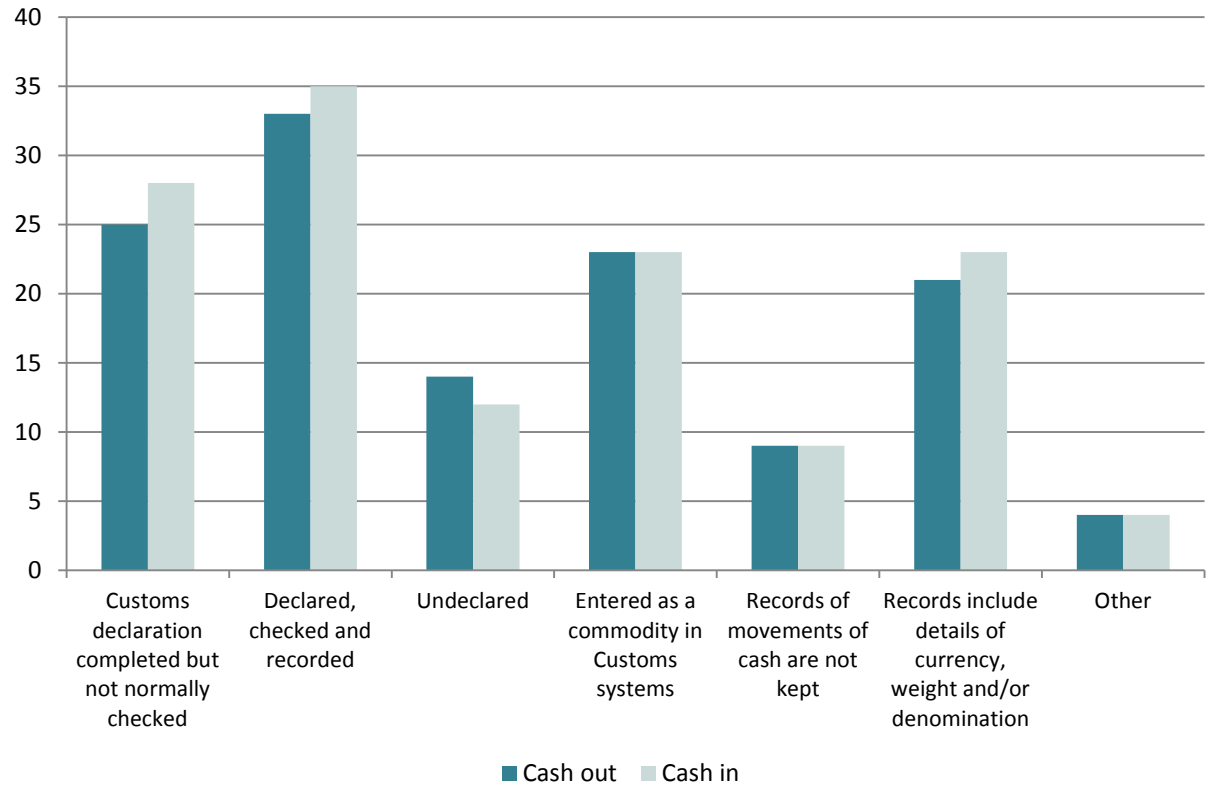
Other countries are of the opinion that the value of the goods declared at customs is always an obligatory element of the declaration, for example as it is mandatory in legislation on statistics. This cannot be the normal transaction value, as the cash has not been bought by the owner (as is mostly the case with all other goods). This means that the intrinsic value of the cash has to be declared (the value of the paperwork, the ink, etc.). In a summary declaration, however, no value at all has to be stated. Apart from the customs declaration, some 20 countries state that they use a specific cash declaration form more or less like the declaration to be used for passengers. In most cases this cash declaration has a threshold of USD 10 000.

Although there is a specific tariff code for banknotes within the HS, some jurisdictions have observed that not all freight forwarders or shippers use the correct commodity code when completing customs clearance documentation. A wide variety of other codes have been incorrectly applied, such as those for 'printed matter'. Because there is no customs duty implication on shipping banknotes, there are no revenue implications for doing so, and in fact not using the correct tariff code can add an extra layer of security as it can help to mask the value and nature of the shipment. This can make it very difficult for national authorities to identify shipments of banknotes, and gather statistics on the trade.

The questionnaire asked counties to detail how movements of cash in cargo and mail were recorded or controlled at their borders. The chart below summarises the responses.

[28] World Customs Organisation (nd)

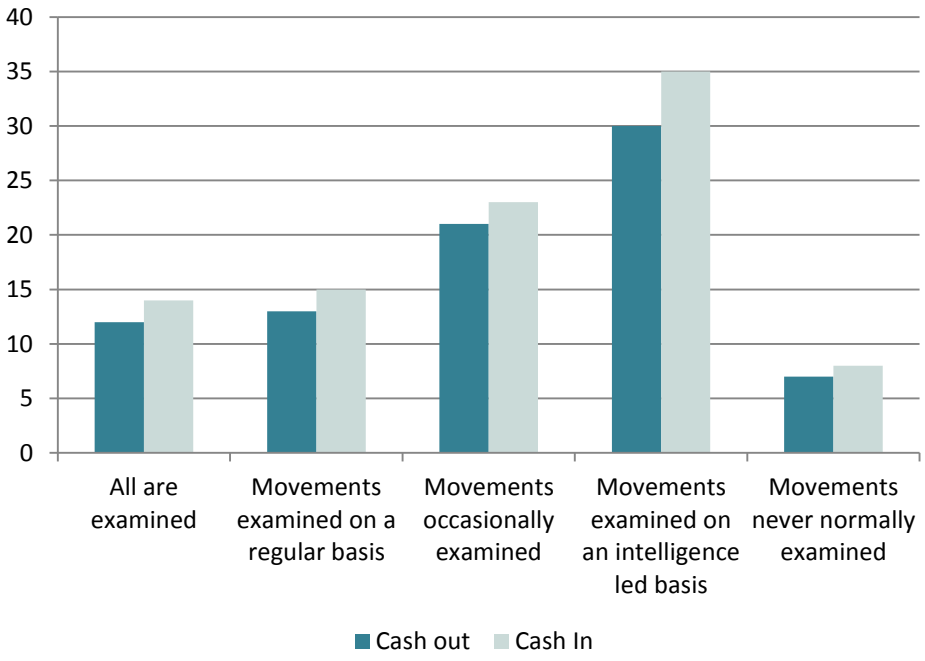
Chart 2. **Movements of cash in cargo and mail**



The chart above shows that most countries stated that shipments of cash in cargo and mail were declared, checked and recorded. However, as the value of the cash is not normally stated on the customs documentation, the checks that are made cannot routinely include the actual value of the shipment (as opposed to the value of the paper, print etc.), which explains why most countries have little or no idea of the value of the cash that is shipped using this method. The fact that there are few figures available is confirmed by the fact that most other countries stated that movements of cash were subject to a customs declaration that was not checked, entered simply as a customs commodity, not declared at all or that they kept no records of cash moved in this way.

Countries were also asked to state what controls were exercised on movements of cash in cargo and mail, other than those transiting their country. The next chart summarises their answers. Some countries stated that they examined all such movements, and about the same number said that they examined them on a regular basis. However, more countries indicated that they only examined them occasionally. The option most commonly selected was that movements were selected for examination on an intelligence-led basis. However, due to the way the customs documentation in respect of these shipments is completed, there is little intelligence available on which to make a judgment (these issues are discussed in more detail in section 4 of this report.). Eight jurisdictions stated that such movements were never examined at all.

Chart 3. **Controls exercised on movements, other than transit, of cash in cargo and mail**



The questionnaire also asked respondents to state why movements of cash were selected for examination; options given were violation of customs regulations, suspicion of money laundering, notifying unusual transactions, profiling or routine selection. All of these reasons were selected, with no one reason standing out from the others.

The countries listed in the table below stated that they have, in addition to the regular customs declaration, a specific system in place that requires the declaration of all transport of cash in cargo and mail above a certain threshold. The threshold is in many cases is USD 10 000, similar to many cash declaration systems for natural persons.

Table 1. **Specific declaration form for cash movements in cargo and mail**

CARGO		MAIL	
1. Argentina	10. Korea	1. Argentina	10. Korea
2. Australia	11. Malaysia	2. Australia	11. Malaysia
3. Azerbaijan	12. Mauritius	3. Azerbaijan	12. Mauritius
4. Bermuda	13. New Zealand	4. Bermuda	13. New Zealand
5. Colombia	14. Panama	5. Bulgaira	14. Panama
6. Guyana	15. Qatar	6. Colombia	15. Qatar
7. Israël	16. Uruguay	7. Israël	16. Uruguay
8. Jordan	17. United States	8. Jordan	17. United States
9. Kingdom of Saudi Arabia		9. Kingdom of Saudi Arabia	

The US[29] and Australia indicated that such a declaration is also obligatory for transit shipments in cargo and mail. Although not explicitly stated, it seems that this is the case in most of the other countries with a specific cash declaration as well.

Box 1. **The global banknote trade**

There is a significant global market in trading of currencies for profit between banks and between banks and non-bank financial institutions. This trade serves to fulfil not only the day to day cash needs of the institutions involved, but also as a means of generating profits by speculating on and taking advantage of exchange rate fluctuations. Banknotes are often traded in packages of mixed currencies, such that a business with a need for euros may only be able to obtain them as part of a package which includes US dollars, Japanese yen etc. In these circumstances the unwanted currencies will be sold on wherever possible to other banks and other financial institutions such as money service businesses (MSBs). Less common currencies will often be sold on as quickly as possible to avoid unfavourable exchange rate fluctuations.

Major international currencies such as the US dollar and the euro are held in reserves away from the countries where they are issued and printed. In the case of the US dollar, the Federal Reserve Bank of New York (FRBNY) operates the Extended Custodial Inventory Programme, where US dollars still in the ownership of the FRBNY are held in secure locations in segregated vaults owned and managed by private sector banks in Frankfurt; Hong Kong, China; London; Singapore and Zurich.

Currency traded both nationally and internationally is generally physically transported by specialist Cash/Valuables In Transit (CVIT) companies who have access to a wide variety of high security measures, such as secure cash centres, safes, cash counting and processing facilities, secure packaging and armoured vehicles. Some of the large CVIT companies also provide a complete 'end to end' service that involves collection, consolidation, counting, customs documentation and clearance and delivery to the intended destination.

Legitimate shipments of cash between financial institutions in different jurisdictions can be transported in a variety of ways, including by the postal service, CVIT company armoured van or in air cargo. The common factor between all shipments of this nature is that the cash handler has strict protocols and procedures in place to ensure that, in event of a challenge from one of the parties to the transaction, or a serious incident occurring, any losses are covered by their insurance and the company and its staff are indemnified against legal action.

In most cases these procedures will include an independent count of the cash, following which it is sealed in tamper evident packaging to guard against external interference (it is worth noting here that any examination of the consignment by customs authorities will immediately be evident because of this). International airports that function as freight hubs will usually have high-value freight sheds, with stringent security measures in place to process high-value shipments.

The percentage profits involved in this activity are small. Currency pairs (the currencies traded against one another, for example USD and EUR or GBP and EUR) are usually traded in exchange rates quoted to four decimal places, and profits often involve differences of one or two 'pips'(a pip

[29] Department of the Treasurey (nd).

is a difference of one hundredth of one percent in an exchange rate), meaning that currencies have to be traded in large volumes to make the process worthwhile.

Because of the small profit margins involved, it important for financial institutions to keep the costs involved in the process as low as possible. This includes the costs related to counting, packing and shipping the cash; these costs are included in the fees charged by the CVIT companies to the financial institutions. In order to minimise these costs, cash is generally shipped in a way that makes processing and counting as easy as possible. The cash is usually packed in blocks of 100 notes of the same currency and denomination, secured with a plastic strap, with blocks of 100 notes subsequently combined to make bigger blocks of 1000 notes, also secured in plastic straps. These blocks are then sealed in robust plastic sacks, with each sack secured with a uniquely numbered seal (the tamper evident packaging referred to above).

Although a shipment of cash may contain multiple currencies and notes of different denominations, each sack will generally contain a set amount of only one denomination of notes of one currency (although some shipments may contain a single sack of 'left over' multiple currencies and denominations that are not sufficient in themselves to make up a complete sack). The customs documentation will usually not give a full value of the shipment, but there may well be additional documents available from the shipping company, including packing lists detailing what currencies and denominations should be in each sack. As mentioned above, the shipping company will have an insurance policy specifying a maximum value of cash that can be transported in a single shipment, and so the shipments will not exceed that value.

Packaging and shipping the cash in this way makes it much easier to count and process and reduces costs to a minimum. Any other type of packaging, such as multiple currencies and denominations in a sack (other than in the circumstances described above), or blocks of notes of varying sizes without the correct banding or strapping dramatically increases processing and counting costs and would be rejected by the beneficial owner of the cash due to the impact on their profits. The financial institutions who volunteered this information to the project team stated that packaging of this nature could be considered as a 'potential indicator of criminal origin of the cash.

In addition to the measures carried out by the CVIT companies, banks and other financial institutions are obliged under their domestic laws to conduct extensive customer due diligence (CDD) enquiries in respect of all of their customers. Typically, this will involve enquiries into the business model of the customer – whether the cash is sourced from its own internal operations, or whether the customer is acting as a consolidation point for other cash rich businesses in the local area. If this is the case, the CDD will extend to obtaining additional information, such as a breakdown of these points of origin of the cash. The financial institution may also conduct research into the customer's market, perhaps to satisfy themselves that the volume and breakdown of the cash they are purchasing is consistent with local conditions (a bank in a destination popular with European tourists may sell more cash in euros during the summer, for example).

The effectiveness of these CDD enquiries is extremely important as the security of a system is only as strong as its weakest point. For example, if the customer bank is acting as a consolidator of cash from smaller businesses, it is important that potential risks are taken into account in the CDD process. If the business model or relationship is one that is assessed to be higher risk in principle, the bank may decide that enhanced due diligence enquires are appropriate, possibly including

having a good understanding of their customer's client base.

Recent work undertaken by both the UK and the Netherlands' authorities has identified that the customs control of large, (ostensibly) bank to bank shipments of banknotes may often not be as rigorous as it could be (or, in many cases, are not controlled at all). Because there are no outward reasons for suspecting these shipments, they are not (and in some cases, due to a lack of the necessary authority, cannot be) routinely selected for examination, and in most cases banknotes transiting a country are not examined at all. In addition, examples of poor practice by CVIT companies, such as removing shipments of banknotes from customs controls before they have been customs cleared, have been identified.

Source: UK authorities, based on liaison and interviews with international companies involved in currency trading and the associated cash transportation.

1.5.3 CONTROL OF LEGITIMATE CASH MOVEMENTS – MAIL

The Universal Postal Union (UPU), established in 1874 by the Treaty of Bern, is the second oldest worldwide international organisation. With 192 member countries, the UPU is the primary forum for cooperation between postal sector players. As a specialised organisation of the United Nations the organisation sets the rules for international mail exchanges.

Member countries provide the International Bureau of the UPU with the name and address of the operator or operators officially designated to operate postal services. The designated operator is any governmental or non-governmental entity officially designated by the member country to operate postal services and to fulfil the related obligations arising out of the Acts of the Union on its territory. Member countries ensure that their designated operators accept, handle, convey and deliver letter-post items.

Letter-post items are:

- priority items and non-priority items, up to 2 kg;
- letters, postcards, printed papers and small packets, up to 2 kg;
- parcels up to 20 kg.

This means that other shipments that are not part of the UPU definition should be treated as cargo, and all cargo procedures are then applicable. This also applies to international courier companies. Consignments handled by these companies are not 'caught' by the above definition. On other legal grounds, however, the same prohibitions and legal constraints as for letter-post are applicable for these companies.

The treaty also defines restrictions and general prohibitions (such as narcotics and psychotropic substances, obscene or immoral articles, etc.), general exceptions to the prohibitions and any extensions of the prohibitions on a country by country basis.

Article 18.6 UPU sets rules on coins, banknotes and other valuable articles, stating that…"It shall be prohibited to insert coins, bank notes, currency notes or securities of any kind payable to bearer, travellers' cheques, platinum, gold or silver, whether manufactured or not, precious stones, jewels or other valuable articles…"

However, some countries have used the possibility of making exceptions (extensions of the general prohibition) in the treaty itself. For example regarding letter-post some countries do not accept registered items containing cash and equivalent items. Other countries do not accept insured parcels containing such items.

The key point is that the UPU restrictions and prohibitions (and national extensions) are not directly binding for the designated operator and the persons using the postal service. All of the prohibitions should be implemented in national postal legislation. Even where this is the case, in general terms, it is not the task of customs to control these prohibitions (80% of the responding countries stated that customs is the prime responsible agency[30]). This will only be the case when violating the prohibitions has been criminalised in that national legislation. Otherwise, not complying with the prohibitions will just mean that the sender didn't comply with the regulations of the designated postal operator.

Some countries' questionnaire responses stated that the UPU prohibits sending cash in mail. As this is not actually the case, these countries may have been referring to a prohibition in their own national (postal) legislation based on UPU guidelines. Another explanation could be that these countries are not fully aware of the legal situation regarding cash in mail as this is not seen as a risk or as something of interest to them. One of the conclusions, however, is that countries differ widely in their approach to cash control in mail. Some of them treat this as being prohibited, other countries treat it as if it is permitted.

Box 2. **Prohibition of sending mail in post - France**

France prohibits sending currency, coins and precious metals by mail by their national *Décret n° 2013-417 du 21 mai 2013 portant modification du code des postes et des communications électroniques*.

In this legislation which was enacted, the French government decreed that it is forbidden to send all forms of currency - coins and cash and all forms of precious metals – coins, bars and jewellery by mail.

Source: France.

For all letter-post consignments with legal constraints, such as cash, a specific customs declaration has to be submitted: the CN 22 or CN 23. Apart from the customs declaration, some 20 countries state that they use a specific cash declaration form more or less like the declaration to be used for passengers. This cash declaration has a threshold of USD 10 000 in most cases.

Some countries have separate systems for postal clearance, while others have integrated postal clearance functions into their national customs systems. It is, however, not unusual that even when customs clearance procedures in one country are automated, this functionality is missing in clearance of postal items.

[30] Most probably this percentage will be even considerably higher, as clearly some countries did not answer section 3 question 1 in the right way. For example, a country with a prohibition and licensing scheme for cash in mail most definitely will have a controlling agency, but the country's answer was "none".

Customs control of letter-post has at least one difference with normal customs control that makes control more difficult. If customs want to open letter-post within a customs control, they are confronted with legal issues regarding the confidentiality of correspondence (for example, in the UK, opening a letter is treated as an interception of a communication in the same way as a telephone interception; this cannot be done without a warrant signed by the home secretary).

Besides these special procedures to open letter-post, there is also the enormous volume of letter-post to be considered: in 2013 3.5 billion items were carried by postal systems worldwide. Considering these amounts and the simplified customs procedures regarding letter-post, modern risk management tools are not very useful.

Responses to the questionnaires indicate that many (but not all) countries do not pay attention to the phenomenon of cash transportation in mail. It seems clear that if countries only look superficially, by simply examining formal declarations of cash in mail, in all probability they would conclude that there is no reason to give cash in mail any attention as it would seem that there is very little to study.

Only two countries provided details in respect of legitimate cross-border shipments of cash in mail. One of those countries paid special attention to this issue during over a defined period of time, to gain an insight into this phenomenon, and to establish if there were any money laundering (ML) and terrorism financing (TF) issues at stake. This research revealed that there were very few formal import and export declarations made (just 1 in 2013). However, over the period that the project ran, the customs authorities in that country made numerous detections of cash concealed in mail. This led them to conclude that cash is transported in mail items quite frequently, but is hardly ever declared at customs, regardless if it is a legal or illegal transportation of cash. One of the outcomes of this exercise was that the customs authorities in that country found it had insufficient legal powers to effectively control ML and TF risks in cargo and mail. As a result, that country is in the process of drafting new ML and TF specific legislation on cash in cargo and mail.

The above mentioned research appears to imply that the phenomenon of cross-border transportation of criminally derived cash in mail may be a higher risk that most countries appreciate. However, it is important to consider also the experiences of Germany and France who also conducted focused exercises to study the issue. The outcome of both of these exercises was that, despite the examination of a very large number of fast parcels and mail, no (undeclared) cash was identified.

The fact that the experiences of three ostensibly similar European countries were very different is in itself significant. Such differences would imply that there may be regional or local factors at play which affect the phenomenon, e.g., the fact that it is public knowledge in some countries (Germany) that international post and parcels are regularly controlled/scanned by post and customs and that they can be opened, while in other countries/regions it is public knowledge that a judicial decision is needed to open post and parcels, or that no regular controls are implemented in this area. Taking these facts into consideration, it appears that more needs to be done to understand the issue[31].

[31] Due to the fact that it is common knowledge that post and parcels are regularly controlled and opened in Germany, the German authorities consider their cases of criminal cash in mail and fast parcels presented in Box 22 and Box 28 to be exceptions.

1.5.4 ESTIMATING THE VALUE OF LEGITIMATE CASH MOVEMENTS – NATURAL PERSONS

Responses to the questionnaire reveal that, because many countries do not keep records of how much cash crosses their borders for ostensibly legitimate purposes, it is not possible to come up with an accurate figure of how much legitimate cash is being transported across the globe, as opposed to sitting in treasury reserves[32]. Likewise some countries do not verify or check the accuracy of cash declarations made by natural persons at their borders. In many cases, declarations that are made are not subject to any form of confirmatory scrutiny, so there is no guarantee that what has been declared was the amount that was transported.

In August 2010, the European Commission (EC) produced a report[33] compiled from data from all but one EU countries which analysed the effectiveness of EU cash controls. (EC regulations dictate that natural persons must declare cash in excess of EUR 10 000 when entering or leaving the EU – there is no requirement to declare intra-EU cash movements.)

This report identified that, between July 2007 and July 2009, natural persons entering or leaving the EU declared a total of approximately EUR 80 billion. No figures were available for the amount of cash transported between financial institutions. In the same period, cash detections (i.e. cash movements by natural persons that were not declared for some reason, but instead were detected by customs or other authorities) amounted to EUR 1.6 billion.

It is likely that the actual amount of cash derived from criminal activities transported across EU borders was significantly in excess of this figure, however no reliable estimates for this trade currently exist.

1.5.5 ESTIMATING THE VALUE OF LEGITIMATE CASH MOVEMENTS – CARGO & MAIL

The questionnaire responses provide more insight into the extent of the legitimate cash movements into, transiting and out of countries. On average[34], at least 65% of the countries that answered the relevant questions indicated that they did not know how much cash is legally transported out of and into their country through cargo on a yearly basis, and 71% of the countries did not know how much cash is legally transported through mail.

This means that only 35 % of the countries that responded would be able to reveal the extent of cash legally transported out of and into their country through cargo and mail on a yearly basis[35]. This figure coincides more or less with the 20 countries that, according to the questionnaires[36], use a specific declaration system for cash in cargo and mail, and the approximately 30 countries that

[32] Alternatively, cash in a foreign denomination may circulate domestically, e.g. in countries with a cash based and dollarised economy.

[33] European Commission (2010).

[34] The average of the number of countries that reported on import and the countries that reported on export.

[35] These figures represents the cash declared at customs (by means of a customs declaration or specific cash declaration). As most of this cash has not been checked on ML and TF, formally countries do not know if all of this cash is legal.

[36] When asked additional information of some of these countries, the project group found that legally nor in practice not all of these countries has a specific declaration system for cash in cargo and mail.

state they have a specific database (other than the normal customs declaration database) that records the import and export of banknotes in cargo and mail[37].

Nevertheless, only 7 countries were able to provide information on the extent of cash legally transported out of and into their country through cargo on a yearly basis[38]. For the other countries, there is no understanding on the extent of legitimate bulk cash movements across their borders and the total amount of physical cash movements declared. The conclusion seems to be justified that cash in cargo and mail is not an item of interest of almost all countries; most of them don't pay attention to this phenomenon, again highlighting that the concept of cross-border transportation of cash in cargo & mail is, with a few exceptions, not very well understood.

This conclusion is underlined by the fact that 39% of the responding countries indicate that legitimate cash movements transiting their country in cargo and mail, are not subject to any form of control, declaration or examination. Almost a third of the responding countries do not know if these movements are subject to any form of control.

The above mentioned 7 countries specified how much legitimate cash on a yearly basis moved into, through and out of their countries in cargo and mail[39]. The figures for 2013 for cargo are:

- the import of cash ranged between USD 26 million and USD 108 billion;
- the export of cash ranged between USD 8 million and USD 296 billion;
- transit of cash ranged between USD 3 million and EUR 3.4 billion[40].

In these 7 countries, around USD 500 billion legitimate cash crosses the border in cargo on a yearly basis. Extrapolating, this would mean that each year USD several trillion in cash is moving across the world's borders.

The details submitted by some of the 7 countries lead to the conclusion that on average, a transportation of cash in cargo contains EUR 3 million, ranging between EUR 100 000 and EUR 150 million per transportation. As a matter of course, a container, even a small one, can contain much larger amounts of cash than a passenger can carry. Compared with the amounts of cash transported across the border by passengers, the amounts transported each time are incomparably higher in cargo.

Overall, the questionnaire responses indicate that, with a few notable exceptions, most countries do not pay a great deal of attention to the phenomenon of cash in cargo and mail. Based on the limited international research that has been carried out in recent years (see section 1.9) an educated guess of the amount of cash being transported across borders in cargo and mail could be several trillions

37 See for a more detailed description section 1.6.

38 There are 21 other countries which reported figures and/or text on the extend of cash legally transported out of, through and into their country through cargo, mail and by passengers. In fact, they reported a total figure without distinguishing between the three (mail, cargo, passengers). It can be assumed that in almost all cases this total figure is only related to passengers.

39 It is worthwhile noting that, as 4 out of these 7 countries have no specific declaration for cash in cargo and mail, they won't have a specific database for these data. It can be assumed that the figures given are based on their national customs declaration database.

40 Only two countries gave figures on transit. It is hard to find any figures related to transit, because in transit situations, a summary goods description may suffice, which makes it more difficult to assess the type of goods.

of US dollars each year, worldwide. The amounts of cash transported each time are incomparably higher in cargo then by passengers (and, it would seem, in mail). Individual consignments of up to USD 150 million in cargo are not unusual. Cross-border transportation of cash in mail is mostly an unknown quantity, but the experiences of one country suggest that it may well be vulnerable to money laundering and terrorism financing.

1.6 CRIMINAL USAGE OF CASH

Criminal markets continue to generate large amounts of cash that pass up the supply chain for criminal goods or form the raw material that criminals and money launderers need to process.

Criminals frequently need to use a significant portion of the cash that they have acquired to pay for the illicit goods they have sold, to purchase further consignments, or to pay the various expenses incurred in transporting the merchandise to where it is required. Despite the advantages and disadvantages of dealing in cash (detailed earlier in this report), for criminal groups, there is often little choice. The criminal economy is still overwhelmingly cash based[41]. This means that, whether they like it or not, criminals selling some form of illicit product are likely to be paid in cash. The more successful the criminals are and the more of the commodity they sell, the more cash they will generate. This can cause criminals significant problems in using, storing and disposing of their proceeds. Yet despite these problems, cash is perceived to confer some significant benefits on them.

The principal benefit is often said to be that **cash is anonymous and leaves no audit trail**. The anonymity of cash is often quoted as one of the main reasons for its use in the criminal economy and there is no doubt that, up to a certain level, this is the case. Demonstrating the provenance of small amounts of cash can be problematical for law enforcement officials. For example, so the sale of dealer quantities of prohibited drugs for cash, can be harder to identify and prove when payment is received in cash. The dealer may be able to give an acceptable (or at least, non-disprovable) account of the wad of cash in his wallet. However the reality is that cash is only truly anonymous in smaller amounts. Criminals tend to be able to justify holding small to medium levels of cash when challenged. However the possession or movement of large amounts of cash with no explanation of their origin or purpose becomes increasingly difficult for criminals and criminal groups.

Once the amount of cash exceeds these limits, there is a general expectation that the person in possession of it will be able to account for it if required. Even in cash-based economies, if a large transaction is undertaken there will generally be some record of it somewhere – a receipt, an entry in a ledger, the physical existence of the goods sold or purchased, evidence of withdrawal from a bank etc. Therefore, the inability of a criminal to adequately account for the large amount of cash in his possession – the fact that it is anonymous - can actually be a hindrance, rather than an advantage.

This absence of a legitimate explanation is a major drawback when trying to introduce funds into a bank or other financial institution. Thanks to the FATF Recommendations, and specifically Recommendations 10, 11 and 20 concerning customer due diligence and reporting suspicious transactions, most financial institutions across the world would now question the origin of a large

[41] This has been concluded in several studies, such as the 2015 report of the Europol Police Office *Why is cash still king. A strategic report on the use of cash by criminal groups as a facilitator for money laundering* (Europol, 2015).

amount of cash that someone was trying to pay into a bank account. Accordingly, criminals seek to avoid such issues by retaining the cash they have generated, and if it is required elsewhere, simply physically moving cash across international borders. [42]

As AML measures are progressively tightened across the world, criminals will face ever increasing difficulties when attempting to place their cash into the legitimate financial system. It seems likely, therefore, that the phenomenon of money laundering through the physical transportation of cash is likely to progressively increase

The way criminally derived cash moves will be covered in more detail later in this report, but based on the questionnaires and the case examples submitted, the most prevalent methods are as follows;

- **By cash courier.** In the context of this report, as cash courier is a person who has been recruited by a criminal organisation to transport criminally derived cash across an international border on their person. The courier may have the cash concealed within his clothing, on his body (for example in a money belt or similar), concealed in his luggage (either within his personal effects or within the structure of the luggage itself) or even concealed internally. Cash couriers may use air, sea or rail transport to cross an international border.
- **Concealed within a method of transport.** This refers to the cash hidden within the structure of the method of transport, rather than in any form of cargo. Methods of transport can include cars, lorries or maritime craft ranging from small pleasure boats to larger vessels such as container ships and ferries. In these circumstances, the person in charge of the vehicle may be fully aware of the concealed cash and complicit in the smuggling attempt. Alternatively, the driver of a vehicle may genuinely not know that the vehicle he is driving has cash concealed within it. Similarly, members of a ship's crew may have hidden the cash in a void on the vessel without the knowledge of the captain or the rest of the crew.
- **In containerised or other forms of cargo.** Cash is heavy and bulky and there is a limit to the amount that a cash courier can carry, either about his person or in the structure of his luggage. Likewise, the physical bulk of cash can restrict the amount that can be concealed in voids in the structure of vehicles or other modes of transport. If a criminal organisation wishes to move very large amounts of cash, often their only option is to conceal it in cargo that can be containerised or otherwise transported across borders.
- **Concealed in mail or post parcels.** Some countries report examples of sophisticated concealments of cash within goods sent by regular mail or post parcel services. Although these concealments tend to be smaller than those within vehicles, or on the person of cash couriers, the use of high denomination banknotes can result in seizures of significant value.

[42] Source: based on research by UK authorities.

- **Hidden in 'plain sight'.** Research conducted in the course of gathering information for this paper, and also by the customs authorities in contributing jurisdictions, has identified that some criminal groups have, by taking advantage of the limited requirement for information regarding cash shipments in customs declarations, or by falsifying such documentation, been able to infiltrate large quantities of criminally derived cash into the systems used by legitimate financial institutions to transport cash intended for use in regular financial systems. The extent of this criminal exploitation is currently unknown.

1.7 THE STATUS OF THE PROBLEM

In April 2014, the project team distributed a questionnaire to FATF and FSRB members which asked responders to give their assessment of whether the phenomenon of ML through physical transportation of cash was increasing, static, declining or fluctuating, and why they thought this was the case.

Two-thirds of the respondents recognised cash smuggling as a significant risk, and of those, half reported that it was an increasing problem. However the remaining third of respondents were unable to assess the scale of the problem in their country.

One country stated that the phenomenon was declining, as a result of improved border controls which were believed to have made it harder for criminals to move cash across the country's borders undetected, and this had resulted in a steady decline in the amount of cash seized.

The countries that said that the problem was increasing gave a variety of reasons for their answers. These included:

- **An increase in the robustness of banking controls**. As AML/CFT measures become more effective and better enforced, criminals find it more difficult to introduce cash into the financial sector, and are forced to physically transport it across borders instead. This was the most common reason cited.
- **An increase in criminal activity**. Some countries perceived that the level of acquisitive crime in their jurisdiction (or a neighbouring jurisdiction) had increased, leading to an increase in the level of criminally derived cash generated.
- **Lax border controls, or a lack of resources or will to implement border controls effectively**. Some countries believe that certain criminal groups have identified that border controls are ineffective in some areas and take advantage of these weaknesses to move cash with little risk of detection.
- **Economic and/or political instability**. In countries where the regular financial system is disrupted due to conflict or serious instability, all types of persons, including those engaged in criminal activity, will seek to move their assets to somewhere safer.

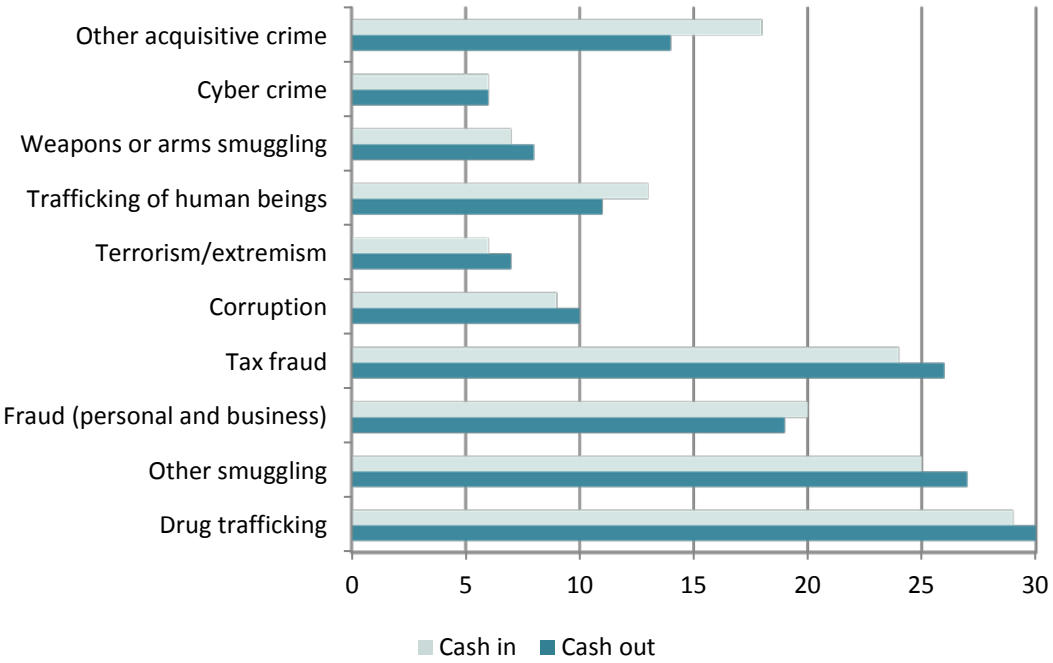
Conversely, some countries remarked that their perceptions of an increase in the problem were based on the results of an increase in the robustness of their border controls and an improvement in their detection capabilities. This raises the question of whether the problem of cross-border transportation of cash is actually increasing, or whether the countries concerned were simply getting better at detecting it.

1.8 PREDICATE OFFENCES GENERATING CASH PROCEEDS

It is clear from the completed questionnaires and case examples received in the course of the information gathering phase of this project that criminally derived cash physically transported across international borders originates from an extremely wide range of predicate offences. One of the questions in the questionnaire dealt specifically with this topic, and provided 12 options for types of offences, with an additional option of 'other' and a request to provide details of any offences not specified in the question. The question also asked countries to differentiate between cash smuggled into their jurisdiction, and cash smuggled out.

All of the predicate offences suggested were selected by at least six of the countries responding to the questionnaire. The responses were as follows:

Chart 4. **Predicate offences generating cash proceeds**



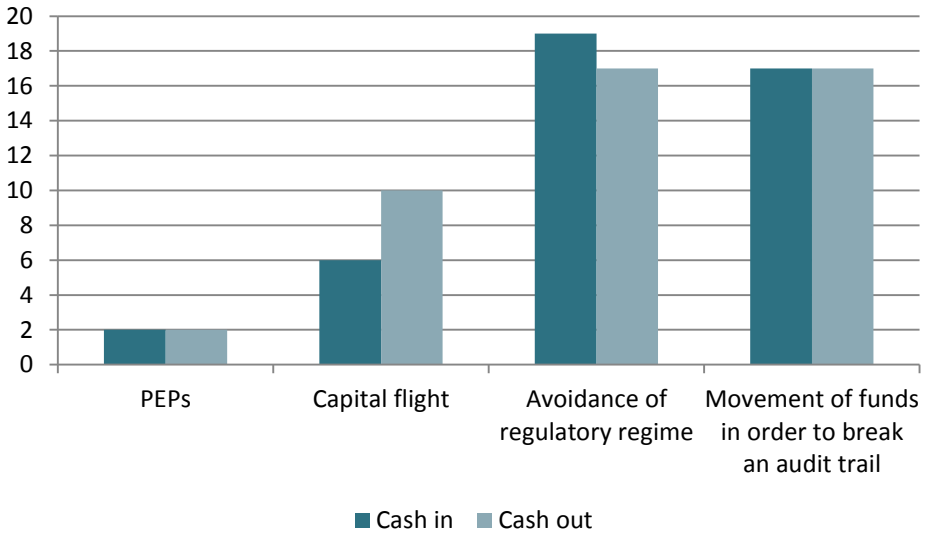
The responses show that the most frequently encountered predicate offence is drug trafficking, although smuggling of other goods (alcohol, tobacco etc.) and tax fraud also feature heavily. The above chart also shows that there is a broad correlation between the reasons behind the movement of cash into countries and those linked to movement in the opposite direction, although this does not necessarily mean the cash always follows the reverse routing of illicit goods.

Analysis of questionnaire responses indicates there are no predicate crimes that are more commonly associated with one method of cash smuggling than another. The method chosen to move the cash is influenced more by the intended use of the funds and the destination to which they are to be moved than by the nature of the crime itself. This issue is explored in more detail in Section 2 of this report.

OTHER FACTORS INFLUENCING CROSS-BORDER CASH TRANSPORTATION

The same question of the questionnaire also asked countries if movements of cash could be linked to factors other than just predicate offences. The graphic below illustrates the responses.

Chart 5. **Other factors link to movements of cash**



As can be seen all, of the options available were selected, with the desire to avoid the regulatory regime in a country, and the desire to break audit trails being major factors. Again, there was a broad correlation between reasons behind the movement of cash into countries and those linked to movement in the opposite direction. The sole exception to this is capital flight, with significantly more countries reporting this as a phenomenon linked to cash leaving their country than entering it. These issues will be covered in more detail in the next section.

1.9 ESTIMATING THE VALUE OF CROSS-BORDER TRANSPORTATIONS OF CRIMINALLY DERIVED CASH

Calculation of the size of something that is by its very nature designed to be concealed, is obviously a problematic exercise, and there are no reliable figures available for the amount of money laundered globally each year. In 1998, the International Monetary Fund (IMF) estimated the figure to be between 2 and 5% of gross domestic product (GDP), but made no attempt to subdivide this amount into money laundered through physical transportation of cash and that laundered by other methods.

In 1999, John Walker estimated this figure to be over USD 2.8 trillion,[43] and in 2005 Baker estimated that more than USD 1.1 trillion was transported across international borders through illicit cash flows globally.[44] In 2009, the United Nations Office on Drugs and Crime (UNODC) calculated from a meta-analysis of the results from various studies that it was likely that the extent of all criminal proceeds was about USD 2.1 trillion.[45] From this figure, cross-border money flows related to transnational organised crime activities were estimated to be around USD 0.87 trillion (USD 870 billion) in the same year.

In order to attempt to gain a 'ball park' understanding of the scale of the problem, the questionnaire included a request for the responding jurisdictions to detail how many ML-related cash detections they had made in the preceding three years, and the total amounts detected. Only about 60% of the countries who responded to the questionnaire answered this question, and not all of these provided a figure for the number of cases and the amount.

When converted into US dollars, the figures provided by those who responded to the questionnaire totalled just over 31 000 cases of ML-related cash detection, representing a little over USD 900 million in three years, This suggests a (very approximate) minimum figure of about USD 300 million detected globally each year[46].

Studies by the USA and the UK suggest that only a very small percentage of the total cash smuggled each year is intercepted. This being the case, it does not seem unreasonable to suggest that the total amount of cash physically transported for ML purposes globally is in the order of hundreds of billions of dollars, an order of magnitude broadly comparable with the academic studies referenced above.

Clearly, the abovementioned figures are only an indication of the amounts linked to transnational illicit financial flows; however they give an indication of just how big the scope of the problem is.

43 Baker, R.W. (2005).

44 Baker, R.W. (2005).

45 UNODC (2011).

46 In 2012 the UK assessed that over EUR 500 million in high denomination Euro notes was sold by currency exchange MSBs in the UK in a twelve month period, and that the overwhelming majority of this was purchased by criminals using them to reduce the bulk of the cash for smuggling purposes. In the same period less than 1% of this figure was intercepted outbound at UK ports.

2. WHY CRIMINALS USE CASH MOVEMENT

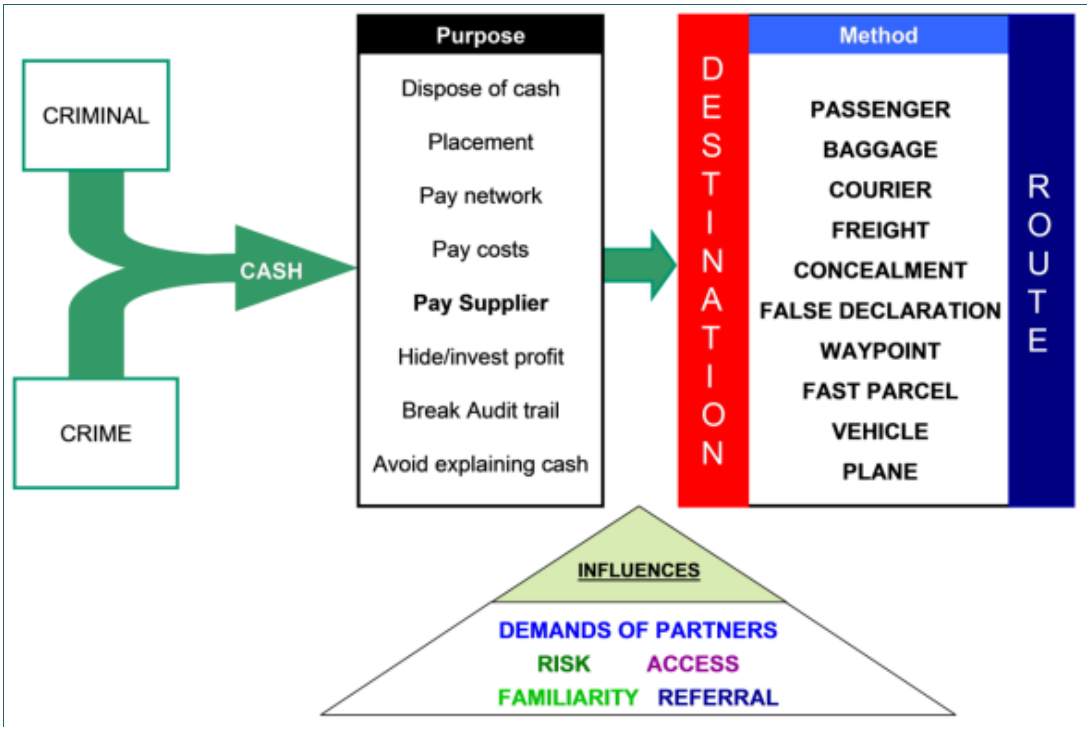
2.1 DRIVERS AND PUSH-PULL FACTORS INFLUENCING CRIMINAL CROSS-BORDER TRANSPORTATION OF CASH

Individuals move cash across borders for a range of reasons, both legitimate and illegitimate. This section seeks to explore in more detail why cash is moved for criminal purposes.

When considering why criminals seek to launder money by physically transporting it across borders, it is useful to consider what the criminal's primary objective is for doing so in the first instance. In general, these objectives can be summarised as RAISING, MOVING, STORING and USING[47] funds, and it is only after deciding on the primary objective or objectives (the 'Why') that a criminal will move on to the methods used to achieve the objectives (the 'How', and equally important, the 'Where'). These objectives are discussed more fully below.

There are numerous factors, which can be referred to as 'push factors' or 'pull factors', which will influence why criminally derived cash is moved from one jurisdiction to another and which go hand in hand with the criminal's requirement to raise, move, store and/or use the proceeds of his criminal activity. These factors are illustrated in the graphic below.

Graph 1. **Criminal decision making influences purpose and method of cash movement**



Source: UK authorities.

[47] 'Raise, Move, Store, Use' is an explanation developed by UK Law enforcement to describe processes in a number of financial crimes, including terrorism finance and money laundering.

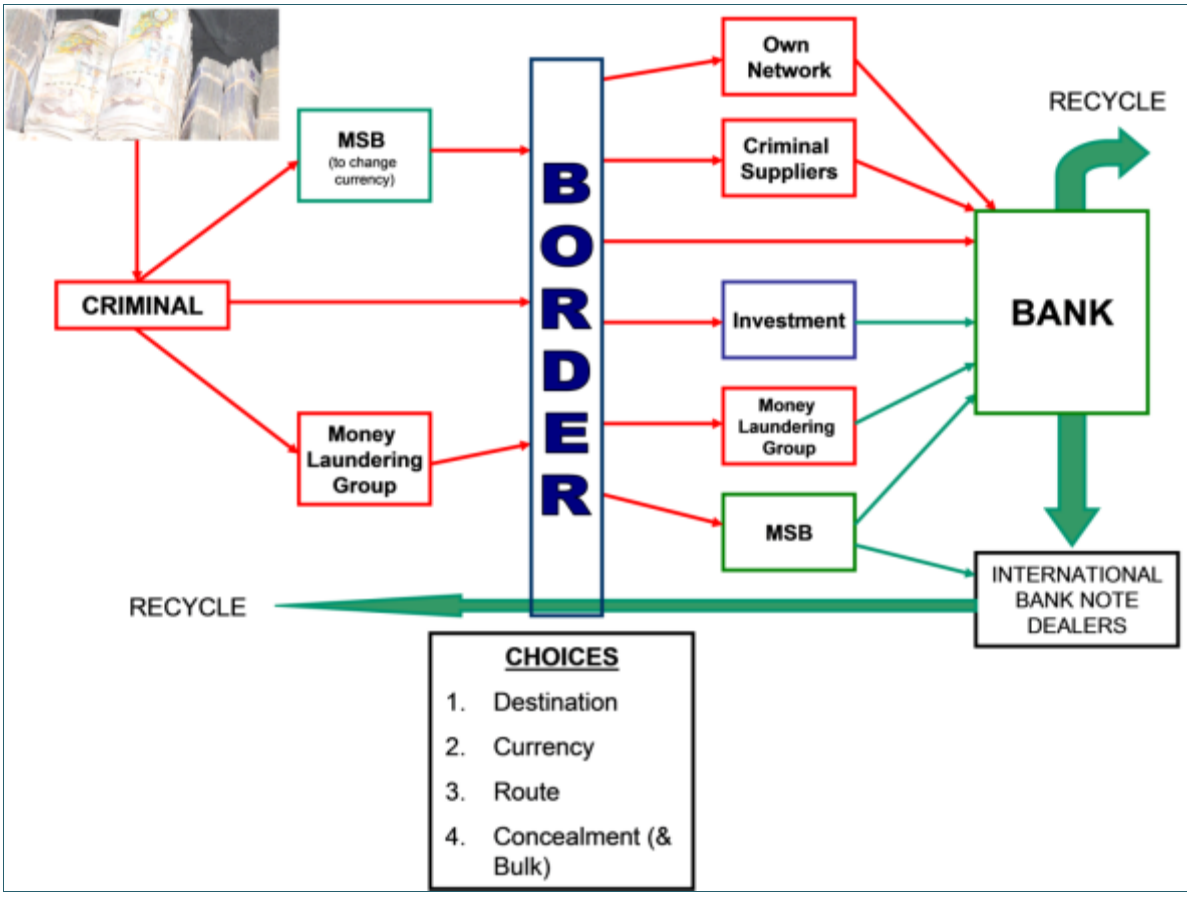
The process starts on the left hand side of the graphic, with the criminal committing the crime that generates the cash. The criminal must then decide what he wants to do with it (pay his costs, pay his supplier, invest the profits etc.)– this is the next step in the chain: the PURPOSE.

It is only once the purpose is decided that the DESTINATION will become apparent; this will be dictated by the purpose. The next step will be to decide how to get the cash to the destination; this will then lead to the next decision: the METHOD, (cash courier, concealment in a vehicle, use of freight etc.), and, closely associated and interrelated to the method and destination, the ROUTE chosen.

At all stages of the decision making process other factors will have an influence – these are shown at the bottom of the above graphic. These include: the risks of choosing one route and destination over another, the availability of (or access to) a particular method (such as a suitable vehicle), familiarity with a system that has worked before etc.

Throughout the process, the cash will follow a route dependant on the decisions of the criminal; however, ultimetely it will re-enter the legitimate fionancial system and will be 're-cycled'. The graphic below is an illustration of what can be termed the 'Cash Cycle'.

Graph 2. **The cash 'Cycle'**



Source: UK authorities.

Starting from the left, the criminal may take his cash to an MSB to exchange the cash into another currency; he may engage the services of a professional money laundering network, or he may use his own resources to move the cash across the border. These choices will depend on factors such as the destination chosen, the currency in which the cash is needed at the final destination, and the chosen routing (and whether any concealment is needed).

Once in the receiving jurisdiction, the cash may be used for a range of purposes – to pay the costs and expenses of the criminal's own network or to pay for further supplies of illicit goods, to invest in assets etc. It may also be passed to an MSB, or banked, as part of an exercise in breaking the audit trail of the money. At some point, possibly a considerable time later, the cash will re-enter the regular financial system, not necessarily due to any action taken by the criminal group. At this point, the bank will either recycle it for use within its own systems – for the purpose of stocking ATM machines, for example – or the cash will be traded on the international currency markets.

The push/pull factors impacting on criminal organisations often differ significantly from those that apply to the movement of legitimately acquired funds, and can therefore help in detailing indicators used to identify movements of criminal cash. In general terms, the main drivers of cash movement for legitimate purposes are business efficiency and cost considerations, coupled with imbalances in the supply and demand for cash (for example, tourism and business transactions, particularly in countries with cash-based economies). All businesses seek to reduce overheads and the financial sector is no different in that respect. Legitimate businesses will also endeavour to comply with local rules concerning anti money laundering (AML) and countering the financing of terrorism (CFT), (not least because failing to do so can result in significant fines, criminal prosecutions and public censure, all of which are bad for business).

Given the tendency of financial institutions to guard their reputation, it is highly unlikely that a developed financial institution or other business in the regulated sector would want to engage in any practices that might affect its 'bottom line' (at least, if it thought there was a risk of this type of activity being discovered). This being the case, it is unlikely that a bank would, for example, prefer to ship cash from a country with a high degree of regulatory oversight to one with less stringent controls for no other reason than to bank it there, or indeed to move cash anywhere without a strong business reason for so doing; as has been stated earlier, cash is heavy and bulky, and is expensive to process, ship and store securely.

Studies carried out by law enforcement agencies in the UK and elsewhere suggest that the most significant driver of cash movement for criminal purposes, in contrast, is safety (as described above, 'safety' in this context meaning in a manner calculated to avoid the scrutiny of law enforcement, or other criminal groups). Academic studies[48] suggest that criminals are more likely to be risk averse when contemplating making a gain, than when contemplating making a loss; in other words, they are likely to be more willing to take risks when seeking to hide their criminal profits from the authorities. Cost, although a factor, is a secondary consideration.

Thus, criminals are more likely to use complex series of transactions with no obvious business purpose, including withdrawing cash from a bank in one country and paying it into a bank in

[48] For example, Johnson and Payne (1996).

another.[49] Serious and organised criminals who often seek to launder large amounts of cash may see the risk of detection at air and sea ports as being lower than the risks associated with leaving an evidence trail, and having proceeds of crime reported officially when transactions are undertaken through the formal financial system.

2.2 RAISING CASH

'Raising' is the first stage of the process, and, in money laundering terms, refers to the actual generation of the criminal proceeds. In other words: committing the crime that results in the acquisition of the cash. This can be the sale of a consignment of drugs or some other illicit commodity, tax fraud, the acceptance of a bribe etc.

In the case of terrorism financing, 'Raising' has a different context. It is possible that funds used for terrorist purposes are derived from some other form of criminal activity, such as drug trafficking, fraud, kidnap for ransom etc. However, it is often the case that the funds have been derived from a legitimate source. For example, the terrorist may have some form of legitimate occupation from which he earns a salary, and he may use some of his salary to purchase components for an improvised explosive device, or to send overseas to make a donation to a terrorist cause.

Similarly, cash moved across a border may have a legitimate origin. As mentioned in Section 1.8, a number of countries identified capital flight as a reason for funds moving across their borders. Capital flight can be defined as 'a large scale exodus of financial assets and capital from a nation due to events such as political or economic instability, currency devaluation or the imposition of capital controls'[50]. The capital being moved does not necessarily have to be derived from criminal activity, although anecdotal evidence suggests that, at least in some cases, the capital being moved to a place of safety may be derived from tax fraud or other illicit activity.

The main driver for capital flight, as is suggested by the definition, is that the funds are perceived by the beneficial owner as being under threat for some reason, and the owner wants to move them to a place of safety. Reasons for the capital being moved in cash may include:

- the avoidance of strict exchange controls,
- the cash having an illicit source, or
- cultural considerations, such as the source country having a cash based economy where banks and other financial institutions are not trusted.

2.3 MOVING CASH

'Moving' refers to a criminal's desire to remove the proceeds of his criminal activity from the location where it was generated, or to move funds held in another location to a place where they are needed. The reason for moving criminally derived funds from the jurisdiction in which they were generated will vary from country to country depending on the economic and social factors there. The most prevalent drivers include;

[49] Source: based on research by UK authorities.

[50] Investopedia (nd).

2.3.1 DISTANCING THE PROCEEDS OF CRIME FROM THE PREDICATE OFFENCE.

One of the primary drivers for laundering money derived from criminal activity is to conceal its illegitimate origins, and one of the simplest methods of doing this is to remove it from the jurisdiction in which the predicate offence was committed. (In the context of this paper, this is viewed as being distinct from breaking the audit trail – see section 2.3.3).

The movement of funds in the form of cash from one country to another fulfils numerous requirements for a criminal. Primarily, it makes the tracing of the proceeds of a crime very difficult for the authorities. Police investigating a crime may never be able to identify the money generated from it if they have been unable to identify any evidence leading them to believe that the cash has been smuggled out of their jurisdiction. Even if the cash is detected in the destination country at some stage of the process, the legal and practical implications of information and intelligence exchange and evidence gathering between the countries of origin and destination can frustrate law enforcement efforts to prosecute offenders and seize the cash.

Long exposure to law enforcement techniques has led criminal groups to appreciate this situation, with the result that, in many cases, one of their first considerations is whether the benefits to be gained from distancing the cash from the crime by transporting it across an international boundary outweighs any other factors, such as the risk of detection at a border.

2.3.2 DEMAND

This is a driver closely related to the need to make use of the funds. Cash may be exported because it is needed somewhere else, perhaps to pay for further consignments of illicit goods. It may also be for some other reason, such as the desire to purchase an asset, or simply to ensure that anyone investigating the criminal's activities is unable to trace, and therefore confiscate, his ill-gotten gains. Similarly, funds may be imported because the criminal has completed a laundering process overseas and wishes to move the laundered funds to a location where they can be used, or perhaps because the country into which the cash is imported has less diligent regulatory oversight and it is easier to place the cash into the banking system there.

The reason for the movement of the cash to the second jurisdiction may also be that that is where the criminal needs it or wants it, regardless of any other factors, such as the controls in place. The local conditions in the destination country might mean that the cash can more easily be banked there. The criminal might intend to spend the money on an asset, such as a property or a vehicle, and needs the payment to come from a bank account, as a large cash payment would be considered suspicious. Similarly, a payment from an overseas bank account with no apparent connection to the purchaser might also be viewed with suspicion.

The person transporting the cash might also be doing so because he has no choice in the matter. He may not the beneficial owner of it, but that person has directed him to facilitate the transportation.

Box 3. **Bulk Cash Smuggling across the US/Mexico Border (and efforts to combat it)**

The United States and Mexico share a land border in excess of 2 000 miles in length, with 417 official Points of Entry, which poses significant problems for both countries in their efforts to combat organised crime. In recent years, the growth of Mexican groups involved in a wide variety of

organised criminal activity, including drug trafficking, organised immigration crime, corruption and weapons trafficking, has led to a significant growth in the volume of cash smuggling across the border with the US. Recent estimates as to the scale of the issue made by academics, accountancy and audit firms and the Mexican government range from USD 6 billion to USD 36 billion annually, with a generally accepted figure being around USD 25 billion. (The US and Mexico governments assess that, despite there being other methods available for moving criminal proceeds across the border, bulk cash smuggling is still used for the great majority of the proceeds generated).

In addition to the flow of drugs, illegal immigrants and firearms from Mexico into the US, there are numerous 'pull factors' within the Mexican criminal economy that contribute to the problem. Firstly, the Mexican Peso is seen by criminal organisations as being less stable than the US dollar, meaning that criminal groups prefer to have their proceeds in Dollars as there is less risk of it losing its value in the financial markets. Secondly, the Mexican criminal groups prefer to pay their bribes and operating expenses in US dollars; and finally the ultimate suppliers of the drugs that are smuggled into the US, the Cartels in Colombia and other South American countries, prefer to be paid in US dollars.

Exactly what proportion of the smuggled cash is used for the purchase of further shipments of cocaine from the suppliers in Colombia and other South American countries remains unclear; estimates range from half to 80%.

How the cash is moved

Cash derived from regional drug sales is generally taken to a central counting house in one of several US cities, including Atlanta, Boston, Chicago, and Los Angeles. The cash in its original form is usually in low denomination notes, and is converted to USD 100 or USD 50 bills, either at the consolidation points or in the original cities of sale. This is done primarily to reduce the bulk of the cash and make it easier to conceal.

Once the cash has been exchanged for larger denomination notes it is usually vacuum sealed to further reduce the bulk, and concealed in the structure of cars or articulated trucks that are hitherto unknown to law enforcement, meaning they have no reason to raise any suspicion if they are stopped. The crime groups often use the same trucks to transport cash south that have been used to transport drugs in the opposite direction.

The potential impact of any seizures is reduced by a variety of means, including regular rotation of transport vehicles and restricting the size of individual shipments to between USD 150 000 to USD 500 000, so that if any one vehicle is stopped the loss is not significant to the criminal organisation concerned and so does not significantly disrupt its operations. Typically multiple cars are sent, each carrying a relatively small percentage of any given cash shipment.

The Mexican criminal organisations constantly rotate drivers who drive the cash shipments from the consolidation centre to the designated border town close to the drug trafficking centre of the particular trafficking organisation. The cash is either aggregated and vacuum packed in a safe house on the US side of the border before being shipped into Mexico, or, increasingly frequently, the drivers continue directly into Mexico to deliver the money. This change is believed to be due to a number of factors, including a growing US law enforcement emphasis on monitoring the sales of particular equipment such as money counting machines and different types of packing equipment.

Efforts to combat the problem – The Merida Initiative.

In 2008, The US and Mexico signed the first letter of Agreement for the Merida Initiative, pledging to work together to counter the threat of drug related organised crime and the associated issue of Bulk Cash Smuggling on both sides of the US – Mexico Border. So far the US government has dedicated USD 2.3 billion to the programme, which has four 'pillars' encompassing a wide range of activities. The pillars are;

- disruption of the capacity for organised crime to operate;
- institutionalise capacity to sustain the rule of law;
- create a 21st century border structure, and
- build strong and resilient communities.

Examples of the activities put in place include;

- supply of specialised aircraft (fixed wing and helicopters) to the Mexican navy and police
- installation of a secure cross-border telecommunications system, providing a method of intelligence and information exchange between security forces;
- provision of specialised training and equipment for Mexican law enforcement and prison agencies, prosecutors and other justice sector personnel in cash detection and other matters
- provision of over 400 dogs trained to detect cash (and also drugs, weapons and explosives)
- supply of specialised non-intrusive scanning equipment enabling the detection of cash and other commodities concealed in vehicles
- supply of a sophisticated border control system providing expedited clearance for pre-approved low risk travellers
- creation and expansion of drug treatment centres and courts in Mexico.

Sources:

1. *Farah, D. (nd)*
2. *US Homeland Security (2010).*
3. *'Merida Initiative' , US Department of State (nd).*

Some countries will be net consumers of illicit goods. Criminal demand for controlled drugs in the UK, for example, is significant, which means that a large proportion of the proceeds of the sale of the drugs tends to be exported in order to facilitate more supply. However compared to the amount imported, a relatively small amount of drugs is exported from the UK to other jurisdictions. This means that inward payments for the supply of these drugs are less significant than the outwards flow, and accordingly cash smuggling outbound is more likely to be drug trafficking related than cash smuggling inbound.

The place of origin of the supply of the illicit goods will act as a push factor in deciding where cash will be smuggled to. In the case of the UK, a large proportion of the drugs consumed by users is

sourced from intermediaries in near Europe, particularly the Netherlands and Spain. Accordingly, cash smuggling related to payments for further supplies of goods are smuggled to these countries. Conversely, cash intended for use as a payment relating to the purchase of assets, such as property, is often smuggled from the UK to more distant destinations such as Dubai and Thailand.

2.3.3 BREAKING THE AUDIT TRAIL

There are clear indications from the questionnaires that a significant driver of the decision to move cash from one jurisdiction to another is to break the audit trail. In other words, it will make it difficult for anyone in the receiving country to establish that the cash is the proceeds of crime in the originating country, thus facilitating easier usage of the cash at the destination. (As referenced in section 2.3.1, breaking the audit trail in the context of this paper is distinct from the act of removing cash from the jurisdiction in which it was generated; instead, breaking an audit trail refers to the use of cash smuggling as a method of frustrating any attempt to trace the movement of funds from one place to another.)

In some cases, the transportation of the cash to another jurisdiction to facilitate placement into the regular financial system may be a precursor to its transfer by bank back to the country of origin. One of the most significant issues raised by contributors to the questionnaire was the problem of the exchange of information between different jurisdictions. This issue will be discussed at greater length later in this report (section 5.2), but the responses clearly suggest that one of the main reasons why cash is moved from one country to another is because it makes it considerably more difficult for law enforcement, and banks and financial institutions in the receiving jurisdiction to establish the provenance of the funds.

Box 4. **Physical transportation of cash to break the Audit Trail**

In November 2013 the Tunisian authorities received a suspicious activity report concerning the actions of a Tunisian national, who was resident in an overseas country but who maintained two personal bank accounts, in Euros and convertible Tunisian Dinar, in Tunisia. The report disclosed that between June and November 2013 the accounts had been credited with in excess of EUR 2.7 million, mostly in cash. The individual had no previous convictions and no business activities in Tunisia.

When questioned, the individual concerned stated that the funds were derived from the sale of property in his country of residence. Checks with customs authorities showed that the individual had declared cash when entering Tunisia from his country of residence on eight occasions between January and November 2013. The amount declared totalled EUR 2 662 000 (It was suspected that the sole reason for the cash declarations was to facilitate the banking of the cash in Tunisia – foreign exchange regulations in Tunisia dictate that cash in foreign currencies imported into Tunisia cannot be banked without being accompanied by a cash declaration form).

After the cash had been banked it was electronically transferred back to the individual's country of residence, to the accounts of corporate bodies (and on one occasion to an account held in the individual's own name). The reason given for the transfers were 'settlement of a loan' and, in the

case of the transfer to the personal account, 'sale of shares in a company'.

Enquiries carried out in the individual's country of residence revealed that he had been the subject of a suspicious activity report in May 2013 concerning a deposit of EUR 220 000 in cash to an account held by him there, which was then transferred to a family member in Tunisia. The reason given for the transfer was the purchase of machinery. The individual was also employed for a minimal wage by an agency organising temporary work placement, and had never owned or had title to any property. One of the companies that had been the beneficiary of some of the transfers from Tunisia was under investigation for tax irregularities.

The Tunisian authorities concluded that the cash was connected to tax fraud in the individual's country of residence.

Source: Tunisian authorities.

2.3.4 AVOIDANCE OF REGULATORY OVERSIGHT

Many developed countries have a highly sophisticated financial sector with rigorous regulatory oversight. This is a 'push' factor, influencing the transportation of cash out of developed countries, as it is difficult to introduce large amounts of cash into the regulated sector without attracting law enforcement scrutiny. Hence, criminals will often seek to physically move the cash to a location where it can more easily be banked.

Similarly, a 'pull' factor may be that criminals perceive the destination jurisdiction to have weaker AML/CFT controls, and that the introduction of a significant amount of cash into the financial system there will attract less attention than it would in the originating country. In fact, this perception may be incorrect and the AML/CFT controls in place at the second jurisdiction may be just as robust as those in the first. This misperception may be down to other factors, such as the second jurisdiction having a largely cash based economy where large amounts of cash are viewed with less suspicion.

There may also be certain regulatory factors in the destination country that may influence the decision to move cash there. For example, the banking sector in the destination country may apply a higher degree of confidentiality to financial transactions. This can be advantageous to a criminal; if the difficulties of the initial placement can be overcome, there can be less chance of anyone being able to establish the true provenance of the funds.

The personal taxation regime in the jurisdiction in question may also be more lenient than that in the criminal's country of birth or primary residence. If the criminal has gone to significant trouble to conceal the criminal origin of his funds, and has been able to present them as legitimate income, it makes sense that he would wish to avoid additional expense by paying as little tax on them as possible.

In the questionnaire circulated as part of the project, countries were asked to consider whether one of the reasons criminally derived cash was brought into their country was that their country is known as a legitimate international financial centre. The purpose of this question was to establish if this could be a significant factor in criminal decision-making. Anecdotal evidence suggests that proceeds of 'white collar' crime such as tax fraud, fraud against the private sector, bribery,

corruption etc. tends to gravitate to major financial centres. Fifteen countries responded positively to this question; unsurprisingly, most were countries with highly developed economies and financial sectors, such as the UK, the USA and Australia.

Box 5. **Cash Placement facilitated by the absence of legislation regarding cash movements**

Lebanese Customs identified a group of travelers (eight in total) who had the same travel pattern, being multiple trips made from a European country (A). Some of them had made frequent travels in an eight month period. Customs officers intercepted the travelers and examined their baggage.

It was found that the travelers were carrying large amounts of cash, in mixed low denomination Euro banknotes and that the amounts ranged between EUR 135 000 and EUR 600 000. When questioned, they gave different justifications for the source of the cash. The preliminary investigation findings were forwarded to the relevant Law Enforcement Authority.

Investigations revealed that the travelers/couriers used to meet in a hotel room in country A, where they were given cash by a national of country B. They were told that the money was from the proceeds of stock market investments and contract business and were paid between USD 1 500 and USD 2 000 to transport the cash to Lebanon. Investigations also revealed that the travelers/couriers worked for two individuals based in Lebanon. In the absence of further information on the origin of funds transported into Lebanon, the cash was returned to the travelers. Based on an existing Memorandum of Understanding between the Lebanese Customs and the Financial Intelligence Unit of Lebanon (SIC), put in place to capture substantially the movement of funds pending the issuance of the cross-border transportation of funds Law (currently in the Lebanese parliament), the case was forwarded to the SIC.

The SIC initiated an investigation by circulating the names of the travelers/couriers and the two individuals that hired them for their services to all banks in Lebanon. Findings revealed the existence of several accounts. Analysis on the said accounts reflected multiple cash deposits. The SIC decided to freeze related bank accounts with a consolidated balance of approximately USD 1.6 million and forwarded its findings to the General Prosecutor.

Lebanon experienced difficulties in obtaining information on any investigations that took place in countries A and B. The decision to freeze the funds was taken by the Lebanese FIU based on suspicion and on media reports from country A, detailing a money laundering scheme. This information derived from the media coverage was provided by the Lebanese Embassy in country A rather than the authorities there. As a result, no judicial action was taken in Lebanon, although the freezing of the funds was maintained.

Source: Lebanese authorities.

Box 6. **Avoidance of regulatory oversight in originating country**

A South African national arrived at Auckland international airport from South Africa in May 2011. The passenger was already of interest to the authorities due to current investigation file relating to his company and undervaluation of goods exported to New Zealand. A baggage search located undeclared cash in a false bottom suitcase and the passenger's wallets, which equated to:

- ZAR 532 000 (South Africa rand)
- EUR 200 015
- NZD 10 215 (New Zealand dollar)
- AUD 20

Total NZD 436 030 equivalent

The passenger stated that at the airport on departure, a friend gave him the cash to take back to South Africa. The passenger then said the cash was going to buy his daughter a vehicle.

The New Zealand authorities concluded that this was an attempt to bypass South African exchange controls (by illicitly holding capital off shore and not returning it to South Africa as was required), and suppress company income for purposes of tax fraud in South Africa, linked to possible tax fraud by a New Zealand subsidiary.

The New Zealand authorities alerted the South African Revenue Service of possible tax offences and breaches of the exchange control regulations committed in South Africa.

Source: New Zealand authorities.

2.3.5 ACCESSING A SERVICE NOT AVAILABLE IN THE SOURCE COUNTRY

Some case examples and responses to the questionnaire indicate that a factor in deciding to move cash to a particular location is that the destination country might offer access to a service that is not available in the country of origin. This may be associated with the avoidance of regulatory oversight, but it may also be affected by other issues. For example, it may be that foreign exchange regulations in the originating country prohibit the exchange of cash into a particular currency, or that the currency required is not available in sufficient amounts without alerting the authorities.

2.3.6 FAMILIARITY

An often overlooked factor in the decision to physically transport cash from one country to another is that this is what the criminal has always done. All human beings, criminal or not, are creatures of habit, and there is a common adage in the English language which states that 'if it ain't broke, don't fix it', which in effect means that if something works or does the job it's supposed to, there is no reason to change or interfere with it. Thus, if a criminal involved in importing cannabis from country X to country Y has discovered that a reliable and low-risk method of transporting cash from country Y to country X to pay for further consignments is to exchange it for high denomination notes and then to give it to a trusted lorry driver who is involved in legitimate freight transportation between

the two countries, he is likely to carry on using this method unless some outside influence comes into play.

The advantages to the criminal of using a tried and tested method, apart from the fact that he knows that it works and can calculate the risks, include the fact that he will be more able to calculate and therefore control his costs, and he will also be able to establish what went wrong in the event that the cash is lost or seized.

2.3.7 REFERRAL

Another important, but often overlooked, factor in criminal decision-making is the influence of other criminal groups. Often, criminal networks involved in a similar activity exist in parallel to one another, and the individuals within those networks know each other and may even migrate from one network to another. As a result, methods and techniques used by one group become known to another, and may even be recommended by one group to another.

Using the above example, a criminal group involved in cocaine trafficking from country X to country Y may approach the group involved in importing cannabis, and ask that they use the same driver to export cash. They may also decide that the system is sound, but recruit someone else to move the cash on their behalf. Similarly, if the cocaine trafficking group needs to move cash to a third country they may decide to use a driver involved in legitimate freight transportation to that country. Likewise, if a criminal network has used the services of a specialist money laundering group to move money on its behalf, an associated criminal network may ask to be introduced to the money laundering groups to use its services.

2.4 STORING THE CASH

'Storing' refers to a criminal's desire or need to keep funds in a safe location ('safe' in this context meaning beyond the reach of law enforcement, or other criminal groups). This may be because the money is to be used as a 'contingency fund' in the event of a crisis, or simply because the relevant criminal enterprise has been so successful that the amount of cash held exceeds the criminal's laundering ability.

The decision to store funds in the form of cash may also affect the nature of the cash used for this purpose. The ECB has frequently stated[51] that one of the principal uses of the EUR 500 and EUR 200 banknote is for store of value purposes. A larger value can be concentrated in a smaller volume, which makes the cash easier to keep in a safe, for example (although research conducted as part of this project shows that the same high value/low volume advantage is frequently used by criminal groups for the purposes of moving large amounts of criminally derived cash across international borders in small concealments).

It is important to emphasise that the use of cash for store of value purposes, and the cross-border transportation of cash in order to facilitate this, is common and is not necessarily linked to any form of criminal activity. As stated in section 1.8, a common reason for cross-border transportation of

[51] Most recently in a speech by Yves Mench, Member of the Executive Board of the European Central Bank, in a speech at the Bargeldsyposium of the Deutsche Bundesbank, Frankfurt 19 May 2014.

cash is capital flight. Although there are occasions when the driver for this will be of an illicit nature, such as tax fraud, the funds may also have an entirely legitimate origin and its cross-border transportation is simply to avoid market events such as the devaluation of a currency.

Any type of currency can be used as a store of value, but the most common ones are the major international currencies such as the US dollar and the euro. These currencies are seen as more stable and less prone to currency speculation and significant variations in exchange rates. In addition, there are numerous countries in the world whose economies are significantly 'dollarised'[52] or 'euroised'[53] , or where the usage of these currencies for various purposes, including tourism, is widespread. As a matter of course, it is useful for stored cash to be useable in as many places as possible without the need for conversion into a less common currency, with the costs and difficulties that this would entail.

2.5 USING THE CASH

'Using' refers to the use of the criminally derived funds to purchase assets, or for normal, licit day-to-day transactions. It also refers to the use of criminally derived funds to generate further criminal proceeds, for example by using part of the proceeds of the sale of a shipment of drugs to pay for the next shipment. If the use of the cash at the destination is the primary objective, then there will be influencing factors that the criminal will need to consider when deciding how and where the money must be moved. There is little point in placing the cash in a financial institution, if the criminal's supplier in an overseas jurisdiction needs the payment in cash, or does not have access to an account into which it can be transferred.

For example, the cash may need to be declared on import into a jurisdiction in accordance with local laws and regulations, in order to give the appearance of a legitimate origin or to facilitate its introduction into the banking system. It may be held in low denomination notes, to make it easier to spend (retail outlets will usually not accept, or at least will question, very high denomination banknotes) and it may be kept or used in smaller amounts that are more easily explainable – by the sale of a vehicle, for example.

Likewise, if the reason for moving the cash is to pay a supplier for further consignments of goods, or to pay the expenses involved in the trafficking of a commodity, the supplier may need the cash in a different currency to the one in which it is currently held. If this is the case, then the criminal will need to have access to a currency exchange facility as well as a method of transportation.

This is the case in the UK due to the fact that, in contrast with most of the rest of Europe, it uses its own currency. This can be a complicating factor for criminals sourcing drugs and other illicit goods from near Europe as the European supply chain for such goods frequently requires payment in local currency. This impacts on the methods criminals in the UK use to transport cash as they will often need to exchange local currency into Euros as a precursor to smuggling it out of the UK. As a result, this has led to a significant and otherwise unexplainable demand for large quantities of high

52 Examples include Egypt, Somalia and several South American countries.

53 Examples include Kosovo and Montenegro – source as footnote 27.

denomination Euro banknotes in the UK, and a criminal market has developed to satisfy this demand.

The other major use for criminal proceeds in another jurisdiction is the purchase of assets. Assets can be used for a number of purposes, all of which are desirable for criminals. The first, and most obvious, is that the criminal wishes to enjoy the benefit of his criminal activities, by purchasing a large house in a desirable location, an expensive car, a gold Rolex watch or similar. Second, the criminal may wish to use an asset as a store of value. Property values in most major financial centres, such as London and New York, are either stable or rising steadily and purchasing a property, even if it is left vacant, can result in a healthy return on the criminal's investment in a relatively short space of time. Third, using cash to purchase a property, which is then sold soon afterwards, has the advantage of turning the cash into a balance in a bank account from an ostensibly legitimate source, thus aiding the laundering process, and finally, a title to a property (or any other high-value asset) can be exchanged between criminals as a way of settling a debt.

If the purchase of an asset is the intended use, then the cash will have to be imported into a jurisdiction in such a way that its introduction into the banking system arouses no suspicions. To this end, a criminal may choose to declare the cash on entry and try to use the cash declaration to deceive bank staff by presenting it as 'proof' that the cash must have a legitimate origin.[54] It may also be necessary to transport the cash into a jurisdiction with relatively lax regulatory oversight first, in order for it to be banked there, and then transferred electronically to the ultimate destination.

Box 7. **Cash smuggled to other jurisdictions for investment in property**

This case concerned a very large ML organisation from Colombia and the Netherlands, partly family, led by a woman of both Spanish and Colombian nationality. The group directed Ecuadorians, Colombians and Venezuelans who travelled the world with suitcases full of money. The money was taken to Spain and to various South American countries, where it was used for investments in property. The group probably worked for various clients. The main suspect was arrested at Schiphol airport in 1996 and sentenced to five years' imprisonment for drug trafficking. Her brother was arrested in 2003 carrying EUR 7 million.. The suspects alternately lived in Cali, Colombia and the Netherlands for ten years. The suspects were not (or no longer) engaged in cocaine trafficking themselves.

The investigation showed that the suspects organised money transports for more than EUR 50 million with profits of over EUR 5.5 million. A few money transports were intercepted. Several suspects also stood trial for drug trafficking preparations and possession of drugs and firearms. More than one million euros were found in the house of one of the suspects, which was hidden above a ceiling tile and in a vacuum cleaner bag.

The case also resulted in the seizure of: 38 premises in Cali, Colombia, money, money counting machines, passports, weapons and the contents of accounts.

[54] See also sections 3.5 and 5.1.

The technique used for smuggling the cash

Cash, probably originating from cocaine trafficking, was flown by the various suspects to South America. Money launderers organised money transports from the Netherlands in order to pay cocaine traffickers in Colombia.

For this purpose, couriers were used who were paid travel and subsistence expenses, and were put on a plane with prepared suitcases and backpacks. These were usually Colombian women who had little money and were given the chance to travel to their country of birth. Moreover, the women were paid well for their services as a courier.

In one case, a woman was intercepted carrying EUR 204 000 in the telescopic handles of her suitcase.

The suspects collected large amounts of money, preferably in convenient EUR 500 notes. They rolled the money, put carbon paper around it and hid it as a large roll inside the telescopic handles of the suitcases.

Source: Netherlands authorities.

A significant factor in a criminal's decision to transport cash to another country may be the ease with which he can use it to purchase high-value items in that country. Many countries consider the use of cash to purchase assets, such as cars, as a ML risk and/or a vehicle for tax fraud (although others disagree that this is the case) and have introduced legislation restricting the amount of cash that can be used in a single transaction. Within the EU, there is a wide variation of practices. Some countries place a limit on the amount of cash that may be used to purchase all goods, or certain types of goods (these limits vary between EUR 1 000 and EUR 15 000), whilst some countries impose no limits at all. Other countries do not impose a limit, but instead require businesses accepting large amounts of cash to implement procedures designed to identify (and discourage) the use of cash by criminals to purchase high-value goods.

3. METHODS AND TECHNIQUES

3.1 ROUTES AND ROUTE SELECTION

The choice of the route to move the cash between jurisdictions will depend on a number of influencing factors and will be determined only after the purpose, destination and method of transportation have been decided. Thus, the decision-making process for a criminal wishing to move EUR 100 000 from the Netherlands to Spain to pay a supplier will be different to that used by another criminal wishing to move the same amount of money from the UK to Spain. The criminal in the Netherlands already has the cash in the form of euros, and may simply decide to put it in a holdall in its existing form, in low-denomination notes, put it in the boot of a car and drive it across Belgium and France land borders into Spain. This choice is more likely than transporting it by air, as EUR 100 000 in low-denomination banknotes is quite heavy and bulky and would be easily detected during baggage scans at an airport. In theory, the cash could be exchanged for high-denomination banknotes, but this would bring with it the risk of being questioned at a bank or financial institution and/or reported to the authorities and inevitably would attract additional costs.

In this case, the choice of route will therefore be influenced by the fact that air transport is a less viable option. Also, under the Schengen agreement, there are no restrictions on movements within the EU, and there are therefore no risky manned border crossings that have to be negotiated during the journey. Millions of vehicles make similar journeys every day and there is very little chance that a customs or police official will select the wrong car for inspection, especially if obvious red flags are avoided, such as ensuring that the car is in good condition and speed limits are adhered to.

For the criminal in the UK, a number of other factors apply. The amount of cash, the purpose and destination are the same, but the method, and therefore the route, will be different. The UK is also an EU member state, but being an island and using its own currency are factors that come into play. The cash will be in the form of low denomination British pounds and so will need to be exchanged for euros in the UK first. Given that this has to be done anyway, the criminal may choose to obtain the euros in high-denomination notes from a 'friendly' MSB at the same time, to facilitate concealment. All of the UK's borders are manned at least some of the time so there is a much greater risk that the cash may be detected by law enforcement at the UK's borders. Concealment of the cash is therefore much more important. Once the cash is in the form of high-denomination notes, and is now much reduced in bulk and weight and more easily concealed, the criminal may choose to give the cash to an air passenger on a tourist flight to Spain. Alternatively, if the risks of discovery by customs officials at the airport were considered to be too high, the criminal might choose to drive it to Spain instead via the channel tunnel and through France (however this would take much longer and would have no cost advantage).

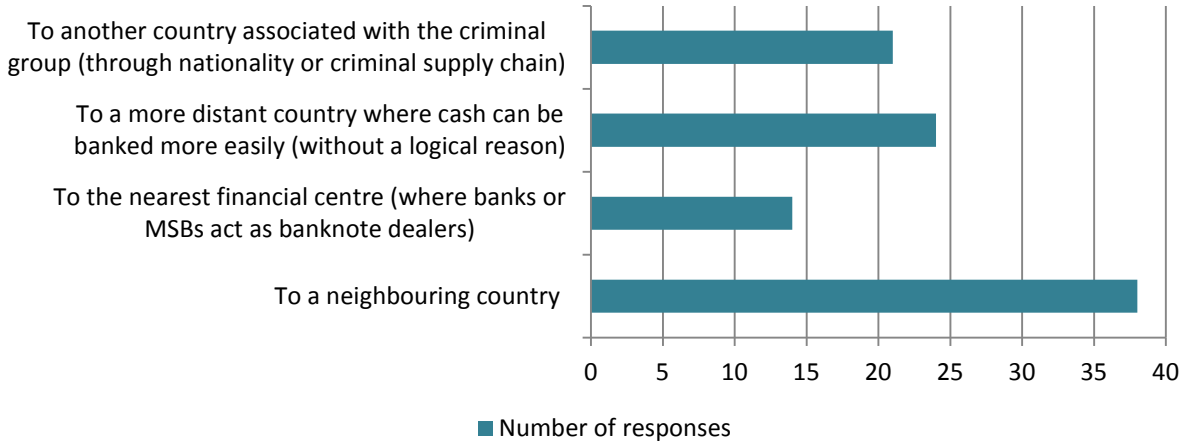
In the same way, any change in the currency and nature of the cash, the intended purpose, destination and method will have an effect on the route the criminal chooses. This being the case it is by no means guaranteed that criminals in the same country, and shipping the same amount of cash to the same destination will use the same routes and methods. Likewise, there is no guarantee that cash derived from the same type of predicate offence will always be transported in the same

manner to the same place. It is not possible to state with certainty that, for example, because cash has been detected in the false bottom of a suitcase destined for Spain, it is derived from drug trafficking, or that all proceeds of cigarette smuggling will go to a particular country.

3.1.1 OUTBOUND TRANSPORTATIONS OF CASH

Two questions on the questionnaire dealt with the issue of the destination and purpose of outbound criminal cash and the purpose and origin of inbound criminal cash. In respect of cash exported, the intention of the question was to establish if it was more common for the cash to be transported only as far as a neighbouring country rather than further afield, and if this was the case, what the reasons might be. The graphic below illustrates the responses.

Graph 3. **Where cash is exported and ML is suspected, where does the cash go?**



All of the choices offered received a significant positive response, and many countries selected more than one option.

The data suggests that the most popular option for criminals (38 responses) is to move the cash to the nearest country; more countries selected this option than those indicating the purpose was to make it easier to bank the cash or related to the ethnic make up of the crime group. As discussed in section 2.3.1, a possible explanation for moving the cash is the desire to distance it from the place where it was generated, rather than the desire to avoid regulatory scrutiny or to make a payment related to the criminal supply chain.

This being the case, it seems likely that the principal desire of a criminal group is that, having made a large amount of money by commiting an acquisitive crime in one country, they wish to take steps to prevent the authorities in that country from detecting their ill-gotten gains by making it harder to locate them. Transporting the cash to the nearest available country is the easiest, and presumably cheapest way of achieving this aim.

The significant number of responses for these other options, however, does demonstrate that the ability to place the cash in the legitimate financial system, and the necessity to pay for further illicit goods, or to pay the expenses incurred in transporting them, are significant influencing factors in route selection.

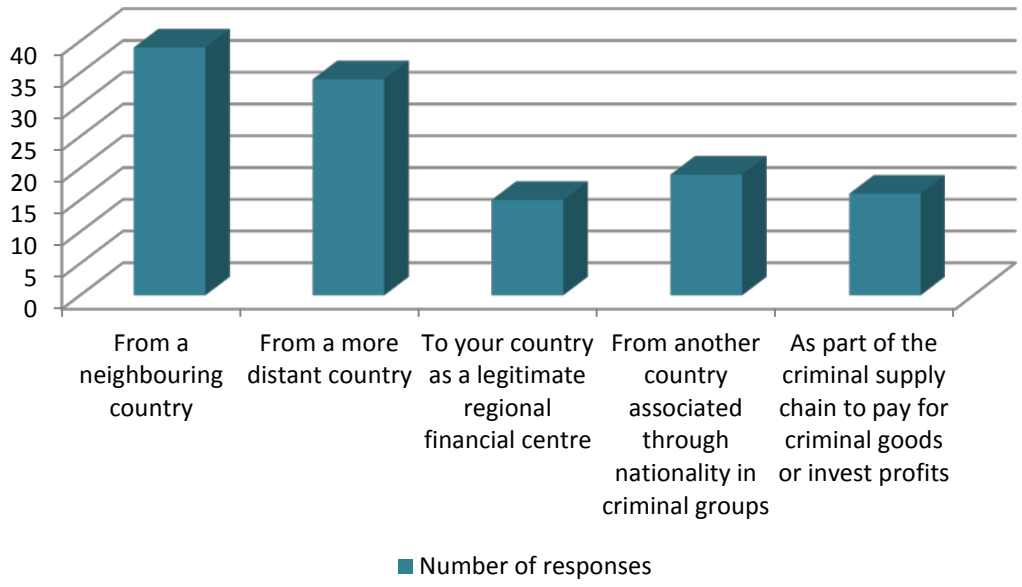
Fourteen countries believed that cash was sent to the nearest financial centre. This closely correlates with the number of countries (15) who believed that their country is a legitimate regional financial centre, and that cash was brough into their country because of this. Respondents to this question included France, Italy, the Netherlands, Panama, South Africa, the UK, and the USA, suggesting the major financial centres do act as a 'pull factor' for cash derived from criminality. This is understandable, as regional financial centres tend to be politically and economically stable, and have a greater number and greater range of small, medium and large businesses located there. Correspondingly, they have a larger concentration of banks and other financial institutions, meaning that the criminal would enjoy more opportunities for disposing of large amounts of cash without drawing attention to himself.

Regional financial centres are usually major cities such as Dubai, London, and New York. These cities are often seen as places of opportunity for the less well-off from many countries. This tends to make them more ethnically diverse, meaning that criminal groups that are ethnically homogenous are more likely to 'fit in' without attracting attention.

3.1.2 INBOUND TRANSPORTATIONS OF CASH

The most commonly selected options in respect of origin and purpose of inbound movements of criminal cash broadly correlated with those for outbound cash (see graphic below). In particular, the most commonly encountered point of origin for inbound cash was a neighboring country.This lends more weight to the theory that the primary driver behind the cross-border transportation of criminal cash is to distance it from the place where it was generated. Moving it the shortest distance possible whilst achieving that aim is the preferred option. However, the fact that nearly as many countries believe that cash is also imported from more distant jurisdictions may indicate that cost and convenience can be less important than the actual distancing process.

Graph 4. **Where cash is imported and ML is suspected, where does the cash come from?**

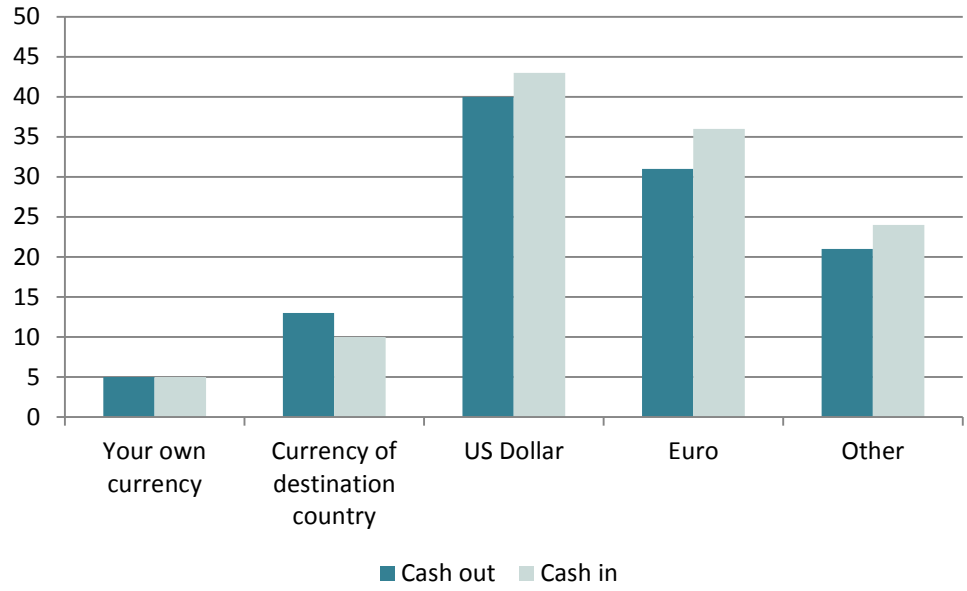


Less significant than the removal of the cash from the jurisdiction where it was generatedThe questionnaire responses illustrated in the above graphic indicate thatan association between a destination country and the ethnicity of a crime group (an ethnically homogenous crime group operating overseas but importing cash into their country of origin, for example), or the need to pay suppliers or expenses, are important considerations.

3.2 CURRENCIES

Countries were asked to identify the currencies most often encountered in consignments of suspected criminal cash transported out of and into their jurisdiction. The graphic below summarises the results.

Graph 5. **Currencies most often encountered in suspected criminal cash transport**



Perhaps unsurprisingly, overwhelmingly the most frequently encountered currencies were the US dollar and the euro. A large number of currencies were identified in the 'Other' category, of which the most frequently encountered were, in order of frequency, the British pound, the Swiss franc and the Chinese yuan, the Canadian dollar, then the Hong Kong dollar, Japanese yen and Russian ruble. All of these currencies were identified in jurisdictions other than where they are used as the main currency, indicating that the cash concerned had either been smuggled into that jurisdiction, or that it had been exchanged into this currency before the transportation took place.

Two features that nearly all of the most frequently encountered currencies have in common are that they are either noted for their long-term stability[55], or are widely used and traded, or both. Clearly, it makes sense for persons wishing to hold money in the form of cash for a prolonged period of time to choose a currency that is going to hold its value on international currency markets and is useable in the widest range of countries. The above currencies are those that best fit those requirements.

[55] The 'top six' are often acknowledged to be the US dollar, the euro, the Japanese yen, the British pound, the Swiss franc and the Canadian dollar (Lee, R., 2013).

Altogether, a total of 34 currencies, other than the US dollar and the euro, were identified in consignments of suspected criminal cash. One of the most striking features of the currencies identified was their regional variation - currencies such as the Saudi riyal and the Qatari riyal were only seen in the Middle East, for example. Moreover, the 'other' currencies identified were very often those of the country immediately adjacent to the country discovering them. Again, this gives weight to the theory that, in many cases, criminally derived cash is simply transported to the nearest possible foreign jurisdiction as a method of separating it from the crime that generated it.

3.2.1 CASH REPATRIATION

Where a country uses its own unique currency, it has the opportunity to gather data concerning the jurisdictions from which its currency is repatriated. This in turn has the potential to tell where its cash is exported to, and by extension, why. Cash in a currency that cannot be used in a jurisdiction, perhaps received in the course of a currency exchange transaction, is generally repatriated to the issuing country by being traded, often as part of a basket of currency, on international currency markets.

The British pound, for example, is only used as currency in the countries that make up the United Kingdom (England, Scotland, Wales and Northern Ireland) and various overseas territories with British ties such as the Channel Islands, the Isle of Man, Saint Helena, Tristan de Cunha etc. Therefore, with very few exceptions, any British pounds found in an overseas jurisdiction must have been transported there or, possibly, hoarded, or traded in the course of currency speculation (the British pound is the fourth most traded currency on international markets and, in terms of value, the third most held in reserves).

In 2008, the UK authorities conducted an in-depth exercise to study the repatriation of the British pound from overseas, drawing on information from customs data and banks and other financial institutions involved in trading on currency markets. Notwithstanding the popularity of the currency as a store of value and on international currency markets, and the distorting influence of regional cash consolidation centres such as Austria and Dubai, studying the phenomenon revealed a lot about where cash was transported to illicitly.

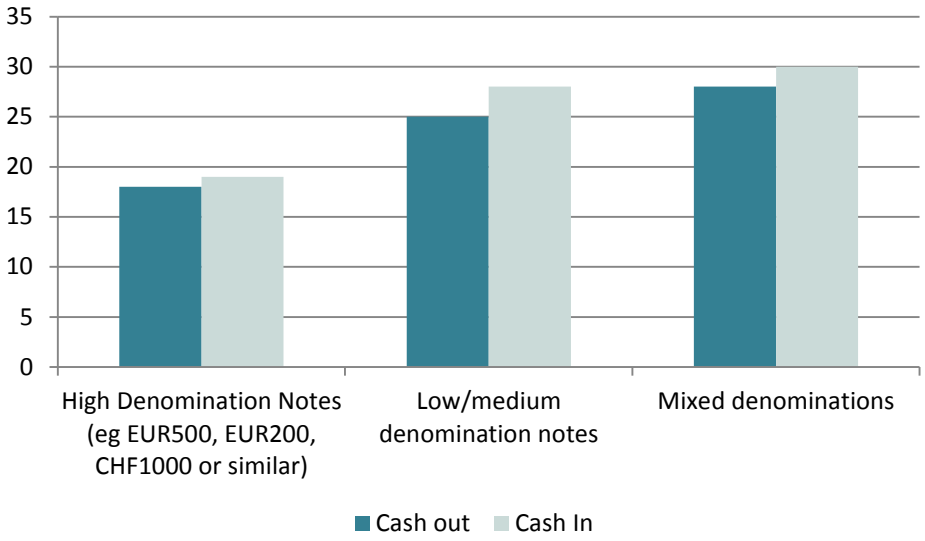
For example, the exercise showed that the amount of British pounds being repatriated from southern Spain was far in excess of what could be justified by international cash trading or the tourist trade. It was also far in excess of what was being repatriated from similar sized countries with similar economies (such as France and Germany). After further study to rule out other factors, the conclusion was that southern Spain was a popular destination for criminally derived cash smuggled out of the UK.

Similarly, in-depth study of data provided by a financial institution involved in international currency trading identified that a large amount of British pounds was being repatriated to the UK from northern Belgium. Law enforcement bodies requested further information from the financial institution who, from their internal paperwork (such as packing lists) were able to identify three branches of a particular bank where the cash had entered the Belgian financial system. When the locations of these branches were plotted on a map it showed that they were in close proximity to an industrial estate known as a consolidation and distribution point for smuggled cigarettes, indicating that the cash could have been linked to excise duty evasion.

3.3 DENOMINATIONS

One of the questions in the questionnaire asked countries to specify what denominations of notes they encountered in consignments of suspected crime-linked cash. The question covered cash both exported and imported, and the options offered were high denominations (E.g. EUR 500, EUR 200, CHF 1000 or similar), low/medium denominations, or a mixture of both. The answers are summarised in the graphic below.

Graph 6. **Denominations encountered in consignments of suspected crime-linked cash**



As can be seen from the data, high-denomination notes are frequently, but not always, encountered. Low/medium denominations or a mixture of both high and low denominations are more frequently seen. There is also a significant disparity between countries which might otherwise be expected to show similar results. For example, the UK reports that far more high-denomination euro and US dollar banknotes are sold by MSBs in the UK than can be explained by legitimate demand, and that there have been many convictions for money laundering of MSBs knowingly selling these notes to criminal groups whose main reason for purchasing them was to reduce the bulk and weight of criminal cash to a minimum to facilitate cash smuggling. A similar preference by criminals of EUR 500 and EUR 200 banknotes is noted by the authorities in the Netherlands.

Box 8. **The sale of high-denomination banknotes to criminals to facilitate cash smuggling**

In the UK in recent years, there have been numerous money laundering prosecutions of Money Service Businesses (MSBs) selling high-denomination euro and US dollar banknotes to persons they knew or suspected to be involved in criminal activity (usually drug trafficking). The evidence in these cases shows that the banknotes purchased were smuggled out of the UK and the reason high-denomination banknotes were used was to reduce the bulk and weight of the cash to a minimum to facilitate concealment.

A significant case concerned a person, K, who between 1994 and 1996 had operated an MSB in the UK which had sold a total of GBP 70 million worth of high-denomination banknotes to criminal customers (in pre-euro days, these were Dutch guilders, Austrian schillings, Deutschmarks etc.).

Almost none of the purchases of these banknotes from currency suppliers, and the onward sale to the criminal customers, were declared in the records of his business. K was prosecuted for money laundering, convicted, and sentenced to 14 years imprisonment (the highest sentence available for money laundering in a UK court).

K appealed to the UK High Court and in 2007 his conviction was quashed on the basis of a technicality. In the meantime he had been released from prison, and whilst he was waiting for the result of his appeal, he set up another MSB, in the names of his wife and son, and almost immediately re-commenced purchasing high-denomination foreign banknotes and selling them to criminal customers.

Law enforcement officers in the UK investigating the criminal activities of a separate MSB involved in similar activity chanced upon evidence indicating that K had re-commenced his previous activities. A separate criminal investigation was launched, and evidence was gathered of known drug traffickers visiting K's MSB and purchasing large amounts of high denomination euro and US dollar banknotes. K was arrested and his business was searched. The new investigation revealed that, once again, almost none of the purchases of the high-denomination banknotes from currency suppliers and the onward sale to customers were detailed in K's records. This time, the total value of the banknotes sold to criminal customers over an 18-month period was approximately GBP 190 million.

Faced with overwhelming evidence, K pleaded guilty to money laundering charges and was sentenced to 11 years imprisonment. His wife and son pleaded guilty to charges in respect of breaches of the regulations for running an MSB.

Source: UK authorities.

In Germany, however, the most common ocurrence is for seizures of low to medium denominations in the context of ML linked to drug proceeds generated within the EU, in particular when Spain, France, Italy, the Netherlands and Germany are involved. The German authorities have evidence that cash of this nature is seized in its 'raw state', apparently because criminals are deterred from changing small to high-denomination notes, due to the risk of being detected and reported by the financial sector in accordance with AML/CFT rules. Furthermore, during these AML operations, the cash is not found hidden in the car, apparently due to the fact that there are regular controls, for example, on the transit motorways from Spain to Germany via France. In the context of such controls, cash smugglers learned very quickly that if money is hidden in a car in the same way that drugs would be hidden, the smugglers could not credibly refer to any legal business as the source. Hiding the cash and the use of high-denomination notes therefore no longer play a signficant role in their plan. This identified modus operandi therefore contributes to the absence of high-denomination notes in cash payments of thousands of euros as an indicator of money laundering in cases as described in this paragraph.

Box 9. **Physical transportation of cash to break the Audit Trail**

Case review and analyses on investigation in ML through cash couriers associated with export of second hand cars.

Funds originating from drug trafficking operations in Europe are gathered and temporarily stored in different European countries. Money laundering groups/ organisations arrange the collection of those funds by cash couriers. The funds are physically transported from one European country to another (e.g. from Spain or the Netherlands to Germany). The transportation of funds is conducted by car on a weekly basis, the funds are not specially concealed (for example, packed in plastic bags and stored under the front seats). The value of the transported sums varies between EUR 40 000 and EUR 500 000; less frequently it goes up to EUR 1 million. The majority of the detected funds are regularly in small denomination of EUR 10, EUR 20 or EUR 50 notes, which is a clear indicator of drug sales on retail level. When running into a cash control the cash couriers regularly try to explain the transportation of the funds with an intended purchase of used cars or building machines.

Once in Germany, the cash couriers distribute the money to different small companies, mostly operating in the second-hand car market. All those companies are managed by the cash couriers, or other persons, with the same ethnic background. Being very cash-intensive, the companies are used as a simple legitimation for their legal income in Germany as well as cover up for their ML-activities. There is always an intermingling of legal and illegal businesses (e.g. integration of drug-related money as well as tax fraud)

Investigation showed that the funds carried by the cash couriers were up to ten times higher than the annual turnover declared to the German Tax Authorities.

The cash is used for purchase of building machines and cars on the second hand marked (grey market) in Germany which are then legally exported to the Middle East. The settlement for the exported goods is carried out over foreign accounts which belong to the car companies mainly located in the financial centers in the Middle East. If cash is needed, couriers will bring the money back into Germany with a proper declaration to the customs authorities. The customs declaration forms are used to legitimise the drug funds transported from various European countries to Germany later on.

The predicate offences for this typological scheme have been trafficking of heroin as well as cocaine.

Source: German Authorities.

The answer to these apparent discrepancies lies in the fact that, once again, other factors influence what denominations will be used when contemplating money laundering through the physical transportation of cash; these are the purpose, destination and method. An in-depth study of the questionnaire reponses and the case examples reveals that high-denomination notes are most likely to be encountered when there is an element of concealment involved in the transportation of the cash.

The reason for this is self evident and has already been discussed in this report. Taking the British pound as an example, measurements of the size and weight of the relevant banknotes shows that GBP 250 000 in 'street cash', a mixture of GBP 10 and GBP 20 notes, weighs between 15-20 kg and is bulky enough to fill an average size sports holdall. The same value in EUR 500 notes would weigh about 0.6 kg and would fit in a fat envelope. High-denomination notes therefore facilitate concealment of large values of cash; by the same token, if the concealment is already available (such

as a specially constructed 'hide' in a vehicle, for example), the use of high-denomination notes means that it is possible to transport a far higher value at a time.

Box 10. **Examples of the size and weight of the relevant banknotes**

Source: UK authorities.

Suitcase filled with EUR 500 banknotes – 12 000 notes, value EUR 6 000 000. The cash weighs about 12 kg.

Source: Netherlands Authorities.

3.4 METHODS OF PHYSICAL TRANSPORTATION OF CASH - PASSENGERS AND NATURAL PERSONS

As has already been stated, it is clear from the responses to the questionnaire most countries directed the bulk of the resources dedicated to tackling money laundering through physical transportation of cash towards natural persons. This may be as a reflection of the wording in Recommendation 32, which is titled 'cash couriers'.

FATF Recommendation 32. Cash couriers *

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

However, the "Glossary of specific terms used in this Recommendation" in the Interpretive Note to Recommendation 32 confirms that the scope includes shipment through containerised cargo and mailing:

Glossary of specific terms used in this Recommendation

Physical cross-border transportation

refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation:

(1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle;

(2) shipment of currency or BNIs through containerised cargo or

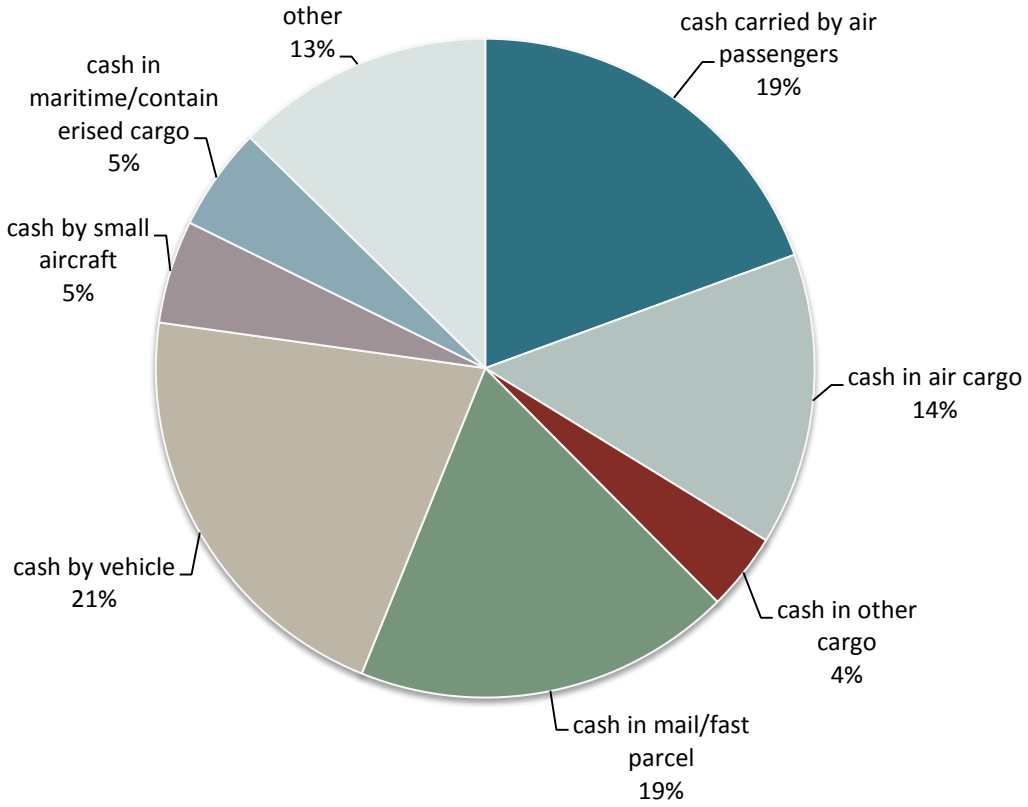
(3) the mailing of currency or BNIs by a natural or legal person.

While the FATF Recommendations cover cash transported by natural persons, mail and cargo, there is a focus on 'cash couriers' both in the title of Recommendation 32 and in its correlating interpretative note.

This focus on 'natural persons' may help to explain why from the questionnaires it appears that many jurisdictions seem to consider that their obligations under Recommendation 32 are limited to have in place a disclosure or a declaration system for transportation of cash by natural persons.

The questionnaire asked countries to rank the methods of cross-border transportation of cash they encountered most frequently in descending order. The graphic below illustrates the results.

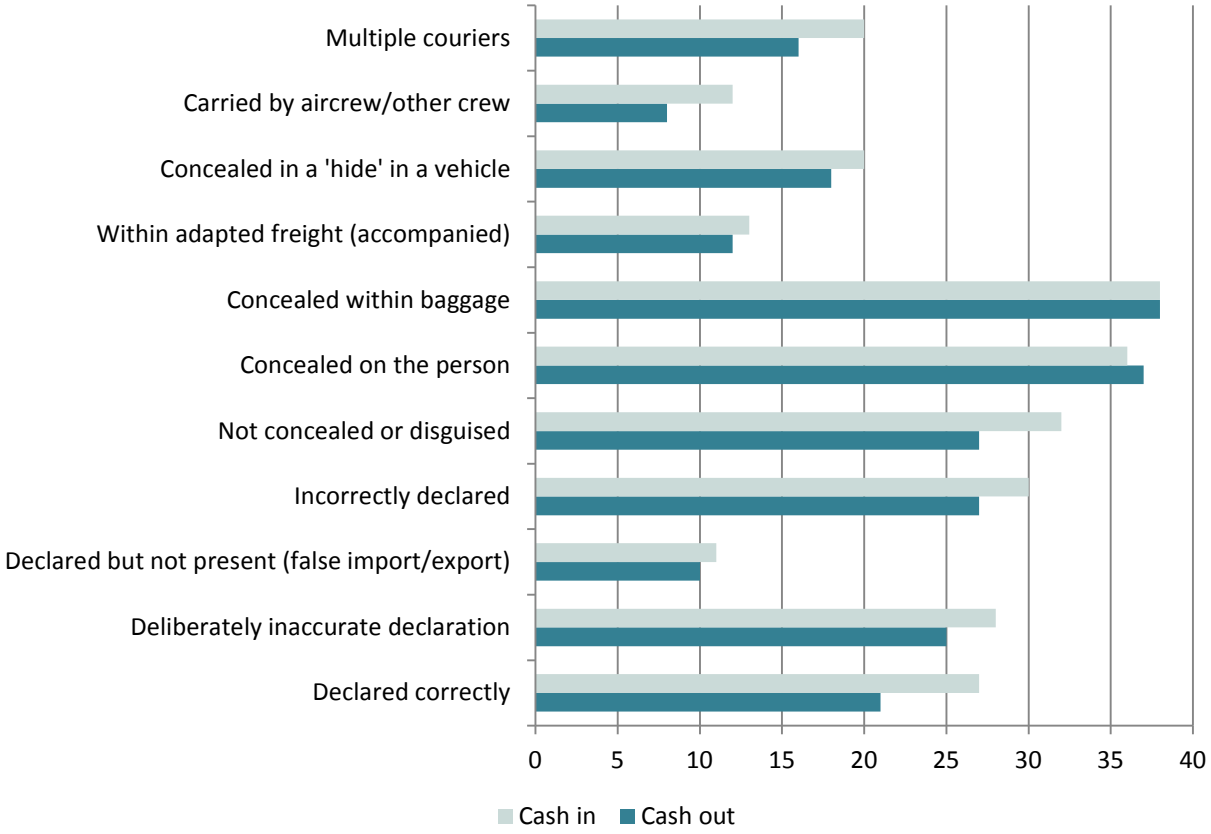
Graph 7. **Most frequently encountered methods of cross-border transportation of cash**



These results show that, in actual fact, many countries do encounter cash movements in air & other cargo and mail (37%). This would imply that countries are choosing to direct their resources against natural persons despite them knowing that cash is moved in other ways. This may indicate an incomplete awareness of the risks involved.

Countries were also asked to detail what, in their experience, were the most common techniques used by criminals when physically transporting cash. The data in respect of natural persons is expressed in the graphic below; it shows that the techniques encountered are broadly similar for cash detected both inbound and outbound.

Graph 8. **Most common techniques used by criminals physically transporting cash**



The techniques can be broadly split into the following categories; criminal cash being declared in some fashion; no attempt being made to conceal criminal cash; concealment on the person (internally, 'body packed' or within items of clothing); concealment in a passenger's baggage; and concealment within vehicles and adapted freight, these techniques are discussed in more detail below.

3.5 CASH DECLARATION REQUIREMENTS

As set out above, it is a requirement of FATF Recommendation 32 that 'countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or a disclosure system' and most countries that are committed to the FATF Recommendations have introduced such a system. The wording of Recommendation 32 makes the purpose of these systems clear; it is to assist in the detection of both licit and illicit cross-border transportation of cash and BNIs, and the wording of the recommendation makes it clear that countries should also have effective and proportionate sanctions in place for breaches of the declaration requirements.

It is, however, clear from both the responses to the questionnaire, the case examples submitted and the discussions during the typology meetings in Qatar in November 2013 and December 2014 that criminal groups are finding ways of turning cash declaration and/or disclosure systems to their

advantage. One issue appears to be that in some countries, passengers completing a cash declaration do not routinely have the declaration checked by the authorities to see if what is written on the declaration form matches with reality (in some countries this is hardly ever done). There is also very little control exercised over the 'customer copies' of the cash declarations (most are completed in at least duplicate, with at least one of the copies being retained by the declarant), meaning that there is nothing to stop the same form being re-used (see bullet 3 below).

There are numerous ways in which a criminal can use a cash declaration requirement to his advantage. These are all real examples of techniques that have been encountered by countries responding to the questionnaire, or taking part in discussions at meetings of the project group;

- **Cash declarations used to lend a veneer of legitimacy to criminal cash.** Countries which acknowledge that they rarely check cash declarations report numerous examples of persons regularly importing large amounts of cash from jurisdictions linked to drug trafficking, who complete a cash declaration on entry into a country, then take the cash to a bank and pay it into an account. When challenged by bank staff, they produce the cash declaration, which the bank staff accept as 'proof' that the cash must have a legitimate origin as it was declared to the authorities and not seized. Cash derived from other criminality may also be accurately declared in order to circumvent local requirements in respect of banking the cash (see earlier case example from the Tunisian authorities).
- **Cash declarations used to create a false record of import or export.** A cash declaration form is completed and submitted, but not checked, when a passenger enters a country, but no cash was actually imported or exported. Instead, the criminal goes to a bank or other financial institution and pays in the cash derived from crime in the destination country to the value of the false declaration, which is accepted as legitimate in the same manner as the previous example (examples have been reported where a passenger declares cash in, say, three currencies but only two are actually present, the absent third currency is then 'made up' from criminal cash in the destination country).
- **Cash declarations re-used.** Cash is genuinely imported or exported and is declared accurately and correctly. The criminal then takes possession of additional cash derived from criminality in the destination country and goes from bank to bank with the same declaration, using the declaration multiple times to lend a veneer of legitimacy to the additional tranches of criminal cash. The bank staff examine the cash declaration form but do not retain it or make a note of the details, so no-one is able to detect that it has been re-used. A variation on this theme is an adaptation of the example above, where a completely fictitious declaration is used multiple times.
- **Cash declarations that are incomplete.** The criminal declares a large amount of cash at a border control and is challenged by the authorities to

produce the cash. The correct amount of cash is produced, it is counted and the authorities are satisfied with the declaration and the subject is allowed to proceed. Had the authorities searched the subject and his effects, however, they would have discovered that he had additional cash in his possession that he had not declared. The subject is later challenged by the authorities away from the border and can truthfully and verifiably state that he made a cash declaration which was verified satisfactorily by the authorities.

- **Cash declared at one end of a journey but not the other.** In this situation the subject may correctly declare the cash on leaving a jurisdiction, for example at an airport, where the authorities do not routinely check declarations. He has no intention of declaring it inbound at his destination as the cash has a criminal origin and he intends to put it to criminal use. However he is intercepted at the destination and the cash is discovered. The subject then claims the failure to declare the cash was an oversight and uses the declaration made at the beginning of the journey as 'insurance', effectively giving the cash a veneer of legitimacy as in the first example (see case reported by Israeli authorities below).

Box 11. **Example of a deliberately incomplete cash declaration**

In October 2013, a Jordanian person arrived at Amman airport coming from Turkey and he declared an amount of JOD 153 000 (Jordanian dinar) (approximately USD 215 000)

After checking the amount and counting the money, it was found that the person was actually in possession of the following, in total equivalent to about USD 290 000:

- AED 384 125 (Emirates dirham)
- SAR 74 300 (Saudi riyal)
- JOD 85 486
- QAR 113 238 (Qatari riyal)
- ILS 31 460 (Israeli shekel)
- EGP 11 091 (Egyptian pound)
- BHD 169 (Bahrain dinar)
- KWD 710 (Kuwaiti dinar) and
- LBP 747 000 Lebanese pound

The money was seized and the Jordanian court levied a penalty of 3% of the cash seized.

Source: Jordanian authorities.

Box 12. **Declaration at one end of a journey but not the other**

The authorities in Israel were alerted by customs officials in another jurisdiction about an Israeli citizen, a diamond dealer, who had made cash declarations on at least 20 occasions, totalling about USD 2.2 million whilst leaving that country to travel to Israel. The Israeli authorities discovered that the individual had not declared any of the cash when entering Israel. An investigation was commenced.

The subject refused to co-operate with the investigation, claiming that the money was from a legitimate source, using the fact that he had declared the money whilst leaving the other jurisdiction to support his claim. The subject was aware of the money laundering laws in Israel.

The cash was suspected to be linked to tax fraud.

At the conclusion of the investigation the subject was fined ILS 400 000.

Source: Israeli authorities.

3.6 NO ATTEMPT TO CONCEAL

As the graphic in section 3.4 shows, in some circumstances no attempt is made to conceal cash when it is transported from one country to another. This can be the case when the transportation is across a land border which is either only manned occasionally or not manned at all (as is the case with all land borders within the EU, see case reported by the German authorities, Box 9).

Box 13. **No attempt to conceal cash**

In 2008, Slovenian customs officials at a land border intercepted a person leaving Slovenia for Croatia by car. Customs noticed a bag on the rear seat of the vehicle and checked the contents. They found a huge amount of low-denomination banknotes. The cash was seized and counted. In total, there were more than 400 EUR 20 notes, more than 400 EUR 100 notes and more than 8 000 EUR 50 notes, totalling in excess of EUR 500 000. The cash was related to drug trafficking.

Customs had stopped the vehicle because the driver was of Serbian nationality, using a Portuguese passport and driving a car owned by a third party with Italian number plates.

In this case, the Slovenian authorities experienced significant difficulties evidencing the criminal conduct of the subject in another jurisdiction. Eventually they had to use information in a newspaper from the overseas jurisdiction (which reported the drug trafficking activities of the subject) to produce enough evidence to convince the Slovenian authorities to forfeit the cash.

Source: Slovenian authorities.

In the above case, as with the previous example from Germany (box 9), the cash was in its 'raw state': low-denomination euro notes derived from sales of controlled drugs in Slovenia. The euro is accepted unofficially by many businesses in Croatia, so there was no real imperative to exchange the

cash before removing it from Slovenia. At the time of this event, Croatia was not part of the EU. As a result of Slovenia's accession to the EU Schengen agreement, controls at the Slovenia/Croatia border were increased in 2007 as this was now an external EU border (and the cash should have been declared under EU regulations). However, as with most land borders in Europe large numbers of vehicles travel between the two countries on a daily basis and the chances of being intercepted were low.

3.7 CONCEALMENT ON THE PERSON

As shown in Graph 8, concealment of cash on (or in) the body, or within the luggage of a person travelling between two jurisdictions, was overwhelmingly the most common technique encountered by countries that responded to the questionnaire. It is important to note, however, that the resources of the customs authorities to check natural persons of most countries are concentrated more at air, sea and land boundaries than anywhere else, so there is an argument to say that the reason these techniques are most commonly encountered is because those are the ones that most countries look for.

Countries were asked to provide case examples, and well in excess of 100 examples were submitted from a wide variety of countries all over the world. There are too many to list individually but the following are examples:

Box 14. **Cash concealed on a person intended for Islamic State (ISIS/ISIL) in Syria**

In April 2014, a female traveller, M, was intercepted at outbound customs controls at London Heathrow airport on her way to Turkey. She was asked if she was carrying any cash. She produced 40 EUR 500 notes (EUR 20 000) from her underwear. She was also in possession of an additional EUR 1 000 made up of four EUR 200 notes and two EUR 100 notes.

M admitted she had been given the cash by a close friend, W, and asked to take the cash to Turkey, where she would hand it to W's husband or one of his associates. W had offered her EUR 1 000 to undertake the trip. W's husband had previous convictions for drug trafficking and firearms offences, but had recently converted to Islam and had travelled to Syria to fight for Islamic State. M claimed she had been told by W that the money was for the deposit on a house, and she did not know W's husband had joined Islamic State.

W was also arrested and evidence, including messages, photographs and videos, were recovered from her mobile phone showing her husband involved in jihadist activities. It was believed that W was preparing to travel to Syria with her two young children to join her husband.

At their trial, M was acquitted of funding terrorism, but W was convicted and sentenced to 28 months imprisonment.

Source: UK authorities.

Box 15. **Cash transported by aircrew**

A money laundering syndicate was suspected of using airline pilots and crew to smuggle millions of dollars' worth of cash out of Australia to Vietnam. Authorities suspect that the money was the proceeds of drug sales in Australia and payments for drugs imported into Australia.

The cash was given to the pilots by owners of several remittance service businesses, and authorities suspect the money laundering network used pilots to smuggle more than AUD 10 million from Australia to Vietnam over an 18-month period.

Searches of AUSTRAC's information database identified that one of the suspect Vietnamese pilots had previously declared AUD 19 000 on an international currency transfer report (ICTR). Since that declaration, the pilot had made no further reports of currency being carried into or out of Australia.

The suspect pilot was arrested after attempting to smuggle AUD 500 000 out of Australia without declaring it. He pleaded guilty to charges of money laundering under the *Criminal Code Act 1995* and was subsequently jailed for four-and-a-half years for smuggling a total of AUD 6.5 million out of Australia.

Source: Australian authorities.

Box 16. **Outbound cash seizure destined for the USA**

In October 2013, at the Bermuda airport, a 46-year old Bermudian male presented himself at the US border control to travel to Atlanta. Officers were suspicious of his demeanour and appearance. When questioned, he admitted he had made a false declaration as to the amount of cash in his possession; whilst he had stated he had USD 1 800 he changed that to USD 8 000.

An initial search resulted in the seizure of USD 10 750 from his wallet and pockets.

The man was detained, he and his luggage searched. Officers body searched him and found he had a home made money belt containing USD 29 900. On searching his carry-on luggage officers seized USD 10 556 hidden in a Worldview Travel cardboard pouch.

When questioned, he stated that local gang members had forced him to carry the USD 50 000 because a drug deal had gone wrong. They had ordered him to take the cash to Atlanta where he would be met. He added that USD 1 206 was his cash from work. He had originally been given all the money in the money belt, but had split it up as it was too bulky under his shirt.

An investigation by the FIU showed that the subject had limited finances and was living within his means. He pleaded guilty to an offence of possession of the proceeds of criminal conduct and received a suspended sentence. The cash was confiscated.

Source; Bermuda Authorities.

3.8 CONCEALMENT IN PASSENGER'S BAGGAGE

As the above example from Bermuda shows, one of the influencing factors regarding whether cash is carried on the person or in their luggage is its physical bulk and weight. In the UK example (box 14),

the courier was able to hide the cash in her underwear as is was made up of high-denomination euro banknotes that reduced its physical size to the minimum possible. However there will be occasions when even the use of high-denomination banknotes will make it impossible for the cash to be concealed about a courier's person. If there is no other transportation option available, the cash will have to be placed in the courier's baggage instead, either simply hidden within the clothing, within the fabric of the luggage itself, or hidden within other items inside the suitcase.

Box 17. **Cash concealed inside items in a passenger's luggage**

On 7 January 2011 , at the international airport of Mexico City, customs officers performed a routine luggage inspection of passengers on flight number bound for Lima, Peru. A cash detector dog made a positive indication on a suitcase, which was sent to the mobile X-ray unit to be inspected.

The inspection showed irregular images that did not match the usual baggage of a passenger. Subsequently, customs staff opened the baggage in the presence of the passenger who owned the suitcase, for a thorough inspection of its interior and contents. Hidden inside a bag of candy and cigarettes packages they found a total of USD 151 000 in USD 100 banknotes .

Source: Mexico authorities.

Box 18. **Cash concealed in the structure of luggage**

On 4 October 2005, customs officials at the Ministro Pistarini (Ezeiza) international airport, Argentina, inspected the luggage of A, just arrived on a flight from Mexico. The luggage consisted of one bag with a backpack inside it. During the inspection the officials assessed that the backpack felt too thick. Both bags were emptied of their contents and X-rayed. The images displayed were suspicious. The customs officials cut the bags open and found that both had a double bottom containing US dollars wrapped in plastic wrap. Nine packs were found inside the two bags. The backpack contained four packs, three containing USD 25 000 and one containing US 23 000. The bag contained five packs, two with USD 50 000, two with USD 60 000 and one with USD 30 000, a total of USD 348 000.

On the same day, customs officials also inspected the luggage of R, who had also arrived from Mexico on the same flight. His luggage was a garment bag. The officials detected excessive rigidness while searching the garment bag. Agents emptied the contents and X-rayed the bag, and again, identified suspicious items. The agents cut the bag open and found a double bottom containing US dollars wrapped in plastic wrap. Eight packs were found, six containing USD 40 000 each and two containing USD 15 000 each, totalling USD 270 000.

The defendants were charged on the basis of "having entered the Argentinean National territory on 4 October 2005, from México DF in the MX 1691 flight, with USD 618 000, and having declared on the customs forms that they were entering with less than USD 10 000. The money was hidden in the luggage… (and) they reported receiving, as profit, that money from criminal source in order to give

it the appearance of a lawful source". The subjects received a penalty of imprisonment in abeyance, special disqualification for six months for the exercise of trade, total disqualification for six years to serve as public officers and the seizure of the money (USD 618 000).

Source: Argentinian authorities.

3.9 CONCEALMENTS IN VEHICLES AND ACCOMPANIED FREIGHT

Many countries share land borders, and where this is the case, a common method of cash smuggling is to conceal it within the structure of a vehicle or within freight carried on the vehicle. The advantage of doing this is that, in general, more cash can be concealed than would be the case with a foot passenger, and the concealment is generally more difficult to identify. As the graphic in section 3.4 shows, a significant number of countries identify this technique.

Of course, the method of transport does not have to be a wheeled vehicle; some countries also report the use of others, such as boats and light aircraft.

Box 19. **Cash concealed in adapted accompanied freight**

On 19 September 2013, at the San Emeterio tactical inspection station, located near Sonoyta, Sonora, an articulated truck with a trailer loaded with 2 058 boxes of fresh apples entered the station to clear customs formalities. After reviewing the cargo documentation, the vehicle and its cargo were sent for customs inspection. The inspection was performed by a non-intrusive scanning system in order to search the vehicle and its trailer for undeclared goods. The scan showed up irregularities in the backside of the trailer just before the rear axles. As a result, officials carried out a physical verification of the goods. Inside the boxes they found a total of USD 1 310 010 in various denominations.

Source: Mexico Authorities.

Box 20. **Cash concealed in a specially constructed 'hide' on a Yacht.**

On 5 April 2008 several law enforcement agencies in St. Vincent and the Grenadines conducted a joint operation. These agencies included the Coast Guard, Rapid Response Unit, Narcotics and the Financial Intelligence Unit. The aim of the operation was to board, and conduct searches on, two yachts suspected to be owned by defendant A. Prior to the operation, the St. Vincent and the Grenadines Financial Intelligence Unit (SVG-FIU) and the Royal St. Vincent and the Grenadines Police Force (RSVGPF) received intelligence from the law enforcement authorities in Bermuda indicating that defendant A had a large cache of money on the island of Bermuda and wanted to smuggle same into St. Vincent and the Grenadines.

During the operation on 5 April 2008, law enforcement officials boarded two yachts, yacht A and yacht B, which were anchored in the territorial waters of St. Vincent and the Grenadines. The main conspirator defendant A was present on yacht B with his children and other minors. Defendants B and C of Trinidad and Tobago and Bermuda respectively were on yacht A. The officers conducted preliminary searches of both vessels and nothing illegal was found. However, all mobile phones were seized and kept as evidence. The yachts and the occupants were taken to the main coast guard base where a more thorough search was conducted on the yachts.

The search of yacht B revealed nothing illegal, and defendant A was released from custody. Yacht A, which intelligence revealed had sailed from Bermuda to St. Vincent and the Grenadines, despite defendant C, the captain of that yacht, informing Bermuda customs that he was sailing to the Azores, was also searched. The search of Yacht A lasted for approximately seven hours before Officers decided to remove some liquid foam insulation that had hardened from around the water tank in one of the cabins of the yacht. Having removed the foam, the officer discovered US dollars in vacuum-sealed bags. Defendant C was questioned and informed the officer that other monies were around the water tank in the other cabin. Officers removed the foam from around this water tank and found US dollars in vacuum-sealed bags.

The SVG-FIU seized the monies and secured it as evidence. Forensic testing was conducted on the monies however no material evidence was recovered. Defendants B and C were charged with money laundering offences and defendant A was also subsequently arrested and charged with money laundering offences. The US dollars recovered from the yacht amounted to USD 1.76 million.

Defendants A and C were found guilty of the offences for which they were charged. Defendant B was acquitted.

Source: St Vincent & The Grenadines Authorities.

3.10 RE-USE OF CONCEALMENTS OF ILLICIT GOODS

Countries report numerous examples of cash being transported in the same concealments that originally contained illicit goods, such as drugs. This is a sensible option for the criminal as it means that only one method of transportation is needed and if the concealment was secure enough to successfully ship an illicit commodity it is likely that it will be secure enough to ship cash. However as stated previously it will by no means always be the case that cash and drugs will be shipped this way. It will only be done if it suits the persons at both ends of the criminal transaction; if the supplier of the goods has shipped them from country A but wants the payment at Country B, for example, this technique will not be suitable and another will be used.

Box 21. **Cash transported in re-used concealments previously used for transporting drugs**

Police investigations and FIU analysis identified an organised group that was laundering money from drug trafficking from South America.

One of the techniques that the group used to import drugs from South America was to import boats fenders. They would hide the drugs inside the boat fenders, and after opening them and taking the drugs out, they would place cash in high-denomination notes in the same concealment. The boat fenders were sent back to the country of origin as defective goods.

Police made several cash seizures. It was also established that there were links between the money seized and drug trafficking organisations.

The investigations revealed that the criminal organisation used several money laundering systems at the same time; cash was also transported by air passengers.

A total of EUR 7.2 million in cash was seized, 11 people were arrested and 2 000 kg cocaine was seized.

Source: Spanish authorities.

3.11 ABUSE OF LEGAL BUSINESS STRUCTURES

Several of the case examples submitted, such as the one from the Spanish authorities above, demonstrate that criminals often use 'front companies' or other legal business structures to lend a veneer of legitimacy to their activities. In many jurisdictions it is very easy to establish a limited company, which is a legal entity in its own right, and can be controlled by members of the criminal group. Once a business has been established it can open a bank account which can be used to deposit cash derived from illicit activities (especially if the business claims to be cash intensive, such as a bar, a night club or similar).

In addition, as was the case in the Spanish example, a business can be set up which claims to legitimately trade with businesses in other jurisdictions. This can then be used as 'cover' for the transport of goods between the two countries, which then can be used to conceal cash. If the goods are sufficiently large and the trade generates sufficient volume then large amounts of cash can be concealed in unaccompanied cargo.

3.12 METHODS OF PHYSICAL TRANSPORTATION OF CASH - CARGO AND MAIL

The questionnaire asked countries about their perception of the extent of the illegitimate cash movements into, transiting and out of their country. Countries were asked how many cash smuggling cases (cash couriers, cargo and mail) they had had in the last 3 years and what the amounts involved were. Countries could also mention their experience with the methods used for the physical movement of cash for suspected criminal or money laundering purposes – countries could tell if criminal cash has been transported by passengers, in (different forms of) cargo or in mail/fast parcels.

Box 22. **USD 89 000 criminal cash in postal packages**

Based on a routine check by customs, an investigation by the joint financial investigation group of police and customs forces in Berlin lead to the discovery of USD 89 000 which were forwarded from the US to Berlin.

Perpetrators, which were unknown to this time, had sent five packages containing electric devices to various beneficiaries in Berlin by post. The money (solely USD 100 bills) was hidden in these devices.

After an information exchange with US authorities it was possible to assign the funds to a group of criminals, which had acquired at least USD 4 200 000 000 through criminal activities (mainly fraud and cybercrime). The money was seized.

Source: German authorities.

Two countries stated that they did not believe that cross-border flows of criminally-derived cash take place in their countries. Twenty-two countries stated that they did not have experience in how cross-border flows of criminally-derived cash take place[56]. However, most of the countries reported the amount of the cash smuggling cases they had the last three years and/or the amount of cash involved.

Only one country, however, made a clear division between cases regarding passengers and cases regarding criminal cash in cargo and mail. However, by combining the answers of both questions mentioned above, the project group was able to determine that 27 countries[57], or almost one-third of all responding countries, in the last 3 years had cases of cross-border transportations of criminal

[56] Nevertheless, some of these countries answered the questions in section 1 of the questionnaire reporting some cases of cross-border flows of criminally derived cash.

[57] Countries explicitly reporting in answering the first question of the questionnaire they had no cases the last 3 years but mentioning experience with cases in cargo and mail in the second question have not been counted in this number.

cash in cargo and/or mail. In total 19 of these 27 countries reported that they have dealt with cash smuggling cases in cargo and 19 countries had cases in mail.

Analyses of these 27 countries based on cross connections between different questions/answers in the questionnaire did not reveal a clear picture of why some countries were able to submit information on cash smuggling cases in cargo and mail and how they were able to detect these cases, while other countries were not able to do this. It might be expected, for instance, that the presence of specific regulations on anti-money laundering and terrorism financing regarding cash in cargo and mail would be a decisive factor, but this could not be concluded from the questionnaires. For instance, 13 of the 27 countries did not have a prohibition and/or a license requirement for cash in cargo and mail, and only 7 of the 27 countries have a specific declaration form for cash in cargo and/or mail. Of the 19 countries that have such a declaration form only 6 reported cases.

Precise figures for the number of cash smuggling cases relating to cargo and mail, and the amounts involved, could not be retrieved from the questionnaires, because the reported cases and amounts were not divided into cash carried by passengers, cargo or mail by any of the participating countries (except one). It was possible to conclude, however, that the actual number of cash smuggling cases[58] identified in cargo and mail was very limited, in total not more than hundred cases world-wide in the last three years. In the questionnaire responses, countries made it clear that almost all the cases detailed related to cash in the possession of passengers. This is no surprise as almost all countries appear to have strictly implemented comprehensive legislation on cash carried by passengers. This was also reflected in the answers on the question to indicate, in descending order, the most frequently encountered methods of cross-border transportations of criminal cash: cash couriers were the most numerous in all except one country[59].

It is worth noting that, while several countries reported cash smuggling cases in cargo and mail, many countries pay no attention to this phenomenon as there is no need to do so in the absence of relevant legislation. One country which reported several cases in mail, for instance, states that customs does not give priority to inspecting mail items containing cash because customs lacks the legal authority to do so regarding anti-money laundering and terrorism financing. Consequently, all findings in this country are 'chance hits'. Customs only makes these discoveries within the context of selection and inspection of other goods and risks. This description will most probably fit all other countries without specific cash and/or anti money laundering and terrorism financing legislation.

The occurrence of cash smuggling cases is remarkable also for another reason. In the circumstances described above, it would seem that criminals do not need to smuggle cash. Instead, they could make a rational choice to simply declare all cash transported. As long as criminal cash is transported the same way legal cash is, customs are not able to identify any difference between criminal and legal money – "the best way to hide a tree is in the forest". On the other hand, when customs, by chance, find a concealed amount of money, it is immediately clear that this is criminal money. Absence of regulation and effective enforcement through appropriate allocation of authority is an encouragement for criminals to use this easy way of transporting criminal or terrorist money.

[58] The terms "smuggling cases" and "illegitimate cases" used in the text have the same meaning.

[59] An other reason for being the number one in that ranking is that cash couriers are only able to transport a limited amount of cash. Multiple couriers have to be used in order to get a reasonable amount of cash across the border. In contrast to a container that could transport the big amount at once.

Recent research underlines this conclusion[60]. There is such a thing as 'ingenuity fallacy', which means that money laundering often takes place in a much easier way then one would think based on theory. If criminals can do it the easy way they won't do it the hard way.

3.13 NO ATTEMPT TO CONCEAL

Information from some counties indicates that criminal groups may have found a way of infiltrating cash into the outwardly legitimate bank-to-bank shipment system, such that it can be 'hidden in plain sight'.

Box 23. **Criminal cash infiltrated into the legitimate bank to bank cash shipment process**

The cash (total value: several million euros) was detected at an EU airport in transit from a bank in North America to a bank in the EU. Customs checks identified several clear money laundering indicators;

- Large amounts of EUR 500 notes
- The secure carrier had never before transported cash to the destination country; this country was a customer-country of another well-known carrier

A criminal investigation was started as customs of the transiting EU country reported a suspicion of money laundering to the FIU and the Police. The subsequent criminal investigation examined the background to the cash shipment, and also the bank concerned in North America in order to establish the suspected criminal origin of the money.

The case involved cooperation between the Police and Public Prosecution Service in the North American country involved and the Police in the EU country.

The investigation revealed that the case was the subject of a global investigation. The results so far are large confiscations, arrests and forfeitures.

Source: Netherlands authorities.

3.14 TECHNIQUES OF CONCEALMENTS OF CASH IN CARGO

As has been discussed earlier in this report, potentially far more cash can be concealed in cargo than can be carried by passengers, or concealed in a vehicle. Yet, the questionnaire responses indicate that in most countries the resources dedicated to detecting cash transported in cargo are a fraction of those dedicated to controlling air passengers. As explained in section. 5.3, this may be related to the absence AML and CTF regulation for cash in cargo in the majority of the countries. This, in turn, may be related to the current wording of FATF Recommendation 32 (see section 3.4).

[60] Soudijn (2015).

Box 24. **Bulk cash smuggling in cargo at Mexican border**

On 9 September 2009, Mexican customs officials on duty at Manzanillo seaport, carried out an inspection of two 40 ft shipping containers. The containers both contained 20 x 1 000 kg super-bags filled with ammonium sulfate, making a total of 40 super-bags. A physical examination of the super-bags and their contents revealed six concealed block shape packages. When opening the blocks, officials found USD 11 054 695, mostly in USD 100 banknotes. The goods were manifested for export to Colombia.

Comment: Although the predicate offence linked to the seizure of the cash is not known, it is highly likely that the cash is related to the trafficking of cocaine. The cargo was manifested to Colombia, which is a major cocaine source country.

Also of note is the fact that only 6 of the 40 super bags of chemicals contained blocks of cash. Clearly, much more cash could have been concealed, had the criminals behind the shipment felt it necessary to do so.

Source: Mexican authorities.

Box 25. **Cash concealed in a shipment of vehicles for export**

This case began due to a random customs control on an export shipment of a large quantity of vehicles consigned to Mexico. In the gear box of one of the vehicles (a pickup truck) customs discovered EUR 825 000 (the gear box was a spare part). This was clearly smuggling: the money was hidden and not declared.

Source: Netherlands Authorities.

Box 26. **Suspicious bank to bank shipment of cash transiting Schiphol Airport**

This case started with a customs control at Schiphol Airport on an international cash transport (transit) of EUR 425 000. It was a bank-to-bank consignment (South America – Schiphol Airport - Germany) that, at that time, took place several times each week. This was remarkable, not only because of the regularity of the transports, but also because in air cargo this is a relatively small amount.

The name of the sending bank changed officially several times. The top managers too, changed rather often, and these managers were known to be managers in dozens of trusts in the region as well. Final consignee and other parties concerned were hidden. The consignment consisted of:

- 780 notes of EUR 500
- 75 notes of EUR 200
- 100 notes of EUR 100
- 200 notes of EUR 50

In total EUR 425 000

The transportation route ceased to be used after Netherlands customs started examining the shipments.

Source: Netherlands authorities.

Box 27. **Operation Pacific Rim – US Homeland Security Investigations (HSI)**

Bulk cash smuggling is one of HSI's primary investigative priorities. As part of the effort to combat bulk cash smuggling, HSI established the Bulk Cash Smuggling Center in 2009. Between fiscal years 2003 and 2013, HSI bulk cash smuggling investigations led to the arrest of more than 2 300 individuals and seizures of more than USD 547 million. The center is an operational, intelligence-driven investigative unit that combats bulk cash smuggling from both national and international perspectives. It disrupts pipelines used to move currency derived from illicit activity including drugs, weapons, human trafficking, foreign political corruption and contraband.

In Operation Pacific Rim, HSI, working closely with the Colombian national police and Mexican authorities, dismantled a major drug trafficking organisation - an industrial and transportation empire with a profit margin measuring USD billions. Drug smugglers - responsible for 42 percent of Colombian cocaine entering the United States from 2003 to 2009 - brought tons of cocaine into the United States on yachts and semi-submersibles along the Mexico/United States maritime border. HSI began Operation Pacific Rim in September 2009 after scoring a previous victory in an investigation where they seized USD 41 million in Colombia and Mexico.

From FY 2009 to date, HSI's international partners continue to play a central role in Operation Pacific Rim. HSI works closely with the Colombian national police, Mexican authorities, and partners in Ecuador, Argentina, the Netherlands, Spain, Morocco and Panama, as well as the US Drug Enforcement Administration. This HSI-led investigation spanned the globe and effectively disrupted one of the most powerful and sophisticated bulk cash smuggling and drug trafficking organisations in the world.

Bundles of shrink-wrapped bulk cash concealed within containerised (conex containers) shipments of fertilizer were intercepted at seaports in Colombia and Mexico and also in armoured vehicles. The ports of Buenaventura and Manzanillo are key points of a well-known route used for smuggling cocaine northward to Mexico and then on to the United States, and for sending cash back into Colombia.

This transnational drug trafficking organisation that was generating the cash was a prolific cocaine source of supply, responsible for nearly half of the cocaine smuggled from Colombia into the United States between 2003 and 2009 – approximately 900 tons with an estimated street value of USD 24 billion.

The 'kingpins' of the Colombian drug trafficking organisation created a double problem for themselves in that they made so much money from their illegal narcotics trafficking that they couldn't launder it all. In addition, the huge scale of the drug trafficking and money laundering operations made concealing it from the authorities almost impossible.

Source: US Authorities.

3.15 TECHNIQUES OF CONCEALMENT OF CASH IN MAIL

Few countries report seizures of cash in post and mail, in all probability because most are not looking, some lack the required legislation, and some appear to think that Universal Postal Union (UPU) guidelines prohibit the practice when in fact they do not. It is clear from the cases that have been submitted that the practice does take place, although the amounts are relatively small when

compared the amounts of cash detected in cargo, for the simple reason that mail items are usually much smaller.

Box 28. **Cash in postal items**

At the customs offices in Hamburg and Hanover, the German postal administration detected nine packages, all part of the same shipment, which had been sent from the US to Germany

According to the declaration of content the parcels contained documents (without a declared value), books, videos and CDs. One parcel was declared as a present.

However, a closer inspection of the parcels revealed approximately USD 158 000 in cash.

Based on these detections, money laundering investigations were initiated against German senders and receivers of the parcels.

The funds were seized by order of the public prosecutor, because there was reason to assume that the money originated out of ML activities.

Proof was obtained that the funds originated from a theft in the US in which approximately USD 3.4 million was stolen.

Source: German authorities.

Box 29. **Cash concealed in priority mail**

HSI Honolulu and HSI Seattle were proactively investigating a criminal organisation responsible for the movement of illicit bulk cash currency as it relates to the distribution and sale of methamphetamines. In December 2013, a priority mail parcel was selected for examination at the Honolulu international mail branch, following a positive indication from a cash detection dog. The parcel was shipped from Guam to the state of Washington. Examination of the priority mail parcel revealed USD 42 000.

Source: US Authorities.

Box 30. **Cash in courier parcels associated to trafficking synthetic drugs**

Over a period of time, 23 courier packages and 29 envelopes were found containing cash. The 23 courier packages contained a total of EUR 92 430. The 29 envelopes contained a total of EUR 1 800 and BRL 14 500 (Brazilian real) (equivalent to approx. EUR 3 100). One parcel, contained a CD-cover, concealing two so-called confidence travel cards by VISA. The amount these cards represent is unknown.

Customs received information from courier company TNT Post regarding 37 EMS/ parcels that had been delivered to the suspect in the period 27 November 2008 to 4 February 2010. It is unknown whether these parcels contained cash.

As a result of the above, in the period between 24 August 2012 and 16 November 2012, a total of another 106 letters (envelopes) containing pills, shipped by PostNL and addressed to PO boxes in

Brazil were identified. The 114 envelopes concerned contained a total of 28 555 pills containing MDMA (popularly known as Ecstasy).

A total of five parcels were intercepted which had been shipped by UPS from Brazil. In each of these parcels a plastic Confidence Travel Card was found, mentioning, among other things, the words " Euro". These cards are so-called prepaid debit cards.

It is suspected that the amounts in euros credited to the five Confidence Travel Cards concerned were the proceeds of the delivery of XTC pills by the suspect to buyers in Brazil.

An associated seizure, revealed envelopes containing cardboard strips impregnated with LSD.

On 14 July 2011 the district court in the Netherlands sentenced the suspect in this case to a non-suspended prison sentence of 24 months and on 13 February 2012 he was released on parole.

Source: Netherlands authorities.

Box 31. **Examples of criminal money transported in mail and fast parcels**

2013. Cash concealed in the sides of the cardboard box of a mail parcel.

Total: EUR 4 200.

2013. Cash concealed in kitchen rolls. (Note – the concealment involves paper hidden in paper,

so the banknotes were not visible using X-ray equipment).

Total: EUR 182 000.

2013. Cash concealed in a box of children's nappies/diapers.

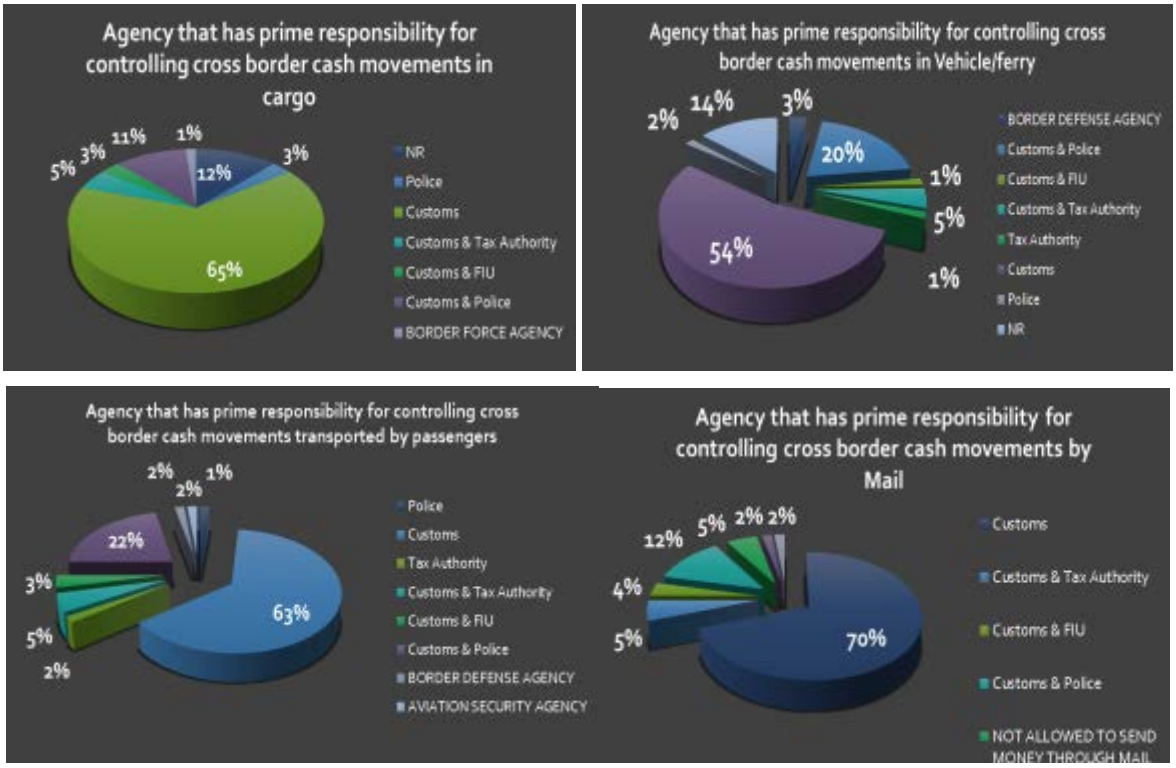
Total: EUR 28 500.

Source: Netherlands authorities.

4. CONTROLLING CROSS BORDER TRANSPORTATION OF CASH

4.1 CONTROLS AT BORDERS – ROLES AND RESPONSIBILITIES

The questionnaire asked countries to specify which agency had prime responsibility for controlling cross-border transportations of cash in cargo, vehicles/ferry, passengers and mail. For all of these different methods of transportation, the most common answer was the customs authorities. However, it was notable that, for all four methods a significant number of countries responded that it was the responsibility of both customs and the police, as shown in the graphics below.



Source: Tunisian authorities, based on questionnaire analysis

Customs and other similar border authorities clearly have a significant role to play in combatting money laundering through the physical transportation of cash, a role that is highlighted and promoted by the WCO. However, customs authorities can only play an effective role when national legislation provides them with sufficient authority to act.

The important role of the police in controlling cross-border transportation of cash is not surprising. In many countries, the customs officials have an administrative role, and the responsibility for conducting criminal investigations rests only with the police. In these situations, a detection of cash thought to be of criminal origin will likely be referred to the police for investigation. Similarly, the police often have other, non-customs related responsibilities (such as crime and national security) at a border, in the course of undertaking which they may encounter consignments of criminally derived cash.

In addition, countries were asked if the responsibility for recording, examining and investigating cash movements was split between different agencies. Thirty-four countries said it was, whilst 19 said it was not. They were also asked if one agency had to, or needed to, work with other agencies to effectively examine, investigate or seize cash. Forty-four countries answered that this was the case, whilst 11 said no. Clearly, these results show that effective co-operation between the agencies concerned is of vital importance to maintaining an effective deterrent to cash smuggling.

Natural persons

Countries were also asked a series of questions relating to the legal authorities held by the agencies controlling the borders in certain circumstances. The first of these was whether agencies routinely examined passengers to identify suspected criminal cash. Fifty countries said yes and only four said no. This is not surprising, given that, as mentioned earlier, the data clearly shows that the bulk of the resources of most countries is dedicated to controlling natural persons, in accordance with those requirements of Recommendation 32 for which detailed guidance is included in the Interpretive Note.

Most countries (44 out of the 52 that answered this question) stated that the level of proof required to detain cash for further investigation was 'reasonable suspicion', although in order to forfeit cash, more countries needed to prove that it was criminally derived to a level beyond reasonable doubt (19 out of 48 countries). This coincides with the cases of criminal cash in cargo that have been submitted. In almost all the cases, the starting point was a suspicion of money laundering from an investigative agency upon which customs acted. This means, in practice, that hardly any customs control on cash shipments from an AML or CTF point of view will be and can be exercised, as the information available from a customs declaration is so limited (see below) that the level of proof needed to detain the cash and to exercise further inspection will seldom be reached.

Another issue arising from the questionnaire regarding Recommendation 32 is the definition of "currency and bearer negotiable instruments". Some 33% of the responding countries felt the definition is too narrow (whereas 23% of the countries did not answer this question).

The case examples submitted by a number of jurisdictions demonstrated that money laundering and terrorism financing also takes place with other valuables, comparable to currency and bearer negotiable instruments. A number of countries, suggested broadening the definition of "currency and bearer negotiable instruments" with commodities such as:

- Precious metals / Diamonds/ Gold/ Gemstones;
- Jewellery/ Watches;
- Prepaid cards;
- Cash cards/ Stored value cards;
- Casino chips;
- E-money (electronic types of money like electronic wallets or Bitcoins);

- Other commodities/instruments that can easily be transferred into cash/Each transmissible instrument in such form that the property of the title can be transferred to one or more persons.

Cargo and Mail

Countries were then asked if these border control agencies had the power to routinely search consignments of cash in cargo and mail from an AML perspective. The answers were overwhelmingly affirmative; 43 said yes and only 8 said no. Once again, this is not surprising as most countries have granted their customs (and police) the legal powers that they believe are required for the effective management of money laundering risks in respect of natural persons. However, further research suggests that in many cases the agencies concerned in fact do not have the power to conduct searches routinely, i.e. without a suspicion of money laundering.

The Harmonised System tariff code for banknotes attracts no VAT or customs duty, and the only details required on the customs documentation is the weight of the consignment and a proper description of the goods. Thus, the description on such a consignment need only say 'banknotes 1 000 kg' to comply with these requirements. There is no need, for example, to record the beneficial owner of the banknotes, the details of the financial institution where they started the journey, or the details of the recipient. Because specialized CVIT companies with depots in the origin and destination locations usually carry out the shipment and the customs declaration, it is frequently the case that the names and addresses of the dispatching and receiving depot of the CVIT company will be shown on the documentation as the addresses of the sender and receiver of the cash.

This, coupled with the fact that research has shown that the cash may be entered under the wrong tariff code (such as the ones for waste paper or printed matter, for example), means that customs authorities will often have almost no information at their disposal to assess whether the cash is a legitimate bank-to-bank shipment, or a consignment of criminal cash hiding in plain sight.

This issue goes to the heart of how customs authorities exercise their authority. No customs authority in the world is resourced sufficiently to examine every single consignment that crosses the borders they control. Nearly all will have to make some sort of reasoned judgment about which consignment to select for examination – in other words they will carry out some kind of profiling exercise. But in this circumstance, there is almost no information on which to base that kind of decision. As long as the customs documentation states that the shipment contains banknotes and their correct weight, the goods have been entered correctly and there is no objective reason for customs to suspect there might be anything suspicious about the cash. In other words, their powers to carry out further investigations and to demand the provision of further information are limited.

However, information gathered in the course of this project has shown definitively that criminal groups have been able to infiltrate very large volumes of cash into the bank-to-bank cash shipment system. It is therefore important that customs are able to inspect shipments and require the disclosure of additional information to enable them to address this risk effectively. The question that has arisen is whether, in the absence of any objective reason for suspicion, they have the legal power to do so (see also section 4.1 for an in-depth analysis of the (lack) of legislation/legal power). One country has examined this issue in detail and has concluded that their customs authority does not have the legal power. They are currently in the process of amending their national legislation to correct this situation.

This being the case, the next three questions in the questionnaire were carefully worded and designed to establish whether agencies tasked with controlling cash in cargo and mail had the legal authority to interfere with a consignment, or require the disclosure of additional information about it, if there were no obvious reasons for suspecting that it was connected to criminal activity.

- The first question was 'Where cash movements are superficially part of normal business, can the relevant agency inspect consignments and make further investigations to determine whether the movement is suspect?' Forty-seven countries answered yes to this, whilst only eight said no.
- The second question was 'Do these agencies have the power to routinely search consignments of cash in cargo and mail from an AML perspective?' Thirty-six countries answered 'yes' and eight said 'no'.
- The third question was 'If there is no apparent violation of customs regulations or banking rules, does the relevant agency have the power to detain a consignment of cash in cargo or mail for further inspection and/or investigation?' Thirty-three countries answered 'yes' and twenty-one said 'no'.

Overall, most countries believed that there were few restrictions on what their customs and other agencies had the legal authority to do, and it is possible that this is the case. However, the experience of one of the countries contributing to the project suggests that some countries may not have given the matter enough serious thought and studied their domestic legislation in enough detail to spot any loopholes that may exist. The effect of this is that most countries will continue to find it extremely difficult to detect any cross-border transportations of criminally derived cash in cargo and mail, and accordingly the matter will continue to be a considerable threat until these issues are addressed.

If countries do not pay greater attention to the issue of cash in cargo & mail, including gaining a better understanding of the legitimate trading of cash on international markets and the way that it is transported around the globe in consequence, they will be unable to use profiling and targeting tools effectively. Therefore, they will not be able to develop an effective response to the problem of criminal ability to infiltrate criminal cash into the legitimate systems used by banks and other financial institutions.

Box 32. **Establishing the nature and frequency of cross-border cash movements – Operation HANNIBAL**

In mid-2014, in response to the close involvement of CTAF, the Tunisian FIU, in the typology working group studying money laundering through the physical transportation of cash, and inspired by a similar exercise conducted by the Netherlands authorities in 2008, the Tunisian authorities conducted a 60-day project in which all transportations of cash into and out of Tunisia were monitored and recorded.

The exercise was supervised by CTAF, and conducted jointly by Tunisian customs and the Ministry of the Interior, in conjunction with all Tunisian banks. The objectives of the operation were;

- To identify different methods of money laundering and terrorism finance through the physical transportation of cash in order to enhance international community efforts in tackling these issues
- To detect, at a national level, the trends of legal importation and smuggling of cash as well as the methods used and its final destination.
- To use the outcomes of the exercise in the preparation of Tunisia's National Risk Assessment and make recommendations on ways of tackling organised crime (money laundering, financing of terrorism , smuggling etc.).
- To make practical recommendations for the best use and sharing of human and logistical resources on a risk-based approach.

The operation was wide ranging, and encompassed;

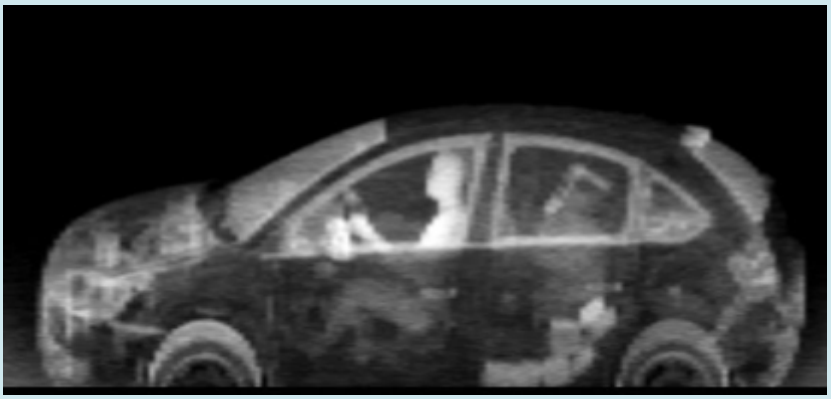
- The monitoring of physical transportation of currency across all Tunisian land, sea and air borders for a two-month time period . The targeted transactions were:
  - Smuggling of cash across the border during imports and/or exports.
  - Currency transactions reports (declared) at import, export and transit levels.
- Tracking the destination of reported currency through post-monitoring mechanisms carried out by national customs, banks, and Interior Ministry (Department of Foreign and Borders).
- Estimating the value of imported foreign currencies not regularised pursuant to Exchange Control Regulations.
- Attempting to determine the final destination of these funds and their potential links to money laundering and terrorism financing.

Information was exchanged using a specially commissioned secure area of the website of the Central Bank of Tunisia and monitored on a daily basis by CTAF. Over 17 000 reports were received, including 2 575 from banks and 14 983 from customs. Of the reports from customs, 28% were received from land borders, 9% from sea ports and 63% from airports.

Of the foreign currency detected, 94% was made up of US dollars, euros and British pounds, with only 6% in currencies of Arab states. Of the reports of movements of foreign currency, 2 935 originated from land border points, 1 348 from sea ports and 9 349 from airports.

As well as gathering a huge amount of valuable data concerning the value, nature and scope of foreign currency crossing their border, the Tunisian authorities detected a number of crimes including;

- A seizure of EUR 1 447 000 from a concealment in a car at a land border crossing; the seizure is believed to relate to the financing of terrorism



X-ray image of the car from which EUR 1.447 million was seized. Note blocks of money hidden under rear seat

- A seizure of USD 2 300 000 from a failed attempt at smuggling at an airport
- A seizure of USD 2 850 000 at an airport, which was being exported using a forged banking license.

In addition, further crimes, including importing and exporting currency without the required notice and the necessary license, cash smuggling, counterfeit currency and breaches of money laundering and terrorism financing laws were identified.

Source: Tunisian authorities.

4.2 METHODS USED TO DETECT AND PREVENT CRIMINAL CASH SHIPMENTS

4.2.1 CASH DETECTION DOGS

A number of the cases reported by respondents to the questionnaire have highlighted the importance and usefulness of cash detection dogs (see box 17 and box 29). Many countries now report that they are routinely using them to facilitate selection of passengers for inspection at ports and airports. One of the features of the Merida Initiative, the programme established to tackle bulk cash smuggling across the US-Mexico border, is that well over 400 dogs have been trained and deployed to detect not only drugs and firearms but cash as well. However they almost certainly also have a very important role to play in detecting illicit cash shipments in concealed in cargo and mail. The sheer size and volume of mail at mail depots, and cargo at ports and airports, makes profiling and control extremely difficult. Especially, as most countries pay little attention, and devote few

resources to the phenomenon. The use of cash detector dogs at container depots and other cargo consolidation points is a valuable asset too in selecting cargo and mail for examination.

4.2.2 X RAYS

As is the case with cash detection dogs, many countries are now using x-ray machines to identify cash concealed in a whole range of vehicles and goods, and a number of cases detailed in this report have resulted from x-ray scans (see box 19). The particular value of x-rays is that they can detect cash shipments even in the most cleverly constructed concealments that otherwise would be missed altogether by the human eye. They also facilitate much faster and more efficient screening of vehicles and persons, meaning more can be controlled and limited resources better utilised.

4.2.3 CONTROLLED DELIVERIES

The technique of controlled delivery is one that has been used for a number of years in many jurisdictions as a way of identifying and arresting persons involved in the trafficking of illicit substances such as drugs, counterfeit cigarettes, stolen goods etc. However, the case examples submitted suggest that the technique is under-used when it comes to large consignments of cash; only one such case was recorded.

The reason for this may be that, in respect of illicit substances such as controlled drugs, it is relatively easy to replace the drugs with a similar low-value substance, thus ensuring that, if anything goes wrong, the authorities have not suffered the embarrassment of losing a high-value consignment of illegal goods. Clearly, this is much more difficult with cash, as it is difficult to find anything that has the same look and feel of a large bundle of banknotes, and the value of the consignment often precludes any risk of loss. In the example below, the US authorities mitigated the risk of losing the subject, vehicle and cash en-route to the handover location by flying them from Mississippi to Colorado in a military transport aircraft, a facility that is not going to be readily available in most cases. Nonetheless, as can be seen from the result, the technique can be put to effective use if the risks can be mitigated.

Box 33. **Successful controlled delivery**

In April 2012, US Homeland Security Investigations (HSI) Resident Agent in Charge (RAC) St. Louis was contacted by the St. Louis County Police Department to adopt a USD 264 925 bulk currency seizure resulting from a probable cause traffic stop. HSI St. Louis special agents responded to adopt the seizure and conduct a post-seizure investigation, during which the subject agreed to co-operate and conduct a controlled delivery of the currency. In support of the controlled delivery, the National Bulk Cash Smuggling Center coordinated with the US Air Force Reserve to obtain a C-130 cargo aircraft to transport the HSI St. Louis agents, suspect, and vehicle to Greeley, CO. Additionally, HSI St. Louis co-ordinated efforts with HSI RAC Greeley and ultimately executed the controlled delivery, which resulted in additional seizures including USD 232 530 in US currency, 3 691 kilograms of cocaine, two vehicles, and one handgun. An additional suspect who was also arrested, agreed to co-operate and set up a meeting with a US-based cocaine distributor for the criminal organisation.

HSI Greeley and the Weld County Drug Task Force were subsequently successful in organising a

meeting with the co-operating defendant and the suspected US-based cocaine distributor for the organisation. The suspected cocaine distributor was apprehended and an additional USD 125 000 was discovered and seized. Furthermore, a fourth subject was arrested while trying to deliver 3.4 kg of cocaine to the co-operating defendant. The co-operating defendants successfully arranged a meeting with the suspected leader of the Mexican-based criminal organisation who travelled from Mexico to Greeley, CO where he was eventually arrested by HSI agents.

Source: US Authorities.

4.2.4 STATISTICAL ANALYSIS OF DATA

As has been discussed, most countries do keep some sort of record of the cash declarations made by passengers at their borders. This is a valuable source of information and can be exploited by conducting statistical analysis alongside other datasets, such as records of criminal convictions, police intelligence databases, suspicious activity reports and taxpayer information. This analysis, identifies criminal trends in legitimate and non-legitimate cash movement, which can assist in the targeting and deployment of resources. In addition the information can also assist in identifying other criminality, such as drug trafficking and tax fraud.

4.2.5 RESTRICTION ON PROVISION OF HD NOTES

Analysis of information resulting from money laundering convictions in the UK over a three-year period from 2008 to 2011 identified numerous cases where criminals were purchasing huge volumes of high-denomination euro banknotes from criminally complicit currency exchange MSBs in the London area. The UK does not use the euro as its currency and extensive research could not identify any substantial legitimate demand for high-denomination euro notes in the UK. It was clear from the evidence obtained during the money laundering prosecutions that the high-denomination banknotes were being used by criminals to facilitate the concealment of cash as an aid to smuggling it out of the UK.

Box 34. **UK Project QUAVER**

As a result of a research project, the UK's Serious Organised Crime Agency (SOCA) had been able to demonstrate, to the satisfaction of banks and other financial institutions in the UK, that the overwhelming demand for the EUR 500 note in the UK was from criminals wishing to use it to facilitate cash smuggling. As a result, banks and other financial institutions voluntarily ceased supplying the EUR 500 note in the UK with effect from the end of April 2010.

SOCA Project QUAVER (which has continued seamlessly in the transition from SOCA to the National Crime Agency, or NCA) was established as a recognition that the traditional approach to tackling the problem of complicit MSBs - arrests & prosecutions – was resulting in criminal convictions but was not having any effect in reducing the scale of the problem. MSBs who had previously sold nothing other than EUR 500 notes before April 2010 shifted smoothly to supplying nothing other than the same value of EUR 200 notes instead. Criminal groups were quickly able to identify replacements for prosecuted MSB owners as MSBs had discovered that they could charge criminals large amounts

of money for their services which the criminals were happy to pay.

Project QUAVER sought to address the problem by concentrating on 'influence activity' – delivering briefings on the problem and how to identify the risks to banks involved in currency supplies to wholesale MSBs. Wholesale MSBs involved in currency supply to the smaller complicit MSBs, and MSB trade forums. The messaging was that banks and wholesale MSBs were now in a position to identify and report suspicious activity in the currency exchange sector to the authorities, and to avoid becoming involved in it; and that if they failed to report it, and simply carried on regardless, then they would be prosecuted for money laundering themselves as they were now in possession of enough information to form a reasonable suspicion.

The verbal briefings were followed up with a series of documents detailing exactly how criminals obtained and made use of high -denomination banknotes, and the results of the study on the criminal and legitimate uses of high-denomination banknotes in the UK (which clearly showed there was no appreciable legitimate use of such banknotes in the UK and that the purchase of large amounts of them was a clear indication of money laundering).

As a direct result of Project QUAVER, the sale of high-denomination banknotes in the UK has now fallen to a small proportion of its previous magnitude (at least GBP 500 million of high-denomination euro banknotes were being sold in the UK per year), the bank that sold the bulk of the high-denomination notes to wholesale MSBs sold its foreign banknote trading division to a rival business, and intelligence from law enforcement agencies shows that criminals now find it far harder to source high-denomination euro banknotes in the UK, meaning that they have to smuggle low denomination notes instead, which is obviously more problematical due to the increase in size and weight of shipments.

Source: UK authorities.

4.3 INDICATORS

The following can all be considered to be potential indicators of money laundering through the physical transportation of cash in respect of natural persons, cargo and mail. They are intended for use by all agencies who need to work together and exchange information and intelligence to control borders effectively, including customs, police and other law enforcement bodies. They include information that can be gathered in respect of natural persons or cargo shipments by researching their available details on law enforcement intelligence databases.

It is very important to note that these are indicators only, and are intended to be an aid to profiling and a prompt for further investigations and enquiries, rather than as definitive descriptors of criminal activity warranting immediate action. Applicability of multiple indicators may be a grounds for suspicion that the funds concerned are from an illegal source, especially when the courier is not able to answer questions adequately. These indicators are drawn from numerous sources, including questionnaire responses and other FATF and FSRB papers (including 'International Best Practices: Detecting and Preventing the illicit cross-border transportation of cash and bearer negotiable instruments', 19th February 2010).

4.3.1 NATURAL PERSONS

- Requests to purchase, or possession of, large amounts of foreign currency without a plausible explanation. Studies carried out by the UK authorities in the course of project QUAVER established that the average amount of foreign currency exchanged by someone legitimately intending to use it as holiday money was in the range of GBP 350 – GBP 450.
- Possession of large amounts of money without an adequate explanation.
- Possession of money supposedly for business reasons while travelling to countries where cash payments are restricted
- Cash is only declared when passenger is intercepted, especially if the passenger first denied having money with him or declares that he carries the money for third parties.
- Requests to purchase, or possession of, large volumes of high denomination banknotes. Very few retail businesses in the EU will accept anything higher than a EUR 50 note for a routine purchase.
- Cash deposits in bank account (possibly indicating previous transportations of cash)
- Illogical travel patterns. For example less than 24 hours between inbound and outbound travel bookings, travelling to non-tourist destinations, convoluted routes for no apparent reason; vague or contradictory details of destinations or reason for travel.
- Little or no luggage
- Repeated short notice travel to the same destination
- Tickets bought for cash at very short notice at higher than normal prices
- Tickets purchased by someone other than the traveller
- Multiple individual travellers who appear to be involved in similar unusual movements or show similar travel patterns;
- Contradictory stories of apparently associated passengers
- Travel patterns that mirror smuggling patterns of illegal goods (i.e. drugs) and human being trafficking routes;
- Demeanour of passengers. Nervous, aggressive, evasive – clothes and baggage inconsistent with 'cover story', overreacts to the presence of detection animals and/or refuses to be in the vicinity of detection animals and/or other detection equipment (i.e. x-ray machines)
- Passenger has a connection (nationality, destination, origin, previous travel etc.) with a risk area or jurisdiction. E.g. those with specific crime issues; jurisdictions with non-functioning state institutions etc.

- Traveller has a criminal record indicating connection with Predicate offences (e.g. drug trafficking, OIC, etc.);
- Traveller has a history of lost or stolen travel documents;
- ID documents appear to have been falsified
- ID documents appear to be brand new
- Passenger has dual nationality
- Passenger's suitcase is 'sealed' (e.g. by wrapping in cling film etc.)
- Has refused to consume food and drinks offered on vessel, indicating that currency might be hidden in body;
- Uneasy movement or unusual body shape due to bulk cash hidden on body;
- Passenger has an iron in his luggage. Banknotes are sometimes ironed to make them easier to pack into small spaces.
- Passenger is a politically exposed person or otherwise a person of interest;
- Passenger leaves baggage at border/(air)port;
- Passenger aborts attempt to cross border;
- Last-minute check-in or boarding
- Previous use of cash declaration forms to legitimise banking large amounts of cash. As per previous discussion in this report; this can potentially be identified by FIU analysis of suspicious transaction reports
- Consignments of British Pounds contain large volumes of Scottish and/or Northern Irish banknotes. Widely acknowledged in the UK to be a reliable indicator of criminal origin of cash (but only if the traveller is not coming from Scotland or Northern Ireland)[61]
- Implausible explanations regarding the potential use or origin of the cash. For example 'I took EUR 20 000 overseas to purchase a car but couldn't find one I liked so I brought the cash back with me'.
- Volume of the currency in possession of the traveller exceeds currency/monetary control threshold of country of issuance;
- Cash is carried in several currencies;
- Currency withdrawn close to the border;
- Possession of large amounts of currency from jurisdictions unrelated to the traveller;
- small denomination, damaged and/or dirty banknotes;

[61] Further information on this issue is available on request from the UK National Crime Agency Expert Laundering Evidence team , contactable using the email address expert.laundering@nca.x.gsi.gov.uk.

- Banknotes carried in concealed form (more than necessary to prevent against theft);
- Possession of illegal goods (i.e. narcotics, endangered species, counterfeit goods);
- Traveller is in the possession of a (new) (pre-paid) mobile phone with unknown and/or few number(s) saved in the phone book;
- Possession of stored value cards that cannot be endorsed in destination country.
- Passenger appears to have detailed knowledge of and/or shows interest in the declaration/disclosure system and/or procedure;
- Passenger leaves jurisdictions with more currency than when the traveller entered the jurisdiction;
- Passenger failed to comply with declaration requirements at origin
- Travel document pages appear to be damaged to conceal past travel;
- (suspected) use of different travel documents to conceal past travel;
- Nationality stated on the travel document does not match the traveller.
- Amounts declared/disclosed do not match the actual amounts carried;
- Traveller does not object when presented with the possibility that the currency/BNI will be seized by the authorities.
- Possession of numerous cash declaration forms
- Cash is only declared when passenger is intercepted
- Cash is concealed even though it has been declared

4.3.2 CARGO AND MAIL

- Method of packing in respect of bank to bank cash shipments. Most banks prefer new notes which are usually bank banded in blocks of 100 notes, and each block banded with others to make a bigger block of 1 000. All should be a single currency and denomination and heat sealed. Banknotes are commonly transported in strong hessian or plastic sacks and each sack should only contain one currency. The seal on the bag should match the paperwork. There may be a packing list in the sack and this should match with the contents. International cash trading is based on very small margins of exchange rates so messy packaging, multiple currencies per sack, bundles of different sizes of different denominations, bundles wrapped with elastic

bands etc. are much more expensive to count and process and can be viewed as a potential indicator of criminal origin of the cash.[62]

- Cash transport is presented as a bank-to-bank transaction, but is not carried out by a Cash / Valuables in Transit Company.
- Uneconomic cash shipments. Shipment is of a very small amount of cash, why was it not simply banked and wired?
- Odd or illogical routing
- Cash is claimed by someone using fake documents - to identify himself or making fake claims concerning ownership of the money
- A frequently used shipment route stops after interference of the authorities / there is a decrease in the apparently legal activities after a criminal investigation
- No contact from the shipper or beneficial owner after a consignment has been inspected
- The owner or carrier of the cash in cargo changes their story concerning the origin and destination of the money
- The owners and carriers of the cash in cargo have different stories concerning the origin and destination of the money
- Cash is transported in high denomination banknotes
- The nature or volume of the currency does not match the point of origin
- Business sense – Why are the goods being shipped if they are readily and cheaply available in the destination country
- No economic justification for the goods or the routing.
- Goods appear to be re-used. The same goods appear to be being shipped to the same destination multiple times.
- Companies do not exist or appear not to trade
- Goods shipped or posted from high risk jurisdictions
- Paperwork is very basic, or appears to have been altered. It may also contain material errors such as spelling mistakes in names of companies, countries etc. The paperwork is not consistent with the goods.
- Beneficial owner of the cash is unclear or appears to have been disguised
- Different qualities of banknotes (some new, others old, worn and torn)
- False customs declaration

[62] Based on interview with major well known international financial institution involved in trading on international currency markets.

- Value of declaration too low for content
- Parcel shipped from/to drugs source country
- Name and address details on parcel are unclear, vague and/or falsified
- Signatures and handwriting inconsistent

4.3.3 VEHICLES

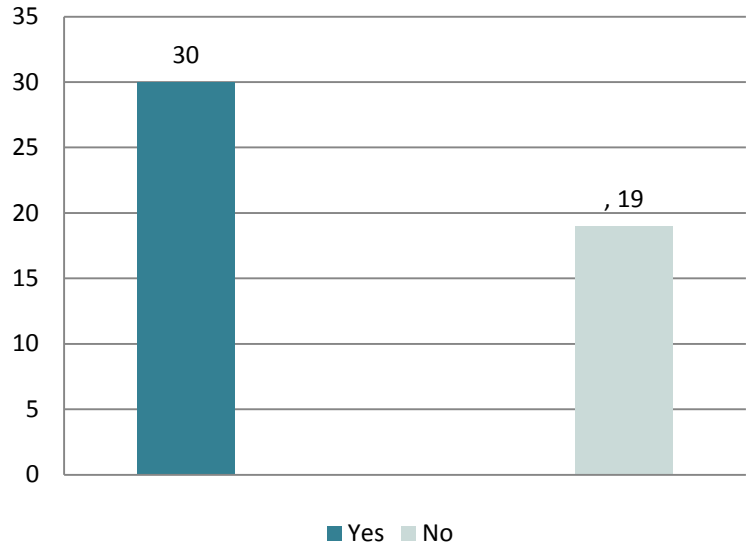
- Driver of the vehicle is not the owner
- Nationality of the driver and the nationality of the vehicle do not match
- Demeanour of driver – nervous, sweating, excessive smoking etc.
- Older vehicle
- Vehicle not insured, or insured in the name of someone who is not the driver
- Vehicle recently purchased
- Vehicle purchased for cash
- Signs of tampering – scratches or fingerprints on wheel rims or around panels, stray sealant, new screws, smell of chemicals etc.
- Inaccessible parts of the vehicle – parts of the boot/trunk, beneath seats etc.
- New wiring or electrical items (possibly electronically operated access to concealment)
- Goods carried by vehicle are uneconomic to ship
- Goods don't match paperwork
- Driver and passengers give contradictory stories
- Driver displays any of the traits detailed given for natural persons above
- Use of rental cars

5. CHALLENGES TO THE DETECTION AND CONTROL OF CROSS-BORDER TRANSPORTATION OF CASH

5.1 AT BORDERS – NATIONAL CO-OPERATION

Perhaps one of the most telling responses to the questionnaire was that to the question of whether customs officers received specific training to identify money laundering through the physical transportation of cash. Again, not all countries answered this question, but the responses of those that did are illustrated in the graphic below;

Graph 9. **Are customs officers specifically trained to identify money laundering through physical transportation of cash?**

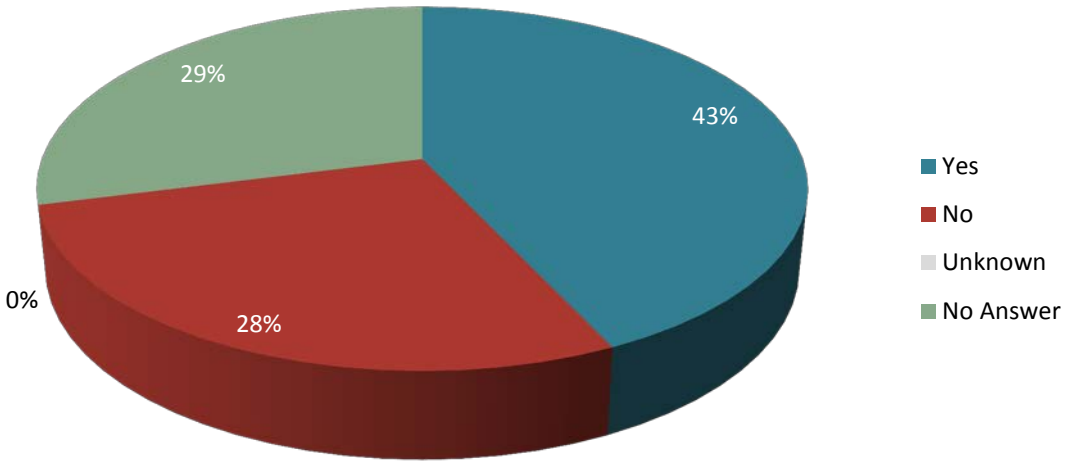


Nearly 40% of respondents do not give their customs officers specific training in how to identify cash based money laundering. This is somewhat surprising, given that cross-border transportation of cash is one of the most basic and widespread methods of money laundering. Most countries who do deliver such training agree that it is a special skill.

A second issue is that, for the majority of respondents, customs and other agencies (mainly the police) need to work together to control borders. This may be for a number of reasons, such as the policies are set by one agency but enforced by another, or because customs do not have the authority to conduct criminal investigations. Whatever the reason, effective internal co-operation is essential in order to effectively control the problem.

Analysis of the questionnaire responses highlights that, for a number of countries, their FIU have an important role to play in collating and analysing records of cash declarations and cash seizures. At least 43% of the countries that have a customs database or some other system that records the import and export of banknotes in cargo and mail, grant their FIU access to these databases.

Graph 10. **Does your FIU have access to this database?**



The figures and statistics for cash declaration and importation in cargo and mail are available to the FIU in approximately 58% of the countries. When the information is not available to the FIU (24% of the countries), it is generally because the information is not shared on a standard basis. In that case, the custom declaration system could generate the figures and statistics concerning cargo and mail for the FIU when needed. 17% of the countries did not know if figures and statistics for cash movement in cargo and mail were available to their FIU.

Resources are another issue. No country has the manpower to police all of its border crossings, all of the time (and within the EU there is a specific agreement that all EU citizens have freedom of movement across between all EU member states). Therefore, countries have to make decisions on where to place their limited resources, which has to be done on the basis of risk profiling. However the questionnaire responses suggest that some countries do not have a full appreciation of the risks, especially in respect of the effective control of cargo and mail, and so may not be in a position to make fully informed judgements.

Some countries do not yet have access to, or make use of, some of the tools mentioned in this paper, such as X-ray facilities, body scanners and cash detection dogs. These are worthwhile investments for any country as they are proven to be effective in detecting illicit movements of cash when targeting or profiling cannot always be relied upon to deliver results.

It seems clear from the number of respondents that highlighted the issue that cash declaration systems, whilst acting as an important tool in the drive to cut cash smuggling, and a valuable source of information about such things as values of cash being moved and the routes that it takes, can also be turned to the advantage of criminals. The principal way in which this may happen is the use of cash declaration paperwork to lend a false veneer of legitimacy to criminally derived cash introduced into the legitimate financial system..

Bank staff appear to have too little understanding of the systems in place and an insufficient appreciation on how cash can be made to appear legitimate by the use of a cash declaration form. In fact, there are indications that bank staff are actively encouraging people to produce cash declaration forms as an indication as bona fides, without checking to see if a declaration was checked at the border or even if it was actually made (rather than just filling out a form). Moreover, the presence of a cash declaration in some cases appears to 'blind' bank staff to obvious questions as regards the source of the funds in the overseas jurisdiction, and why the cash was imported as cash rather than being banked overseas and sent by electronic transfer.

5.2 INTERNATIONAL CO-OPERATION

During discussions of this typology, and in responses to the questionnaire and case examples submitted, the single most common challenge raised by countries was that in international co-operation. Clearly, all cash smuggling attempts have two ends, in two different jurisdictions. However, with a few notable exceptions, such as the Merida Initiative between the US and Mexico, the level of co-operation between countries at all levels appears to leave ample room for improvement.

5.2.1 INTELLIGENCE EXCHANGE

There are obvious benefits to the free and open sharing of intelligence between jurisdictions, assuming that legal issues can be overcome. Intelligence sharing makes countries aware of issues like similarities and differences between their legal arrangements, cultural and diversity issues (such as trends within ethnic groups) and current trends in typologies and methods. It can also raise awareness of features unique to a particular jurisdiction, for example the fact that large amounts of Scottish and Northern Ireland banknotes in a consignment of British pounds is a reliable indicator of criminal origin of cash.[63]

At present, there is no global framework for co-operation and exchange of data. Most countries are member of the Egmont Group of Financial Intelligence Units. However, unless data on cash seizures, cash declarations and customs information in respect of cash movements in cargo and mail (legitimate or otherwise) is routinely shared with the FIU (which again emphasises the need for national as well an international co-operation) this information will not be available, or at least not readily accessible, for sharing with another jurisdiction. In this respect, it is worth mentioning that in case of suspicion of money laundering or terrorism financing 39 countries share information on cash movements in cargo and mail with the country of origin or destination and 3 countries even share this information if there is no suspicion (spontaneous information sharing).

The WCO maintains a comprehensive database (the Customs Enforcement Network, or CEN), a valuable tool which holds large amounts of information about customs seizures and offences, acts as a website containing enforcement-related publications, and provides a separate secure system (CENcomm) to facilitate communication between users at an international level and to hold operational data in respect of criminal cases. The system can be used for a wide range of analytical

[63] See footnote 41.

purposes and can highlight new and emerging trends and methods, as well as providing statistical data that would be invaluable to most countries.

The problem is that usage of CEN and CENcomm is patchy at best. Some countries regularly input large amounts of data into the system, whereas some countries appear not to use it at all. Clearly, this has the effect of diminishing the usefulness of the data and any analysis of it that is carried out. It is not possible to state with certainty that the reason that one smuggling route appears to be prevalent is because it actually is, or because a country has decided to take special interest in it. Other countries may experience cash smuggling on a much larger scale through other routes but if they do not enter information into the system no-one will be able to benefit from their experience.[64]

It seems clear that efforts to tackle money laundering through the physical transportation of cash would be more effective if countries were more willing, or more readily able to exchange intelligence, either through CEN, the Egmont system or by any other means, for example by Memoranda of Understanding.

5.2.2 EVIDENCE GATHERING AND SHARING

A closely related issue is that of the exchange of evidence between countries. It is of paramount importance that this matter is properly handled by countries since, as has already been made clear in this paper, one of the main drivers of money laundering through the physical transportation of cash is the separation of the cash from the crime that generated it, by the simple expedient of moving it to another country. As has also been discussed, each cash movement involves at least two countries and if any criminal prosecution is to succeed, it is vital that one country is able to obtain evidence to support its case from the other. The project team has been made aware of numerous cases where requests for legal assistance have not been serviced in an appropriate timeframe (or indeed at all) by the counterpart country.

Most countries will deal with requests for mutual legal assistance from another country by preparing and submitting an International Letter of Request, or ILOR, unless the matter is covered by other statutes or conventions to which both are signatories. Discussion of the practical implications of these processes is not relevant to this paper, however the general principle is that a court in one country requests a court in another country to obtain evidence on its behalf.

One of the main challenges faced by this procedure is that countries sometimes have no appreciation of the legislative processes in the country from which they are seeking to gather evidence, or are unable to understand if the request is actually practical or even possible to comply with in that country. This will have a direct impact on the ability, and willingness, of the receiving country to service the request in an appropriate timeframe. It may be that the information requested is not centrally collated or recorded, for example, and obtaining what is sought might involve the receiving country in a marathon country-wide paper chase and the interviews of dozens of witnesses. It may also be that there is a legal impediment in the receiving country which prohibits the disclosure of the information requested, or that the information provided in the ILOR is insufficient to convince a court that coercive powers should be used to obtain the information.

64 Source – WCO presentation at Joint Expert's Meeting , Qatar December 2013.

Alternatively, the ILOR might not make it clear to whom the request for assistance would best be directed; to police or to customs authorities, for example.

Another issue is the fact that some jurisdictions receive a great many ILORs and do not have the resources to deal with them all in a timely manner. It is a natural desire of an investigating authority that the receiving country should deal with the ILOR without delay, but if the ILOR is only the most recent of twenty that have been received that week, it is unlikely that the delay will be looked on patiently by the requesting jurisdiction. Furthermore, if the request is vague, would involve a huge amount of resource to service, or is simply not legally possible, it is likely to be relegated to the bottom of the pile. An additional problem with this is that any future requests from the same country in a similar case are likely to be given similarly low priority.

At least part of the answer to these issues is better intelligence and information sharing. Countries need to have good relations with the countries from whom they are most likely to request legal assistance. They need to be able to call someone in the receiving country who will be able to advise them on the sort of information that might be available (and what will not be), how to word the request, who to send it to, and what the likelihood is of it being serviced in an acceptable timeframe. This is a matter not only for the central authorities but for the agencies themselves. Sharing information and closer co-operation are the key to ensuring an effective response to the problem.

5.3 LEGISLATIVE ISSUES

As has already been discussed, there is an issue for some countries in that, although they have a comprehensive legal framework in place to address cash smuggling by natural persons through ports and airports, they may not (without realising it) have the necessary legal tools to properly address issues in respect of cash in cargo and mail. In particular, where a shipment is (reportedly) between two financial institutions and the (sparse) customs paperwork contains all of the information legally required under customs regulations. They may not have the legal authority to detain shipments for further information or to require the disclosure of further information. If this is the case, they may also lack the legislative tools needed to investigate appropriately. In addition, there may be issues when dealing with cash that passes through a country in transit from one destination to another.

The detection of the physical transportation of cash itself is usually insufficient for establishing a well-grounded suspicion of a money laundering offence, needed in order to initiate an investigation by law enforcement agencies. At the same time in some countries, Customs would not have the authority to conduct its own research/inspection, even though the circumstances would raise questions. The latter appears primarily to be an issue of lack of legislation.

In addition, the law in some countries requires that, in order to prove a money laundering offence, investigators also need to prove the predicate offence that generated the money being laundered. This can be a significant difficulty, particularly where the predicate offence took place in another country. This again highlights the vital importance of effective international co-operation in tackling money laundering through the physical transportation of cash.

5.3.1 PROHIBITION AND/OR LICENSING OF CASH IN CARGO AND MAIL

Some countries have enacted other legislation on cash in cargo and mail in addition to their national legislation relating to specific cash declarations. In 16 countries, it is prohibited to transport cash in cargo and mail without a license. For one country, the response to the questionnaire appears to suggest a total prohibition, as this country did not mention the possibility of applying for a license. Five countries mention in their questionnaire response that they do not have a prohibition, but a license is required for cash to be transported in cargo and mail.

In conclusion, 21 countries forbid cash transportation in cargo and mail without a license. In 10 of these countries, a specific cash declaration (in addition to the normal customs declaration) is also required. Eight countries have no licensing system in place, but do require a specific cash declaration, meaning that in total 29 countries have specific legislation in place on cash in cargo and mail.

The legislation varies considerably between the countries. Countries provided the following details in their questionnaire responses:

- the threshold for applying for a license is the equivalent of USD 10 000 or USD 5 000;
- only banks authorised by the central bank have the right to conduct cross-border transportation of cash in cargo and mail;
- The central bank issues a license to permit the export of currency in cargo or mail and applies a threshold which is subject to exchange control restrictions;
- transfer of funds has to be subject to prior approval issued by the central bank for commercial institutions, and non-profit organisations require prior approval for this from the Ministry of Social Affairs;
- courier services need to be registered with the Chamber of Commerce and hold the necessary licenses;
- exporting the national currency above a threshold requires a license from the central bank;
- the licensee is required to comply with money laundering legislation;
- transporters have to comply with reporting requirements.

It is important to note that a substantial part[65] of the legislation of the 29 countries is of a monetary nature. Only some of the 29 countries actually have legislation regarding money laundering and terrorism financing in place. Also, only in some cases do customs or other authorities have the legal power to check cash in cargo and mail in respect of money laundering and terrorism financing. (This also highlights the importance of international cooperation, when addressing transnational transportation of criminal cash).

65 From the questionnaires it was not possible to find out exactly how many countries have just monetary legislation.

5.3.2 CASH IN TRANSIT

Due to customs legislation, some form of customs declaration is obligatory in all cases of cash transiting a country in cargo and mail, and customs has the legal power to check these consignments. The formalities to check transit movements of cash in cargo and mail, however, are even less extensive than in case of import and export. A brief declaration and description of goods is sufficient. That means, for example, that a transit declaration for a parcel containing second-hand books will look exactly the same as that for a box with a large amount of cash in it (assuming the cash is not declared). If there are no grounds for suspicion, and when there are no specific legal obligations relating to the transportation of cash, such as a specific cash declaration or a prohibition on transporting cash without a license, these transiting cash movements are not checked in relation to money laundering and terrorism financing. Checks only take place within the domain of customs regulation (e.g. correct declaration), but following the current risk-based approach (no tax on cash and no other legislative burdens) no consignment containing concealed cash will be selected for customs inspection. When there is a reasonable suspicion, transiting cash movements are selectively examined for money laundering and terrorism financing purposes.

Nevertheless, 39% of the responding countries indicate that legitimate cash movements *transiting* their country in cargo and mail, are *not* subject to any form of control, declaration or examination. Almost a third of the responding countries do not know if these movements are subject to any form of control. It can thus be assumed that in most countries there is no control on the transit of cash.

In responding to the questionnaire, some European Union member states mentioned a EU-wide problem regarding the limited scope of Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community. This Regulation is directly applicable in all EU member states. The barrier here is that this EU law only sets rules for cash transported by passengers (natural persons) and to cash (bearer-negotiable instruments including monetary instruments in bearer form such as travellers' cheques).

The EC is currently conducting a review of the implementation and scope of this regulation, and has sent a separate questionnaire of this issue to all member states. In the light of the responses received as well as additional analysis by the EC, this process could result in changes to the regulation.

5.4 TYPOLOGIES AND GUIDANCE

Some countries, when asked about challenges they faced in developing an effective response to the problem of money laundering through physical transportation of cash, mentioned the following issues;

- There is a perceived lack of clear and usable typologies and best practises; both from an international and national perspective. Research, including a literature review, in the course of the preparation of this report did identify that, although many individual countries and FSRBs had studied the issue, there has been no single paper that comprehensively pulled together all of this experience. Hopefully this paper will go some way to addressing this issue.

- There are no profiles available that target packages and cargo that may contain undeclared (and/or criminal) cash (essential for the risk-based approach of customs). Again, this paper is designed to address this issue.
- There is a lack of relevant information available to judge whether cash being transported across borders may possibly be connected to money laundering. As described above, this could be addressed by greater international co-operation and data sharing, and potentially by closer co-operation with the WCO.
- Once cash has been discovered in cargo or mail, barriers exist regarding the rapid and timely exchange of information between countries regarding the origin/ source of the cash. It would appear that closer co-operation between countries (particularly those who share land boundaries or ties such as ethnicity or frequency of travel by citizens between them) would be an advantage, such that the countries become more aware of the unique circumstances in each other jurisdictions, and the barriers that they need to address to enable the necessary information sharing.

ANNEX
JURISDICTIONS WHO RESPONDED TO THE QUESTIONNAIRE

Argentina
Australia
Austria
Azerbaijan
Belgium
Bermuda
Bulgaria
Canada
Colombia
Czech Republic
Denmark
Egypt
Fiji
Finland
France
Georgia
Germany
Greece
Guyana
Hungary
Isle Of Man
Israel
Italy
Jersey
Jordan
Kazakhstan
Korea
Latvia
Lithuania
Luxembourg
Malawi
Malaysia
Malta
Mauritius
Mexico
Mongolia
Montenegro
Netherlands
New Zealand
Norway
Panama
Peru
Poland
Portugal
Qatar
Saint Vincent & the Grenadines
Sao Tome & Principe
Saudi Arabia
Sint Maarten
Slovakia
Slovenia
South Africa
Spain
Sri Lanka
Sweden
Thailand
Trinidad & Tobago
Tunisia
Turkey
Turks & Caicos
United Kingdom
United States
Uruguay
Vietnam
Yemen

BIBLIOGRAPHY AND REFERENCES

Website addresses valid as per September 2015

Bagnal, J., Bounie, D. et al (2014) 'Consumer Cash Usage – a Cross Country Comparison with Payment Diary Survey Data', *ECB Working Paper Series,* no. 1685, June 2014, European Central Bank, Frankfurt am Main, Germany, https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf

Baker, R.W. (2005), *Capitalism's Achilles Heel: Dirty Money and How the Renew the Free-Market System*, John Wiley & Sons, Inc. New Jersey, United States, ISBN: 978-0-471-64488-0.

Botta, John J. (2003), *Criminological Theories and Theorists; An American Social Perspective on Crime,* Authorhouse, Bloomington, United States.

Department of the Treasurey (nd), *Report of International Transportation of Currency or Monetary Instruments*, FinCEN form 105, Department of the Treasury, Washington DC, United States, www.fincen.gov/forms/files/fin105_cmir.pdf

ECB (nd a), *Banknotes and coins circulation*, European Central Bank, Frankfurt am Main, Germany, www.ecb.europa.eu/stats/euro/circulation/html/index.en.html.

ECB (nd b), *Statistical Data Warehouse,* European Central Bank, Frankfurt am Main, Germany, http://sdw.ecb.europa.eu/reports.do?node=1000004112.

ECB (2014), *The international role of the Euro*, p. 23. European Central Bank, Frankfurt am Main, Germany,www.ecb.europa.eu/pub/pdf/other/euro-international-role-201407en.pdf?456475aa49c78ac8f912d9828d374c52.

European Commission (2010), *Report from the Commission to the European Parliament and the Council on the application of Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community pursuant to article 10 of this Regulation*, COM(2010) 429 final, European Commission, Brussels, Belgium, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0429&from=EN.

Europol (2015), *Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*, Europol, The Hague, Netherlands, www.europol.europa.eu/content/why-cash-still-king-strategic-report-use-cash-criminal-groups-facilitator-money-laundering.

Farah, D. (nd), *Money Laundering and Bulk Cash Smuggling: Challenges for the Mérida Initiative,* Working Paper Series on US-Mexico Security Co-operation, Douglas Farah, May 2010, www.wilsoncenter.org/sites/default/files/Chapter%205-Money%20Laundering%20and%20Bulk%20Cash%20Smuggling%20Challenges%20for%20the%20Merida%20Initiative.pdf

Federal Reserve (2015a), *Currency in Circulation: Volume*, updated 19 February 2015, Federal Reserve, Washington, United States, www.federalreserve.gov/paymentsystems/coin_currcircvolume.htm.

Federal Reserve (2015b), Currency in Circulation: Value, updated 19 February 2015, Federal Reserve, Washington, United States, www.federalreserve.gov/paymentsystems/coin_currcircvalue.htm.

Federal Reserve Bank of New York (2013), *How currency gets into circulation*, Federal Reserve Bank, New York, United States, www.newyorkfed.org/aboutthefed/fedpoint/fed01.html.

Hewit, Mike (2009), *Fiat Currency in Circulation, How Much Money Is There?,* The Market Oracle, www.marketoracle.co.uk/Article11576.htm

Investopedia (nd), Capital Flight, Investopedia, Oakland, United States, www.investopedia.com/terms/c/capitalflight.asp.

Johnson, E. and Payne, J. (1996), 'The Decision to Commit a Crime: an Information-Processing Analysis' in *The Reasoning Criminal: Rational Choice Perspectives on Offending,* Chapter 11, Transaction Publishers,

Judson, R. (2012), "Crisis and Calm: Demand for U.S. Currency at Home and Abroad from the Fall of the Berlin Wall to 2011", *International Finance and Discussion Papers*, Federal Reserve Board, Washington DC, United States, www.federalreserve.gov/pubs/ifdp/2012/1058/default.htm.

Knouse, K.C. (1996), *True Prosperity: Your Guide to a Cash-Based Lifestyle*, Double-Dome Pubns.

Lee, R. (2013), *Top 8 Most Tradable Currencies,* Investopedia, Oakland, United States www.investopedia.com/articles/forex/08/top-8-currencies-to-know.asp.

Soudijn (2015) *Comparing actual money laundering investigations and the three phases of money laundering: Some remarks*. (forthcoming).

State Bank of Pakistan (2014), *Foreign Exchange Manual, State Bank of Pakistan*, Karachi, Pakistan , www.sbp.org.pk/fe_manual.

Swift (2015),*RMB Tracker*, Swift, La Hulpe, Belgium www.swift.com/assets/swift_com/documents/products_services/RMB_Slides_January2015_SDC_final.pdf.

UNODC (2011), *Estimating illicit financial flows resulting from drug trafficking and other transnational organizes crimes*, UNODC, Vienna, Austria, www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

US Department of State (nd), *The Merida Initative*, US Department of State, Washington DC, United States, www.state.gov/j/inl/merida.

US Homeland Security (2010), USA-MEXICO Bi-National Criminal Proceeds Study, US Dept. of Homeland Security, Office of Counternarcotics Enforcement, Washington DC, United States, www.ice.gov/doclib/cornerstone/pdf/cps-study.pdf.

US Treasury (2006), *The Use and Counterfeiting of U.S. Currency Abroad, Part III,* US Department of the Treasury, Washington DC, United States, www.federalreserve.gov/boarddocs/rptcongress/counterfeit/default.htm.

World Bank (2015), *The Little Data Book on Financial Inclusion 2015*, World Bank, Washington, DC, United Statesdoi:10.1596/978-1-4648- 0552-3, http://data.worldbank.org/products/data-books/little-data-book-on-financial-inclusion.

World Customs Organisation (nd), *What is the harmonized system?*, World Customs Organisation, Bruxelles, Belgium, www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx

www.fatf-gafi.org | www.menafatf.org

October 2015

MONEY LAUNDERING THROUGH THE PHYSICAL TRANSPORTATION OF CASH

In order to break the audit trail, criminals often choose to remove their illicit assets from their bank account and transport these funds to another country to spend it or reintroduce it into the banking system. This report identifies the methods and techniques that criminals use to transport funds across the border and highlights the main challenges that relevant border control agencies face to detect and disrupt these transports.

This report provides a series of case studies and other information for use by all agencies, who need to work together and exchange information to control their borders.

Appendix MM:

FATF, *FATF Report: Money Laundering through the Football Sector* (Paris: FATF, 2009).

FATF • GAFI
Financial Action Task Force Groupe d'action financière

FATF Report

Money Laundering through the Football Sector

July 2009

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. Criminals have shown adaptability in finding new channels to launder the proceeds of their illegal activities and sports is one of the many sectors that are at risk of being inflicted with criminal money.

2. With the growing economic importance of sports during the last two decades, especially football, money gradually started to exert a strong influence on the world of sports. This influx of money has positive effects, but also negative consequences.

3. In order to get a better understanding, this study identifies vulnerabilities which make the football sector attractive to criminals. These are mainly related to the structure, the financing and the culture of this sector.

4. The study analyses several cases that illustrate the use of the football sector as a vehicle for laundering the proceeds of criminal activities. After this analysis, money laundering (ML) through the football sector is revealed to be deeper and more complex than previously understood. Indeed, this analysis appears to show that there is more than anecdotal evidence indicating that a variety of money flows and / or financial transactions may increase the risk of ML through football. These are related to the ownership of football clubs or players, the transfer market, betting activities, image rights and sponsorship or advertising arrangements. Other cases show that the football sector is also used as a vehicle for perpetrating various other criminal activities such as trafficking in human beings, corruption, drugs trafficking (doping) and tax offences.

5. The ML techniques used vary from basic to complex techniques, including the use of cash, cross border transfers, tax havens, front companies, non-financial professionals and PEPs.

6. In many cases, connections with other well-known ML typologies were identified such as trade-based ML, the use of non-financial professionals and NPOs for ML purposes, ML through the security sector, the real estate sector and the gaming sector.

7. Various initiatives are taken by international and national actors in order to combat threats to the integrity of football, including ML. Looking ahead, there appear to be a number of areas that could be considered to improve the capacity to cope with the ML risks associated with the football sector.

INTRODUCTION

8. In reaction to the increasing compliance of financial institutions all over the world with the Financial Action Task Force (FATF) anti-money laundering and counter-terrorist financing standards, criminals have shown adaptability in finding new channels to launder the proceeds of their illegal activities. Simultaneously, the globalisation of financial markets and the development of information technology have gradually boosted the criminal economy and have expanded the possibilities for economic crime. In this context, there are growing concerns that various legitimate sectors are at danger of being infected with criminal money.

9. The sporting industry is one of the many sectors that could be attractive for criminals for money laundering purposes and merits closer consideration given the large scope of monetary transactions and the increase in the number of individuals involved.

10. In order to get a better understanding of the process of money laundering, of ways in which criminality can be connected with legal economic activities, and how criminal money finds its way into legitimate businesses, the FATF decided in June 2008 to study on money laundering through the football sector.

11. The following countries joined the project team and contributed to the study: Argentina, Belgium (as project co-leader), Brazil, France, Ireland (as project co-leader), Italy, the Netherlands (as project co-leader), Norway, Sweden, Switzerland and the United Kingdom. The report was written with support from the OECD sub-group on tax crimes and money laundering.

Scope

12. The aim of this project is to study one specific sport which could reveal money laundering schemes that may also be occurring in other sports. As one of the largest sports in the world, football[1] was chosen. Both professional and amateur football were to be examined. Although the scale of vulnerabilities to money laundering is potentially different, risks in both areas were considered likely to be similar.

13. On the other hand, the title of the project was broadened from 'clubs' to 'sector' because focussing on clubs was too narrow. Vulnerabilities not only occur within clubs but concern also other important stakeholders within the football industry. For these reasons, the original scope of the project 'money laundering through sporting clubs' consequently has turned into 'money laundering through the football sector'.

[1] The term *football* is used in different ways in different parts of the English-speaking world. The name *soccer* (or *soccer football*) was originally a slang abbreviation of the word *association* from *association football* and is now the prevailing term in the United States, Canada, Ireland, Australia and New Zealand. Of the 45 national FIFA affiliates in which English is an official or primary language, only three (Canada, Samoa and the United States) actually use *soccer* in their organisations' official names, while the rest use *football*.

Methodology

14. This report is based on four main sources: an extensive literature review, the analysis of the answers to a questionnaire sent to FATF and FSRB members; the results of a typology workshop and subsequent consultation with the football sector.

15. Results to the questionnaire[2] were obtained in October 2008 from 25 countries, mostly European, seven South-American countries, two from Asia and Australia.[3] The responding countries differ widely in size, role and organisation of football in society (ranging from large countries with big football leagues to smaller nations or nations with only non-professional football). Differences in information, position and interest in the person or organisation that provided the answers (national football association, government representatives, national FIUs, the police or judicial authorities) needed to be taken into consideration as well.

16. Following the analysis of questionnaires, a workshop on money laundering and the football sector was held in Monaco in November 2008 as part of the 2008 FATF/MONEYVAL Typologies meeting. This workshop was very well supported by members of the FATF, MONEYVAL and representatives of other countries. The following participants were involved in the 2-day breakout session which considered issues in depth: Belgium, Brazil, Cyprus, Egmont Group, France, International Olympic Committee (IOC), Ireland, Italy, Monaco, Norway, Russia, Slovenia, South Africa, Switzerland, the Netherlands and the United Kingdom.

17. The study has also relied on the experience and cooperation of the private sector. A representative of the IOC attended the Monaco workshop in November 2008. Consultation with representatives of the Fédération Internationale de Football Association (FIFA) and of the Union of European Football Associations (UEFA) also took place in January and April 2009. Those representatives received a copy of the report and were given the opportunity to comment. All the comments of the private sector were taken into account when considered relevant.

18. The project team would like to acknowledge the input of all the participants.

[2] The questionnaire is attached as an annex.

[3] Completed questionnaires were received from: Argentina, Australia, Belgium, Brazil, Canada, Chile, Colombia, Ecuador, France, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, Portugal, Romania, Singapore, Sweden, Switzerland and the United Kingdom.

CHAPTER 1: MONEY LAUNDERING AND SPORTS

19. Since ancient times, societies throughout the world have devoted considerable resources to sports, as well as offering praise to the exploits of sportsmen. What is new today is the surge of commercialisation of sport, the unprecedented internationalisation of the sports labour market, the considerable sums of money flowing in from broadcasters and sponsors, and massive cross-border investments by sponsors, including the sporting industry itself and sometimes "super rich" private investors.

20. It is difficult to ascertain the overall economic value of sports. According to some recent estimates in Europe, the sporting industry accounts for from 0,5 to 3,7 of overall EU-GDP, depending on the definition of sporting industry.[4] Big matches in large stadiums are undoubtedly important to local economies. In addition, sport has an important social and psychological function at all levels of the society.

21. With the growing economic and social importance of sports and increasing profits that can be made out of sports, money now exerts a strong influence on the world of sports. The influx of big money has positive effects such as an increase of sport facilities and their availability to a larger number of people, yet this money also brings negative consequences. There is a higher risk of fraud and corruption given the amount of money at stake. Sport also can be used as a channel to launder dirty money.

22. Sports governing bodies as well as national and international authorities recently expressed their concerns on the inflow of dirty money into the sporting industry. The EU White Paper on Sport – the first EU Community document to recognise the importance of sport in European society – which was published in 2007 – stated, "Sport is confronted with new threats and challenges, such as commercial pressure, exploitation of young players, doping, corruption, racism, illegal gambling, violence, money laundering and other activities detrimental to the sport."[5]

Which sports?

23. Based on a literature review and the results of the FATF-questionnaire, several sports can be identified as being vulnerable to money laundering. Sports that are regularly indicated as being vulnerable

[4] Sound and comparable macro-economic data are generally lacking, due to, among others, problems of definition. For example, according to a paper presented to the EU in 2006 the sporting industry in Europe should be responsible for 0.5% (sport defined in a narrow sense) to 3.7% (according to the widest definition including tourism, insurance and for example better health) of overall European GDP (See: Dimitrov, D., Helmenstein, C., Kleissner, A., Moser, B., Schindler, J. (2006)). However, the vast majority of sporting activities still take place in non-profit structures, many of which depend on public support. At the same time a large part of the growing economic value of sports is linked to intellectual property rights (such as copyright, commercial communications, trademarks and image and media rights).

[5] Commission of the European Communities (2007).

to criminal money are football, cricket, rugby, horse racing[6], motor racing, car racing, ice hockey[7], basketball and volleyball.

24. Just like any other business, sport can be used by criminals to launder the proceeds of crime or to perpetrate illegal activities for financial gain. Unlike other businesses, it is not always the profitability as such that make sport attractive to criminals. Connections that criminals seek to make with sport are not only motivated by the desire to gain money. Social prestige is another important factor. Popular sport can be a route for criminals to become 'celebrities' by associating with famous people and moving upwards to powerful circles within established society.

25. Sports that could be vulnerable to money laundering problems are either big sports (worldwide like football or on a national basis like cricket, basketball or ice hockey), sports like boxing, kick boxing and wrestling (sports that have traditionally links with the criminal milieu because of the relationship between crime and violence), high value sports (such as horse and car racing where there are ample opportunities to launder big sums of money), sports using (high value) transfer of players, sports where there is much cash around, which give criminals opportunities to turn cash into non-cash assets or to convert small into large bills. This fact means that virtually all sports could be targeted by criminals, although for different reasons.

26. A topic that deserves separate attention is betting on sporting activities. This touches upon a broad range of sports. Money laundering through legal and illegal betting, especially on the internet, is considered as a huge and increasing problem that should be explored separately in more detail. For the purposes of this study, betting on sporting activities falls outside the scope of this work and has therefore not been studied in detail.

Why football?

27. If we want to examine money laundering through sport, football is an obvious candidate. Football is by far the biggest sport in the world. There are 38 million registered players and 5 million referees and officials. Football is played all over the world and is the most popular sport in many countries. Football can count on a broad base of support, ranging from loyal fans attending weekly matches of their club, to

[6] The FATF in earlier research has already pointed out that gambling on horse races provides ample opportunities for money laundering. Circuits have been set up to organise systematic buy-back of winning tickets from their legitimate holders. Furthermore, persons can also gamble money in order to have it laundered. If their chips are repaid at the end of their gambling session in the form of a cheque from the gambling or betting agency, apparently verifiable "winnings" are obtained. The New York Police discovered an underground operation involving the large-scale conversion of small bills into large ones with a Jamaican gang acting as a front for the Gambino crime family (New York Times 2001). This is according to the New York Police a typical form of money laundering designed to facilitate the smuggling of cash out of the country by reducing the bulk (Office of the New York State Attorney, 2001). Other ways by which money laundering can be laundered through horse racing are the acquisition of horses and the organisation of illegal races.

[7] The National Hockey League (NHL) has 30 teams in the US and in Canada, almost 1 million registered players and is one of the largest money making sports leagues in the world generating billions of dollars in revenue. It is also popular in Russia, Scandinavian countries and central European countries such as the Czech Republic. The Russian mafia is reportedly attracted to hockey, both in the former Soviet Union and abroad (Hill, D. (2008)). There are various famous cases of extortion by Russian mobsters against Russians playing in the NHL. There are examples of infiltration in hockey franchises, not only by criminals from Russia. Internet gambling on hockey, connected with match fixing, is another way by which criminals can launder millions of dollars without any suspicion.

passive spectators at home in front of their television screens. The FIFA World Cup Final in 2006 attracted just over 1 billion viewers or 15 percent of the world population.

Table 1. Key Statistics Football Around the World (2006)

Total players	265 million
Female players as % of male world population	8%
Registered players	38 million
Referees and officials	5 million
Number of clubs	301.000
Top-20 countries with most registered players in 2006:	Germany (> 6 million), USA (> 4 million), Brazil (> 2 million), France, Italy, England, South-Africa, Netherlands, Japan (> 1 million), Canada, Russian Federation, People's Republic of China, Ukraine, Czech Republic, Poland, Spain, Austria, Sweden, Chile and Iran (> 0,4 million)

Source: FIFA 2007.

28. The professional football market has undergone an accentuated growth due to a process of commercialisation since the beginning of the 1990's. Money invested in football surged mainly as result from increases in television rights and corporate sponsorship. Simultaneously, the labour market for professional football players had experienced unprecedented globalisation – with more and more football players contracted by teams outside their country and transfer payments of astounding dimensions. Transfers are carried out all over the world. The cross border money flows that are involved may largely fall outside the control of national and supranational football organisations, giving opportunities to move and launder money. At the same time money from private investors is pouring into football clubs to keep them operating and can give the investor long term returns in terms of media rights, ticket sales, proceeds of sales of players and merchandising.

29. Betting on sports offers another means of allowing substantial money flows to move beyond the control of governing bodies. Due to its particular structure, as well as the considerable need to finance the system at short sight, notably at club level, football offers an interesting platform for irregular betting activities.

30. Football has changed from a popular sport into a global industry with an increasing economic impact at the top and important social functions at lower levels. Football can serve not only as a source of income for many people, but also as a tool for local economic development, social cohesion, education, personal development and the transmission of human and cultural values. Partly due to the industry's growth, football seems to be confronted with various forms of crime and corruption - including money laundering.

31. The multiple relations between crime and football have been described and analysed in several books[8], and some 'headline-grabbing' money laundering cases have been revealed by the international media. There are connections between criminal organisations and the world of football – ranging from internationally operating organised crime infiltrating top football to locally operating criminals with connections in local lower leagues or even amateur football.

[8] See for example Hill, D. (2008) and Johnson, G. (2006) on the influence of organised crime on football in the UK. Or Robert, D. (2006), who states that "*le football est devenue un formidable machine à blanchir l'argent*". Also interesting in this respect is Glenny, M. (2008) on the modern spread of transnational crime after the break-up of the Soviet Union and the simultaneous deregulation of global markets. Glenny also touches upon connections between Eastern European criminals and the world of football.

CHAPTER 2: STRUCTURE OF THE FOOTBALL SECTOR

Football governance

32. The international governing body of the football industry is the Fédération Internationale de Football Association (FIFA). FIFA's purpose is to promote and develop football throughout the world. FIFA also is the guardian of the regulations of the game. FIFA consists of six confederations (AFC, CAF, CONCACAF, CONMEBOL, OFC and UEFA)[9] which are the umbrella organisations for the national football associations. Professional and amateur football clubs are members of their national football associations. National associations must be members of both FIFA and the confederation in which their nation is geographically resident for their teams to qualify for entry to FIFA's competitions. FIFA has in total 208 member associations (one per country). The whole industry is built on two main pillars: club football and national team football.

33. UEFA is one of the biggest of the six confederations of FIFA. It is by far the strongest in terms of wealth and influence over the global game. Virtually all of the world's top players play in European leagues. This is in part due to the salaries available from the world's wealthiest football clubs, particularly in England, Germany, Italy and Spain. Two of the top seven teams in the FIFA World Rankings are nevertheless CONMEBOL members (Brazil and Argentina).

34. At a lower level, the FIFA confederations like UEFA consist of national associations, of which the English Football Association, founded in 1863, is the oldest. The national associations of each country operate league systems, normally comprising several divisions. The national associations are the supreme regulatory and disciplinary body of the sport within national boundaries. Their autonomy however is restricted to the fact that they have to abide by the rules of FIFA and the six confederations like UEFA and CONMEBOL. In some countries the football sector is organised in regional associations on a lower level. The individual clubs - according to FIFA - are the basic cell at the foundation of the pyramid.

[9] AFC - *Asian Football Confederation* in Asia and Australia, CAF - *Confédération Africaine de Football* in Africa CONCACAF - *Confederation of North, Central American and Caribbean Association Football* in North America and Central America, CONMEBOL - *Confederación Sudamericana de Fútbol* in South America, *OFC - Oceania Football Confederation* in Oceania and UEFA - *Union of European Football Associations* in Europe.

35. Traditionally sporting associations have defined the rules of the game, including financial rules, at an international level. FIFA was established in 1904 in response to the need for a single body to oversee the game worldwide. One of objectives of FIFA is prevention of practices that might jeopardise integrity of the sport. It is for this reason that FIFA insists it is necessary to have global football regulations that apply to everyone everywhere.

36. National governments still adhere to some degree to the policy that the specific nature of sport, its important social, educational and cultural functions, sets it apart from any other field of business activity. In Europe for example the European Council officially endorsed in the Nice declaration of 2000 the need to protect independence, autonomy, self-regulation and self-organisation of sports according to the principle that *'sports and politics don't mix'*, however also while respecting individual EU and national legislations.[10] Regulatory functions for the sports sectors are performed by private organisations – sports governing bodies – rather than by governments. For historical and cultural reasons, all EU member states have, to various degrees and to a large extent, left the regulation of sport to the sports bodies. It is believed that this has helped to remove (or at least reduce) the risk of political influence being brought to bear on sports matters. The European Council believes that this principle should be preserved for the future.[11] Sport also has very specific economic characteristics – for example the necessarily joint-production of 'the product' (football matches, football competitions) by competitors.

Football finances

37. There are no comprehensive figures of the overall size of the football sector in the world. However, according to the Deloitte Annual Review of Football Finance (which is the leading yearly overview on the finances of football in Europe) the total size of the European football market has grown to an estimated at 13.8 billion EUR in 2007 (which is 0.1 percent of EU GDP). Behind these numbers, football sector revenue can be represented as a reversed pyramid. The big five European leagues – the premier League in England, Bundesliga in Germany, la Liga in Spain, Serie A in Italy and Ligue 1 in France - attracted more than half of these revenues (see table).

Table 2. Revenue distribution in the professional European football market, 2007

	%	billion EUR
'Big five' European leagues	52	7.2
'Big five' other leagues	16	2.2
Non 'big five' top leagues (other 48 UEFA countries)	15	2.1
Non 'big five' other leagues	3	0.4
FIFA, UEFA and National Associations	14	1.9
Total	100	13.8

Source: Deloitte 2008, chart 1.2.

38. It is in these five leagues that the richest football clubs in the world can be found. To be more specific, all but one of the Forbes' list of 25 most valuable football clubs in the world belong to these 'big

[10] Point 7 of the Nice Declaration reads as follows: "*The European Council stresses its support for the independence of sports organisations and their right to organise themselves through appropriate associative structures. It recognises that, with due regard for national and Community legislation and on the basis of a democratic and transparent method of operation, it is the task of sporting organisations to organise and promote their particular sports, particularly as regards the specifically sporting rules applicable and the make-up of national teams, in the way which they think best reflects their objectives."*

[11] Arnaut, J.L. (2006).

five' European leagues (the exception being Celtic in Scotland). The other half of the total European football sector is divided between the other top and lower leagues in Europe and FIFA and UEFA.

39. Professional football in Western Europe relies on four main revenue sources: match day revenues (gate receipts and all-season tickets), television rights, sponsorship (brand name placing on shirts and around stadiums), and other commercial revenues (licensed merchandise, conference and catering services). As table 3 shows, the relevance of television money is especially big for top-division clubs in the big five European leagues, depending on the size of the television market (35 to over 60 percent of total revenues). Clubs in countries with less developed economies rely for the biggest part on financial support from owners and in some cases also local or national government.

Table 3. Revenue breakdown for the ten biggest European leagues , 2006-07

	Total (in million EUR)	Matchday %	Broadcast %	Sponsorship %	Other %
England*	2 273	35	39	26	-
Germany	1 379	22	35	26	17
Spain*	1 326	26	42	32	-
Italy	1 163	13	63	12	12
France	972	14	58	18	10
Netherlands	398	30	17	40	13
Scotland*	259	50	21	29	-
Portugal	239	33	19	13	35
Austria	151	13	9	60	18
Sweden	87	30	28	32	10

* Sponsorship and other commercial combined.

Source: Deloitte 2008, chart 1.3 and 1.8.

40. On the spending side, roughly more than half of the budgets of professional football organisations is spent on salaries and related costs – which means players' salaries plus net transfer payments. Other payments include salaries paid to other staff, business costs, image rights, signing-on fees and transfer fees, including fees to players' agents. In smaller countries and lower divisions, players may be part-timers with a second job, or amateurs.

41. Within the big five European leagues, over half of the revenues is spent on salaries and related costs for players – these amounts paid to a very select group of top players, agents, managers, coaches. The industry is thus characterised by a very uneven distribution of income - ranging from amateur players at the lowest level, to half professionals, full professionals, and a select group of world star players.

42. To give an idea of the recent growth of professional football in Europe, total revenues in the big five European football leagues rose from EUR 2.5 billion in 1996-97 to EUR 7.9 billion in 2007-2008. Most of this increase came from broadcasting, of which a large part was channelled to increasing wage costs as the top European leagues attract most of the world's best players. Wage costs increased to over EUR 4.2 billion, compared with 1.2 ten years ago.

43. As already mentioned, the total size of the European football market is estimated at EUR 13.8 billion EUR, of which EUR 4.2 billion is spent on salaries in the big five European leagues, comprising only 98 clubs in total. This means one third of the football money flowing into the hands of a

select group of just a few thousand star players and their managers. There are thousands and thousands of clubs – professional, semi-professional and amateur – scattered all over the world that fall outside the national and international elite of top clubs. The top clubs are able to attract young talent and best players from less wealthy clubs, including clubs in Africa and South America.

44. Considering these money flows, several important financial actors in the football industry can be identified: the clubs (basic cell of the industry), football players (most valuable assets of the industry), corporate sponsors (in most levels most important investor), media (especially powerful in top-league football), individual investors ('club patrons'), local business clubs or talent pools (investing in a club or in the acquisition of individual players), football agents (acting in the interest of the player or as an intermediary on the transfer market), (local) governments (subsidising clubs, acting as a lender of the last resort, sometimes owner of the stadium complex), tax authorities (in some cases a failing club will delay meeting its tax obligations in the hope of avoiding liquidation), real estate proprietors (stadiums are not always owned by the clubs or local government). In addition associations or leagues can act as regulators as well and sometimes operate financial clearinghouses for transfer payments. In some countries, supporters provide large amounts of cash and have an influence over club owners, the management and supplying businesses as well as, in a small number of cases being allegedly linked with organised crime. If there is fraud, corruption, tax evasion or money laundering it takes place within the complex network of relations between these actors.

CHAPTER 3: VULNERABILITIES OF THE FOOTBALL SECTOR

45. What makes the football sector specifically vulnerable to money laundering? A long list of possible vulnerabilities can be compiled based on responses to the questionnaires.[12] These vulnerabilities are not unique to football or even sport in general, and they vary depending on the specific size and structure of the football sector on an international, national or even local level. Most vulnerabilities apply to professional football; a smaller set occur also in amateur football.

46. Several factors combine to make football one of the many sectors that is attractive to criminals. Based on our analysis, three areas of vulnerabilities were identified, which relate to the structure of the sector, the sector's finance and the sector's culture.

Vulnerabilities related to the sector's structure

47. ***The market is easy to penetrate***: This is mainly due to the low or absent entry barriers of the sector. Football fans from all areas of society meet at the football stadium. Meetings between government and corporate officials, and the legitimate and criminal world present opportunities for collusion.

48. ***Complicated networks of stakeholders****:* The sector is complex and characterised by opaque networks of stakeholders and interdependence between the different actors. With the growth in the number of international transfers and the skyrocketing sums of television and sponsorship money that is spent on sales and purchase of players, more and more people are involved in the sector such as managers, intermediaries, sponsors and companies who own players. This large number and range of stakeholders and the money flows facilitates the concealment of fraudulent activity, in particular as many of the transactions and the criminal activities are carried out abroad.

49. ***Management lacks professionalism***: Except for the major professional leagues, which have been managed professionally for a number of decades, the management of the football sector has only recently begun moving from a style appropriate to the sport of amateurs to one of professionals. The real sports business is fairly new. It really started only twenty years ago. Even today, management can still be volunteer and inexperienced. However, in many cases there is indeed development towards levels of professional management that is more in line with the current management standards – both in amateur and in professional football.

50. ***Diversity of legal structures***: the legal structures of football clubs vary from private limited companies to foundations. Often the stadium activities are managed through different companies. In some cases players' funds (talent pools) are separate legal entities. The lack of regulation or control over legal structures and the ownership or control of football clubs means that they are easy to acquire.

[12] Less than half of respondents answered 'yes' to the first question of the FATF questionnaire ("Do you consider the football sector in your country vulnerable to money laundering?"). Mainly smaller countries, countries without a professional league or where football is not the biggest sport answered 'no'. Football seems to be more vulnerable when the football sector is big and deeply rooted in society.

Vulnerabilities related to the sector's finance

51. ***Considerable sums are involved***: The sector deals with considerable cash flows and large financial interests. Many of the transactions within the sector involve large amounts of money, for instance on the transfer market. Competition is stiff, both nationally and internationally, and the performance of a club on the field also determines its financial position. Financial circuits are multiple and global, and the international money flows that are involved risk falling outside the control of national and football organisations. Often these money flows move in and out of tax havens or involving many countries. It was not unusual for clubs that had a large proportion of their revenues from stadium entry tickets to receive nearly all their revenues in cash.

52. ***Irrational character of the sums involved and unpredictability over future results:*** Prices for players can appear irrational and are hard to control. As well with the discovery and subsequent training of young talent, massive but uncontrollable profits can be made. Transfers are carried out all over the world, providing ample opportunities to launder money. In addition, sport is essentially characterised by a high level of unpredictability over future results. This 'culture of unpredictability', might lead to an increased tolerance towards seemingly irrational payments. There is a wide variety of different accounting methods applied. Finally, the intangible nature of player values has led to some strange practices – for example, in some countries there was historically a practice of reciprocal over-valuation of players between two clubs in a deal where players were exchanged allowing inflation of asset values/the balance sheet.

53. ***Financial needs of football clubs:*** Despite the tremendous growth of the industry as a whole, many football clubs are financially in bad shape and their financial trouble could urge football clubs to accept funds from dubious parties. The financial fragility is partly the result of the nature of the game. Big clubs need large sums to have success and to be able to buy players. Sport is a typical 'winner-take-all market'.[13] Winner-takes-all markets do not pay according to absolute performances but according to performance relative to others. Losing just one game can have massive financial consequences (decline of income from sponsors, television rights, relegation to a lower division). Financial vulnerabilities can make football clubs an easy target for dirty money. Clubs that face relegation or are in financial trouble could be in need of 'financial doping'. The inherent financial fragility could be exaggerated by the recent global financial crisis, which has made it harder to find sponsors. There is a risk that clubs that are in debt will not ask many questions when a new investor appears. Moreover, a very high proportion of the sector's cost base is composed of tax, meaning in some cases a culture of seeking to circumvent tax and closer proximity to underground activities.

[13] In certain jobs, the market pays individuals not according to their absolute performance but according to their performance relative to others. The income of window cleaners depends upon how many windows they clean, but sportsperson's pay may depend upon their performance ranking (and window cleaners are easily substitutable unlike top sports talent) (see Rosen, S. (1981) for example). Slightly more talented window cleaners will make only a small difference to the transparency of their customers' windows, but in sports that slight edge can mean everything to their clubs' status and financial position. Rewards at the top are therefore disproportionately high, and rewards below the top are disproportionately low. People in these professions are often willing to work for very little just to have the chance to compete for the top job and the jackpot that comes with it. In a normal market, sumptuous superstar incomes would attract competition from more applicants to do the jobs that pay them. This would then bring salaries down to less exotic levels. In a winner-takes-all market, this does not happen. This sort of economics has long been prevalent in celebrity-dominated businesses such as entertainment and sport. Globalisation has expanded the market for skills, increasing the opportunities for the rich to become even richer. Source: *The Economist*, www.economist.com, research tools, economics a-z.

Vulnerabilities related to the sector's culture

54. ***Social vulnerability of some players:*** (This is especially the case with younger players.) If they are badly advised, players could easily be subject to shady businesses. This could make it easy to manipulate some market's key players.

55. ***Societal role of football***: People are reluctant to shatter sports' illusion of innocence. Therefore, illegal activities may not often be reported. Furthermore, the image of sports is very important, particularly to the sponsors. Sponsors try to buy a good image by supporting a particular sport. A rumour about money laundering will likely result in the withdrawal of the sponsor and his funds and loss of fans and the revenue they bring. This makes it less likely that money laundering or other crimes are reported by the management of football clubs.

56. ***Non-material rewards:*** Football has a status with which many people would like to be associated. Criminals often seek a status outside the criminal world and football can offer the opportunity for acquiring such a patron status ('sugar daddy') thanks to supporting a club no matter where the money comes from. An investment in a football club can provide the criminal the favoured status. In most cases investments in football clubs are characterised by a high degree of uncertainty over future results. However there are strong non-material rewards for wealthy individuals who invest in football clubs or players. Football clubs are deeply rooted in (local) societies. This makes football clubs an attractive way to gain social status in the local community and get entry to the establishment. By investing in football, criminal organisations might also gain control of associated activities such as betting, real estate businesses and contracts with the local government (in some countries, many club owners have come from the construction industry). This complex set of financial and non-financial motives could make football attractive to criminals seeking legitimate social status. What is happening is that the laundered money is being 'integrated' and being used to buy celebrity and influence which have a value of their own and provide opportunities for further legal and illegal gains. The criminal is buying an entrance ticket to a social milieu. Football has indeed a long history of investments by private wealthy individuals or companies who have achieved success in other businesses. There are also instances of individuals with more dubious background investing in football – both on the highest levels of the football pyramid and on local amateur levels – and gaining legitimate status in society might be a motivator for this.

CHAPTER 4: CASES AND TYPOLOGIES

57. Based on our analysis of the use of the football sector as a vehicle for laundering the proceeds of criminal activities, a variety of money flows involving various financial transactions increase the risk of money laundering. These are related to:

- Ownership of football clubs
- The transfer market and ownership of players
- Betting activities
- Image rights, sponsorship and advertising arrangements

58. What evidence do we have about these risk areas? Over twenty cases of money laundering through the football sector, ranging from simple cases of smuggling large amounts of cash that seem to be derived from illegal transactions, to complex international money laundering cases, have been collected from the responses to the FATF questionnaire, cases presented at the 2008 FATF/MONEYVAL Typologies exercise and a literature survey. Some of the most interesting cases along with fictional typologies, constructed to highlight the vulnerabilities in the sector, are presented below. Most cases identify pure money laundering. Some cases that are presented below also focus on other predicate offences in connection to football. In these cases, money laundering appears as a potential risk or as the inevitable consequence of the predicate offence.

Ownership of clubs

59. Investments in football clubs can be used to integrate money of illegal origin into the financial system, akin to investment of proceeds crime in real estate. Football clubs are indeed seen by criminals as the perfect vehicles for money laundering.

Case 1: Funding of a non professional football club

Following the receipt of a STR made by an accountant, a European FIU investigated a case regarding the funding of an amateur football club. It appeared that the accounts of the club were regularly in deficit and were balanced at the end of the season by exceptional payments from a businessman through a number of his companies. This businessman was the president of the club; however, his investments appeared suspicious for the following reasons: (1) the funding was provided without any negotiated compensation, neither financial nor sportive, (2) the funding was provided through the companies of the businessman to their prejudice: the amounts invested in the football club were extremely disproportionate to the companies' financial possibilities.
Further investigation by the FIU revealed that the accounting information of some of the companies had not been correctly registered as required by the law. So it was not possible to verify the exact financial capacities of those companies. Finally the financial analysis revealed gaps between the accounting documents showing the breakout of the various payments for funding the club and financial flows observed on the bank accounts of the various companies of the businessman, the president of the club. By excessive withdrawal of funds from the treasury of its companies without economic justification and in a way which compromises the financial balance of those companies, the businessman was misusing company assets, which is a criminal offence. The funds derived from this offence are illegal and their use to fund the football club constituted a ML offence. The case was transmitted to the public prosecutor on the basis of a presumption of misuse of company assets and laundering of proceeds from the misuse of company assets.

Source: France.

60. Investments in football clubs are a risk area for money laundering due to a lack of transparency regarding the source of funding. Indeed, investments may be unclear and obscure, making it difficult to verify the origin of the invested funds. This situation is in fact not different from the acquisition of any private company in the industrial or commercial sector. The preventive measure foreseen in the FATF Recommendations and in the AML legislation of FATF members is indeed the customer due diligence measures that financial institutions and non-financial professions would apply in this kind of transactions. However, suspicions of the influx of dirty money into football through these "sugar daddy" investments are hard to prove. If private investments in football clubs occur from the lowest amateur levels up until the world's top clubs, the targets are frequently clubs in financial trouble looking for "lifesaving" sponsors.

Case 2: Investing in a club in financial difficulties

The FIU of country B received a disclosure from a bank with regard to suspicious transactions concerning club A. This club, which was in financial difficulties, was looking for funds (several million EUR) in order to avoid bankruptcy. A financing proposal was put forward by a financial group established in South America. It was linked to an individual that had already invested funds in various foreign clubs. These funds were suspected to be of illegal origin. After the bank inquired into the origin of the funds the financial group withdrew from the negotiations. A second financing proposal was then put forward by Mr. COX, a European investor through his company located in a tax haven. Suspicions were aroused because this individual, unfamiliar to the world of sports, had suddenly suggested investing money of unknown origin in club A. Additional information showed that Mr. COX was known to the police and FIU for various cases of fraud. In this case the different possibilities for investing in club A can be considered to be attempts to launder money of illegal origin.

Source: Belgium.

61. Football has a long history of private persons investing in clubs, with investments often being made by individuals who have made profit in other businesses including politically exposed persons (PEPs) and individuals with a suspected or even known criminal background. As football clubs may not always be very profitable and future returns on investments are highly unpredictable, investments may not essentially be made for purely economic reasons. An investment in a football club can provide the criminal a favoured status. By investing in football, criminal organisations get entry to the local or even national establishment.

Case 3: Drug trafficking and investment in a football club

Mr Heep, a person of humble origins living in a small town in the interior of the country migrated overseas, returning 5 years later with a lot of money and ownership of various companies in the border area (businesses that require investments of large amounts of money which obviously were not in his purchasing power). Later Mr Heep acquired a football team which was at that point languishing in the third division. The team was not an attractive investment. One advantage was its location in a major city in the country; however, Mr Heep moved the team to a small town of barely 30,000 inhabitants, where it could expect lower profitability because of the smaller numbers of followers. This activity showed all the indicators of a non-profitable business; however, the salaries and infrastructure paid under this new administration were well above the average of other teams in the same category, and the sponsoring companies were known for their low financial solvency. It is presumed that the payment of high salaries, infrastructure and the alleged sponsorship were aimed at increasing the value of the franchise in order to legitimise its investors as recognised entrepreneurs and important people in sports sector. The team rose from third to second division in a year. Later, the investor was identified as the leader of a drug trafficking network.

Source: Mexico.

62. It has been observed in several countries that some owners and / or investors in football clubs are often awarded contracts for public works.

Case 4: Corruption and PEPs

A pseudo-businessman linked to local government officials acquired a profitable team in the professional football league and used this as a means to attract politicians and officials of various levels of government. Thanks to his team and football matches, he had access to local officials with decision-making power over the state's public works, and he used these contacts to ensure that major public works were assigned to him.

Source: Mexico.

63. The following are examples of the way in which a football club could become a vehicle for money laundering, through the investment in or purchase of a club[14]. It is not vital to the mechanism that the business at the centre of it is a sporting club, merely that the business can be bought easily and that high value transactions are part of its normal business model. Any business with a significant cash turnover would be as vulnerable to manipulation in this way.

Case 5 (fictional): Securities based money laundering

A is a well known international figure who has substantial available funds from business enterprises (Sound Co) in loosely regulated jurisdictions. A buys football club X and recapitalises the club partly by a loan to the club and partly by the sale of new share equity. The value of the club (and the share equity) rises because of the involvement of A. He retains a majority shareholding and the club repays the loan from the new share equity.

A enters into negotiations through agents on both sides to buy players from a number of other clubs. A's agent is an offshore corporate entity based in a low tax jurisdiction. The transaction involves secret pay back fees paid by the selling club to A's agent which are built into the price of the players paid by A. The commission paid to A's agent is paid onwards to a third party, which is an offshore entity controlled by A, and this commission equals A's original investment. A now owns the majority shareholding in a high value football club at no net cost to himself he has also laundered the original purchase price of the club.

In this example the sum of USD 1 million which circulates through a series of transactions may represent the proceeds of crime introduced into Sound Co. Equally it may represent the remuneration due from Sound Co to A and the transactions may simply be an effort to evade tax from foreign earnings.

Case 6 (fictional): returns from investment

A is a business man who owns a successful scrap metal business as well as a number of other business enterprises. A is involved in the purchase of stolen metal. A uses the money from his legitimate businesses to buy a lower league football club in his home town and introduces GBP 5 million of new capital. The club (controlled by A) expends GBP 4 million on improvements to its ground, new canteen facilities and new kit. Each of these are provided by companies controlled by A and are paid at an inflated price. Funds are channelled from these companies to an intermediary management company based offshore controlled by A.

A vests his shares in the club in the intermediary management company and moves that offshore. A channels cash from his criminal dealings in stolen scrap into the club through gate receipts and the canteen. This cash injection and the general revival in the clubs fortune causes a significant increase in the clubs profits which are then paid in dividends to the shareholders. The majority of the dividend payments go to the intermediary management company owned by A.

In this example A has recovered most of his original investment through the sale of services to the club, he retains a majority shareholding in a now profitable business and he has laundered the proceeds of his illegal scrap metal dealings through the club.

64. Cash received from ticket sales for football matches may be open to manipulation in order to launder funds by falsifying the books of a football club. A football club would however not be different from other cash-generating businesses outside the football area, such as restaurants, bars etc. Also in this case, the vulnerability may be higher for amateur clubs than for major league clubs. In major leagues, clubs

[14] Fictional cases are constructed to highlight the vulnerabilities in the sector and to provide guidance to law enforcement agencies, FIUs and the private sector.

have been required to implement, also for safety reasons, strict controls (through machines) on the number persons entering the stadiums. In some countries, the local federations agree to supply a very large number of tickets. Even though clubs state these are all sold, the federation does not check this. In reality there can be as many as 500 spectators less than full capacity, and money is laundered by buying the remaining seats. The increased presence of large denominations in the takings for the day may be an indicator of this practice as medium value notes are commonly used by the public when purchasing tickets.

65. It is important to obtain properly documented and corroborated information as to the identity, background, business and sources of wealth and funds of each club and its owners. It is therefore vital to understand who the real beneficial owners and controllers of a club are. This requirement is needed to preserve the independence of clubs but will also assist in the fight against money laundering.[15]

Case 7: Ownership of a football club

Italy has experienced an attempt to launder money through the purchase of a famous Italian football team. The investigations[16] to detect the case started from judicial proceedings in 2006. The *Procura della Repubblica* suspected that financial crimes were occurring, such as, money laundering, insider trading and misuse of market information..

Initially, a lot of rumours spread concerning a well-known Italian football team and intentions to purchase its shares on the capital market. Almost immediately after the purchase, the shares increased in value rapidly and strongly. At the same time, the judicial authorities started to investigate suspected threats made to the President of the concerned football team in order to convince him to sell the shares. Meanwhile, rumours around the purchase continued, including a public announcement by a European pharmaceuticals firm of a EUR 24 million investment, a purchase offer that was later denied.

Investigations uncovered evidence that the money used to buy the shares was supplied by a criminal association operating in Central Italy.

Further, a part of that money, supposedly offered to the football team as sponsorship, was then diverted to another company to purchase real estate, which was subsequently seized by Italian judicial authorities. Investigators identified that the criminal association was strongly interested in purchasing the football team with funds obtained from several offences.

As a result of these investigations, the criminal attempt to get hold of the football company failed. Proceedings for money laundering, insider trading, extortion, unfair competition and other offences are ongoing.

Source: Italy.

The transfer market and ownership of players

66. The increasing internationalisation of the market for football players has added to the vulnerability to money laundering.[17] At the Wold Cup of 2006 for the first time in history over half of the players in the best national teams of the world were playing in foreign football clubs.[18]

15 Arnaut, José Luis (2006), p.82

16 These investigations involved collaboration amongst several Italian public authorities: Guardia di Finanza, Digos, Consob (National Commission over listed companies and stock market), the Italian FIU, the Procura della Repubblica and other judicial authorities.

17 Internationalisation started in the 1930s when national teams were taking on players of other nationalities in order to reinforce their squads (*e.g.* Italy with Argentinian players for the World Cup in 1934), a practice which continued after that. At club level, there were also several examples of foreign players in major leagues: for instance, the Real Madrid in the 1950/60s had several foreign players (Santamaría from Uruguay, Puskas from Hungary, Di Stefano and Rial from Argentina, Kopa from France), and it was not the only club in this situation (for instance, Luis Suárez moved from Spain to Internazionale Milano in the 1960s). Cruijff and Neskeens (Netherlands) were playing in 1975 for Barcelona (Spain), which in the 1970s had already recruited Krankl (Austria) or Simonssen (Denmark); Real Madrid recruited the 1974 German world champions Breitner and Netzer

67. The worlds' best players, both from within and outside the EU, are contracted by the richest European leagues. On the supply side, Brazil has long been a big exporter of footballers not only to Europe but also to Asia. In the course of the last few years, Africa has emerged as a less expensive source of new talent. Talented players from the former European East Bloc also gravitate towards rich clubs elsewhere in the world.

68. The liberalisation of the TV markets and the expansion of private TV chains in Europe greatly contributed to the increase of budgets of clubs, the salaries of players and, consequently, the internationalisation of the market for football players. Tax factors played a role as well. In recent years, for a top club in the UK or Spain a foreign player (i.e. not resident in the UK or Spain at the moment of being recruited) was/still is in some cases less costly because of the different tax treatment for "temporary" residents.

69. The internationalisation of the labour market for football players was further helped by the Bosman ruling of 1995 when the European court of Justice decided on the free movement of players between member states. This revolutionised the rights of footballers and has contributed to the vast increase of salaries of top-players.

70. The transfer market is vulnerable to various forms of misuse, such as tax evasion, insider fraud and also money laundering.[19] Vulnerabilities are connected with lack of transparency in relation to the funding for certain transfer transactions and the opportunity for funds to be paid offshore with limited disclosure requirements regarding beneficial ownership of destination accounts.

71. Estimating the transaction price for a player is often unfeasible, since large amounts are involved, often carried out in one transaction or transferred abroad, making it difficult to verify their final destination. The over-evaluation of a player corresponds to a money laundering technique similar to the over-invoicing of goods and services seen in trade-based money laundering. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value.[20]

72. The football specificity is that the transfer of a football player (it would be more correct to say the termination of a contract with a previous employer – unless such contract has expired – and the subsequent signing up of a contract with a new employer) implies a compensation from the second employer to the

in the 1970s and later on Jensen (Denmark) and Stielike (Germany); Brasilians Leivinha and Luiz Pereira were playing for Atlético Madrid in the 1970s. British clubs started to recruit top foreign players only from 1978 onwards.

[18] Compared to 11.4% of the players of the participating national teams during the world tournament of 1978, 27.1% in 1990, 33.0% in 1994, 42.6% in 1998, 48.2% in 2002 and 53.1% in 2006. *Source*: Frick, B. (2009).

[19] For instance, in Spain (one of the four major leagues) the legal form of top football clubs is either an "association" (such as Barcelona or Real Madrid) or Sport limited liability company (such as Valencia or Sevilla). In both cases, profits/dividends may not be distributed by law. This means that if those controlling the club want to extract value from it, they need to do it through related-party transactions. The easiest way to divert funds for the direct benefit of directors would be through the transfer market.

[20] FATF (2006), p. 4.

first employer. Compensations may be high and largely increase the costs of transfers, therefore increasing the attractiveness of these transfers for illegal activities such as money laundering.[21]

Case 8: Acquisition of players

A football club with high debts in Latin American country Z signed a management contract with a collective investment fund, constituted in a tax haven, under which the investment fund pledges to allocate funds in order to cancel the society's debts and to share the results.
The club then acquired the player "Ito" from another local football club (Argentina) for USD 20 000 000. The football club based in country Z transferred the funds to an account that the selling club has in a third country. The funds never entered Argentina. Thus, little was known about the origin of the funds or the account into which they were deposited in the third country.

This typology was characterised by the following stages:

- Unknown (anonymous) investors willing to allocate funds.
- Collective Investment Funds constituted in tax heavens.
- Acquisition by collective investment funds of the management of football clubs with debts or in an irregular situation, in need of attracting investors.
- Allocation of funds for the acquisition of football players.
- Money transfers to the football club that acquires the football player, to accounts located abroad.

Warning Signs:

- Investor groups constituted in tax havens.
- Acquisition of management quotas of societies with large liabilities, compromising to cancel them and to share results.
- Football club based in developing countries that have offers of football players prized in millionaire sums.
- Football clubs receiving contributions through companies constituted in tax havens, where the real investors of such funds remain unknown.

Source: Argentina.

73. When ML occurs in the transfer market, football agents are often a focal point of these illegal transactions. In an increasingly complex legal environment, players (but also sport clubs) increasingly ask for the services of agents to negotiate and sign contracts. The international transfer market consists of over 4 000 football agents with an official FIFA registration. There are no limits to the role of agents. They manage their players but could also be managing the customer's funds (asset management consultancy), giving tax advice (tax consultant), offering an image contract or taking care of their publicity (advertising agents). Their position is crucial because they often determine whether a transfer happens or not (through their influence over a player and relationship with a club).

74. There are rules that cover this activity, yet some countries are more rigorous in applying them than others. For instance, to combat the non-transparency of the football agent sector, FIFA, as a private entity, has set strict guidelines for players' agents. According to these new regulations, which are private laws, players' agents should respect and adhere to the regulations, directives and decisions of the

[21] The current football transfer system is the result of historical development and contractual practice. The transfer system is not a necessary condition for the organisation of high level/good quality sport competitions, as shown by examples in other countries/sectors (see for instance the system in the USA concerning professional basketball, in particular the competition organised by the NBA). Therefore, one could imagine that, alongside monitoring the transfer system for possible abuses, structural measures could be put into place to reduce the attractiveness of this type of transfer for money laundering purposes.

competent bodies of FIFA, the federations and the associations, as well as the laws governing job placement applicable in the territory of the association (see also chapter 5).[22]

75. However, many agents still operate without license (players can for example also choose close relatives or lawyers as their agent) and are thus not controlled by the FIFA or any other continental or national football association. Agents (licensed and non-licensed) form a closed community, which makes it difficult to screen the transactions that are conducted by them. The stricter FIFA regulations can therefore not prevent money laundering or other irregular activities completely.[23]

Case 9: Unlicensed agent and money laundering

Following the receipt of STRs from banks, a European FIU studied the financial activity of an individual X and his company A which specialised in consulting and advising sports people. The apparent activity of the company, along with the particularly high amounts of various international wire transfers crediting the bank account of company A, individual X and his wife, all confirmed that X was clearly a players' agent, at the European level. Neither X nor his company A held the FIFA license required to negotiate players transfers, however. The financial flows observed on X's account and on his wife's and company's accounts actually characterise the illegal exercise of player's agent, which is punishable by one year imprisonment and a fine of EUR 15 000 by the law in the country in question. The players and clubs who used the services of this unlicensed agent had also breached the FIFA regulation.

Further analysis revealed that many international wire transfers crediting the bank account of company A originated from company B and from an individual Y. Y was a licensed agent from an Eastern European country and was known to be closely linked to the organised crime in his country. The wire transfers he ordered in favour of company A and of X may characterise money laundering operations. The organisation and the identity of the associates of company B were vague. Information collected by the FIU revealed that X and Y were managers of company B and were using it as a vehicle for laundering proceeds of crime. Regarding the ML aspects, first the proceeds derived from the illegal exercise of a regulated profession are themselves illegal and the use of them constitutes a ML offence. Second, many international wire transfers ordered by individual X may be considered as ML transactions, as X was known in his country to be closely linked to organised crime. There were also suspicions of corruption regarding player transfer activity in another European country. As X was involved in the management of company B which was also the origin of international wire transfers, this company may have been used as a way to disguise the origin of the transferred funds. The case was transmitted to the public prosecutor on the basis of a presumption of illegal exercise of the profession of players' agent and money laundering of illegal proceeds.

Source: France.

76. Another problem is raised by the multiple financial transactions that occur during the transfer process. Besides the transfer sum which is stated in the contract, there are transfer bounties and the additional costs that are made to attract a football player (house, car, financial arrangements for the family etcetera). All of these items can be used for the benefit of players but also by clubs, managers and agents. There are no fixed rules on how these transactions should be accounted for. The overall settlement of the transfer could therefore remain non-transparent and provide opportunities for money laundering.

77. A relatively recent development is the possibility of ownership of players (or rights in players) by individuals or entities that are not football clubs. These persons fall outside the direct jurisdiction of the football organisations. The ownership structures often involve companies in offshore jurisdictions with

[22] See: The Football Association 2008).

[23] Concerning the problems related to the activities of agents, an independent study on players' agents is currently being carried out on behalf of the European Commission by external contractors. The objective of this study is to analyse the situation regarding sports agents in the European Union and to identify the problems posed by their activities, as well as the solutions already provided by public and/or private stakeholders, in order to enable the European Commission to assess whether intervention is required. The study will address issues such as financial transparency and ethics in the conduit of players' agents. The results of the study should be made available by October 2009.

complex and often impenetrable ownership structures. A significant amount of money is generated as a result of player transactions that have resulted in significant sums being paid to such entities where they hold the ownership rights to certain players. Due to the limitations of the football organisations jurisdiction, the basis of the acquisition of these rights and the trading, funding and ownership position of the entities through which such transactions are managed is opaque and often impossible for the football organisations to establish.

78. Full legal ownership of players is particularly a South-American phenomenon. In Europe private investors sometimes collect funds through a closed talent pool. These talent pools are however no legal owners of a player, giving them only the right to (part of) the revenues when a player is sold to another club. Talent pools are often better options to actually get a return than through the investment in a football club as such. Talent pools could be misused for money laundering.

Case 10 (fictional): Talent pools

A club purchases a player for EUR 10 million but states in the official documents that it has purchased the player for EUR 5 million. The total amount of EUR 10 million is provided by the investors. These investors invest EUR 5 million in the talent pool and provide the club another EUR 5 million of the books which could be 'dirty' money. The player needs to improve himself and will later be sold to another club for a transfer sum of say EUR 15 million. Everyone who is involved in the deal will gain by the acquisition and sale of the player. The club can by the extra donation of EUR 5 million buy a better player. The investors can launder EUR 5 million and get a return on their investment. And the players' agent gains a good commission since his player is bought for EUR 10 million instead of EUR 5 million and is later on sold for EUR 15 million.

Betting activities

79. There is an ambiguous relationship between betting and sport. On the one hand, betting has historically been an important revenue source for sport in many countries. On the other hand, betting has also been associated with attempts to fix matches and alter the results of sporting competitions. Betting can be used both for the generation of illegal proceeds from game fixing and for pure money laundering purposes.

80. The FIFA Task Force "for the Good of the Game" has observed that "due to its particular structure, as well as the considerable need to finance the system at short notice, football offers a tempting platform for irregular betting activities. As the media and the public eye focus on fixtures in top competitions and top leagues, irregular betting activities can frequently be observed in less important fixtures (including lower divisions of domestic championships), where the environment can be manipulated more easily. Recent scandals in which betting has resulted in the manipulation of matches have brought the game into serious disrepute".

81. While problems linked to betting are not new, it appears that betting in sport has reached new levels of sophistication with various operators involved across several countries and continents and new offshore betting companies being established. Moreover, the use of the Internet for online betting further increases the risk of money laundering.

Case 11: SOGA I and II

Illegal soccer gambling is a serious problem in Asia. A recent Interpol operation, SOGA II, provides an idea of the scale of illegal soccer gambling in that region. Interpol announced that 1 300 people were arrested on the suspect of illegal soccer gambling and USD 16 million in cash were found during the operation (Interpol, 2008). 1 088 gambling dens were identified of which most were associated with organised crime. It is estimated that these dens handled bets which were worth nearly USD 1.5 billion. This is however not the first time Interpol has taken action in this area. In 2007 SOGA I resulted in 400 arrests, 272 illegal gambling dens and confiscation of USD 680 million worth of bets (Interpol, 2008). It is of course not said that the gambling sites are only used for money laundering. However, illegal soccer gambling is according to Interpol often related to money laundering.

Source: Interpol.

82. UEFA has called on the police organisation Europol to investigate possible match-fixing by Asian betting syndicates in top-flight European football. Meanwhile, Europol has recognised the danger emanating from corruption in sports. "The phenomenon of game fixing in organised sport is one of the areas that Europol has on the radar as a crime on the increase"[24].

83. However, illegal football gambling does not necessarily only involve Asian criminals. On the contrary, most of the Asian bookmakers are professional and well organised companies with a lot of expertise in the field. They do not deal with the gamblers directly, but only by means of a network of intermediaries. In other words, they do not know the individuals or organisations that are placing the bets. The problem is often situated elsewhere. International organisations or syndicates in Europe, for example, are trying to secure their investments in the Asian betting market by manipulating games through clubs, players or referees. Other parts of the world are also associated with match-fixing gambling scams. According to UEFA, there is an international network of organised crime behind certain European matches believed to have been fixed for betting reasons. Money traded on a single website can surpass EUR 100 000 for a third division football match. The UEFA however reports even higher stakes of EUR 1 million to EUR 2 million per match and stakes that can even increase for large tournaments.

84. Due to the fact that most countries have different gambling regulations, the gambling market is non-transparent and is a heterogeneous market with a mix of private and state companies acting both nationally and internationally. Providers are often established in countries which allow the organisation of gambling activities or in countries that do not regulate or supervise gambling. It is however not easy to take legal action against providers who offer their services online and are established abroad. This in combination with the non-transparency of the gambling market makes betting an interesting money laundering vehicle for criminals.

Case 12: Irregular betting

Several individuals regularly went to casinos in European country A to purchase chips for a substantial total amount. Analysis revealed that one of the individuals involved was a foreigner without any link to country A. The other individuals involved are either directly (players or coaches) or indirectly (relatives of players or coaches) linked to the world of football. There was no economic justification for the large amount of money used to purchase the chips. Police sources showed that the individuals were known in an investigation into rigged matches. The foreigner was suspected of bribing players before certain matches with money originating from betting activities linked to fixed matches. An online betting company established in a foreign country recorded exceptionally high bets for these matches. His aim was to invest in different clubs to control and corrupt them to play matches that were rigged beforehand. He mainly focused on clubs in financial trouble that were looking for "lifesaving" sponsors. The extraordinary scale of the betting or the unusual result of some matches (8-0) pointed to fraud. The money used to bribe players and to buy the chips could have originated from criminal activities of which the individuals were suspected.

Source: Belgium.

[24] World Sports Law Report (2007).

Image rights, sponsorship and advertising arrangements

85. Players with an excellent reputation and sometimes others as well get the chance of concluding so-called "image contracts" with companies that generally have their registered office abroad. These contracts take advantage of the "rights to the player's image" and are a tool to exploit personal appearances by the player as part of broad publicity campaigns but could represent vulnerabilities in respect to tax evasion and money laundering activities, even if the research for this report was unable to turn up any examples of proven cases.

86. The money due as stipulated in the contract is transferred to the company's account, often in a tax haven. This implies various risks: risk of fraud for the players with a very powerful image as they may be tempted to not declare part of the money received or be used as a "gatekeeper" for financial transactions in favour of a third party, and risk of money laundering for the players with an image that is not so powerful, they are used to launder money that is not related to their image. The player needs to be an accomplice in order to successfully complete these transactions.[25] Another scheme may be set up internally. When the club needs to "release" cash for some dubious use it will "officialise" this release under the pretext of paying for an image contract and then recover part of it.

87. Another possibility could be the use of fictitious image rights. In this scheme, payments for fictitious image rights are not remuneration for the use of the image rights of the player. In fact the payment is part of the football salary. The club pays a sum which does not make any connection with the actual value of the image rights or with the income to be earned. The players involved often have high football qualities, but a poor, even minimal exposure. Therefore afterwards, it emerges that the club has not or hardly made any commercial use of the rights. By disguising a part of the football salary as a payment for image rights the club and the player try to postpone or entirely cancel taxation in the same way as described above for the real proceeds of image rights.

88. Another risk area involves large money flows stemming from sponsorship and advertising arrangements. Part of professional football clubs' income depends on sponsors who invest in football for marketing reasons. If no check is done on sponsors' backgrounds, organised crime can use sponsoring as a gateway to legitimate business. By acquiring a certain dominant position within a professional sporting organisation the sponsor gains access to a corporate network.

89. Similarly issues concerning the relationship between the sports sector and sports media (television in particular) have become crucial as television rights are the primary source of income for professional sports in the large Western European countries. Conversely, sports media rights are a decisive source of content for many media operators. Sport has been a driving force behind the emergence of new media and interactive television services. There are no proven cases of dirty money going into football through media contracts however this remains an area of concern for football governing bodies.

Related illegal activities

90. Several cases show that the football sector is used as a vehicle for perpetrating criminal activities. Those criminal activities mainly refer to illicit trafficking in human beings, corruption, drugs trafficking (doping) and tax crime.

[25] SCPC (2003).

Illicit trafficking in human beings

91. Several cases linked to trafficking in human beings involve individuals directly or indirectly linked to the world of football. The problem of trafficking young players became apparent in many European countries at the beginning of the 1990s. Currently, population movements, mainly from African and Latin America, are becoming ever more significant and the circumstances surrounding the players' recruitment and accommodation are sometimes unclear. Dishonest agents set up networks that have led to a series of irregularities and have been involved in trafficking in human beings. Nowadays the football competition boasts many foreign players from African and Latin American countries but there are clear signs that this phenomenon is spreading to Eastern Europe and some Asian countries.

Case 13: Trafficking of players

Mr. LAN, an African citizen residing in his country of origin, had opened an account with a bank in Europe. An international transfer took place from this account. Part of the money had been transferred to an account of Mr. SMO, a European citizen. The latter immediately withdrew two thirds of the amount in cash. Mr. LAN's account also regularly received cash deposits. Analysis revealed that Mr. LAN acted as agent for international transfers of football players. Mr. LAN was not mentioned on any official list as a registered manager though. One of the individuals who held power of attorney on his account was a former football coach. Police sources showed that Mr. LAN was known to be involved in illicit trafficking of football players to which Mr. SMO was an accomplice. The transactions performed were probably linked to the commissions received for this trafficking. There was an amount of EUR 160 000 involved.

Source: Belgium.

Corruption

92. According to *Play the Game*, an organisation devoted to ethical values in sport, the rising incidence of corruption is due to the changing role of sport: its increasing commercialisation and the resultant increase in media coverage, advertising revenue and corporate sponsorship. Star athletes earn salaries comparable to top CEOs or stars in the entertainment industry, and major sport clubs deal in sums that rival many corporations. The mere presence of such money makes illicit behaviour attractive. Gambling encourages unethical conduct such as bribery of referees, officials or players to fix matches or influence league positions. The construction of sports facilities and the purchase of large amounts of equipment provide fertile fields for corruption in procurement. Where money flows, corruption often follows. Often seen are cases of match fixing to profit from betting or to affect league positions.

Case 14: Corruption and match fixing

The FIU of European country A sent information to the FIU of European country B regarding possible corruption related to football which was being investigated in country B. This information concerned Mr. PINO and Mr. FLY. Mr. PINO's assets of around EUR 1 million were divided over various accounts with a bank in this country. In a period of a few months, the account received several hundred thousand euros. Mr. FLY had also opened an account with this same bank. This account regularly received cash deposits. Analysis revealed that Mr. PINO was the chairman of a football club and was the subject of an investigation into corruption with respect to fixed matches. Mr. FLY was the lawyer of this football club. Mr. PINO and Mr. FLY held several accounts in country B and held power of attorney on accounts opened in the names of several companies. They carried out numerous cash deposits on various accounts totalling to several hundred thousand euros. Transfers between different company accounts were also performed, often involving use of transit accounts. The transactions carried out in country B and the assets abroad have been linked to offences that are currently under investigation.

Source: Belgium.

Drug trafficking – Doping

93. The issue of doping was very prominent in recent years due to several cases of doping products used by sportsmen. A broad range of products is available and, it is now extremely easy to buy forbidden

substances over the Internet. Organised crime has a clear influence on this type of trafficking. Indeed, it involves schemes akin to those used for drug trafficking.

Case 15: Doping

The company DIET, selling food supplements, had an account over which Mr. LATE held power of attorney. Following several changes to the articles of association, the activity on the company's account increased considerably. In a few months' time the credit transactions amounted to almost EUR 2 000 000. International transfers also began to take place on this account. Analysis revealed that the transactions were linked to a vet, Mr. HONY and represented invoice payments. The official activities of the company DIET did not justify why a vet was one of its customers. Mr. LATE and Mr. HONY were known to the police for trafficking of hormonal substances as part of a doping investigation in cycling and football. The transactions on the company DIET's account were linked to hormone trafficking.

Source: Belgium.

Tax evasion

94. Tax evasion and money laundering often use the same mechanisms. For example the money launderer may seek to conceal the proceeds of crime in corporate entities registered in regimes which have light financial regulation or strict banking secrecy laws. The tax evader will seek out the same secrecy jurisdictions. For a football club the channelling of money in a transfer deal through companies resident in low tax jurisdictions may be a method of laundering money, equally it may be tax evasion. And it is also likely that both offences may be present.[26]

95. The financial investigator faced with a complex series of transactions will have at some point to distinguish between money laundering and tax evasion as the objective. It follows also that co-operation, between financial investigators and tax authorities, is an essential part of the fight against both money laundering and tax evasion. Whilst tax evasion may be the predicate offence behind money laundering it is also likely that the objective of the suspicious activity is tax evasion. In the latter case recovering the proceeds of crime may be better effected by the application of tax powers and the recovery of tax, interest and civil penalties.

Case 16: Tax evasion through football agents

A disclosure was made by a player, revealing that his signing on fee was disguised as part of a fee to a foreign agent. He confirmed that the agent then paid him GBP 300 000 abroad and did not previously disclose this to the UK tax authorities. It is likely that the club concerned was fully aware that the payment to the agent included a signing-on fee for the player and the benefit to the club in such an arrangement is that it avoided Social Security contributions of GBP 38 000.

Source: United Kingdom.

96. The use of image rights is also used increasingly as a way of disguising remuneration. Image rights agreements have been used to disguise payments to agents. The amount of the image rights payment is inflated to account for payment made by the club to the agent. Once the image rights payment has been made to the offshore company, the agent will receive his entitlement, but without declaring the income for his services.

[26] There may be reasons other than money laundering or tax evasion for maintaining funds in "regimes which have light financial regulation or strict banking secrecy rules". Sometimes, it may be a problem of lack of confidence in the financial system of one's country, in the thoroughness of the country's supervisory systems or in the value of the currency (*e.g.* capital flight).

Case 17: Tax evasion through the use of image rights

A player (non-UK national) entered into an image rights agreement with a club. The player had transferred the rights to exploit his image exclusively on a world-wide basis to a company registered in a known tax haven in return for shares of that company. Unlike all the other players at the club, he was the only individual not to have either a signing on fee or a loyalty bonus and appearance fees. The club had not exploited the player's image in any way and after 2 years had sought professional advice, only to be advised that the image had no commercially exploitable value. Nonetheless, the club renegotiated both the playing and image rights contracts after 3 years, increasing the level of payments in both. The club concerned conceded that the image rights agreement was part of the employment terms and paid over additional duties of GBP 938 688. Additional duties of GBP 404 480 were also to be paid over the future life of the image rights contract.

Source: United Kingdom.

97. In the examples above, the common feature is the payment of money outside the "home" jurisdiction, the effect being to conceal the ultimate destination of payments. Image rights are used to disguise the true character of the payments.

CHAPTER 5: OVERVIEW OF ANTI-MONEY LAUNDERING INITIATIVES

98. The fight against money laundering became one of the priorities of public policies about 20 years ago, when the States realised that the significant development of circuits reinvesting dirty money constitutes a real threat to social and economic framework of the world. More recently, various international and national actors started to express concerns on the integrity of the football sector, including money laundering.

International and national public authorities

European Union

99. The EU recently produced several documents in which economic and social values of sports in general including football are praised, connected with statements about action that has to be undertaken to combat crime including the fight against money laundering.

100. In 2006, a European independent football review launched by the UK presidency resulted in a report to the EU Commission.[27] The objective of this Independent Review was to consider certain concrete issues facing sport and to adopt a series of recommendations on how the EU institutions, the EU member states and the European football organisations could provide a comprehensive and robust legal framework for European sport in general and football in particular.

101. The European Parliament adopted in March 2007 a resolution on the future of professional football in Europe. In this resolution the Parliament asked the Council of the European Union to develop and adopt measures for the fight against the criminal activities that haunt professional football, including money laundering, illegal betting, doping and match fixing, and enforced prostitution on the sidelines of major football events.

102. In July 2007, the European Commission published the White Paper on Sport.[28] For the first time the Commission addressed sport-related issues in a comprehensive manner. Its overall objective is to give strategic orientation on the role of sport in Europe, to encourage debate on specific problems, to enhance the visibility of sport in EU policy-making and to raise public awareness of the needs and specificities of the sector. The White Paper recognises that corruption, money laundering and other forms of financial crime affect sport at the local, national and international levels. The White Paper proposes to tackle cross-border corruption problems at the European level and to monitor the implementation of the EU anti-money laundering legislation with regard to the sport sector. As part of the implementation of the Pierre de Coubertin Action Plan, a number of studies have been launched or are in preparation concerning the issues covered by this report. A study on sports agents should be completed by the end of 2009. The study will address problems posed by the activities of sports agents in Europe. Another study on internal market barriers to the financing of sport will be carried out in 2010. It will address, among other things, the issue of sports betting.

---

27 Arnaut (2006).

28 Commission of the European Communities (2007).

National public authorities

103. Some national authorities undertake their own initiatives to support greater financial transparency including the prevention of money laundering and tax evasion through football.

104. France has set up a Direction Nationale du Contrôle de Gestion (DNCG) controlling the finances of professional and amateur sporting clubs. DNCG is a voluntary body within the French federation of football consisting mainly of accountants and lawyers that warrants the "fairness in sports". It ensures the books are balanced for the sporting season. Even though DNCG ascertains the solvency of investors, by asking for guarantees on their personal assets, it has not the mandate to check the legal origin of funds. However, its members in their quality of professionals subject to the AML/CFT regime (accountants, lawyers) do have the legal obligation to report suspicious transactions to the French FIU. In addition, according to the financial and monetary code, the French FIU has the power to obtain information from the DNCG. It is worth to note that the French code of sports provides for each sport federation with a professional league to set up a DNCG, competent for both professional and amateur sector. As a result, there is a DNCG for the rugby, basketball, handball, etc.

105. Initiatives have also been undertaken by Italy which has set up COVISOC which is a surveillance commission responsible for the financial control of professional football clubs and depends on the Italian Football Federation. In Brazil, there is a voluntary working group on football clubs involving football organisations, the central bank, FIU, the police and judiciary authorities. This working group has to assess vulnerabilities to ML, propose solutions to the problem and obtain operational results. Since the mid-1990s, the Dutch tax authority has followed the policy of dealing with sports by way of concentration and co-ordination. All professional football clubs are handled by one unit: the National Specialist Unit of Professional Sports. Club management often consult about fiscal matters with the Unit.

Sports organisations

FIFA

106. According to FIFA, their organisation bears a special responsibility to safeguard the integrity and reputation of football worldwide. FIFA is striving to protect the image of football, and its own image, from harm as a result of immoral or unethical methods and practices. In this connection, the Code of Ethics was developed in 2004 and revised in 2006. This revision was prompted by a decision of the FIFA Congress made in Munich in June 2006, requiring the creation of a new and independent Ethics Committee to constitute FIFA's third judicial body.

107. In November 2005, FIFA established a special task force "For the Good of The Game", aimed to investigate and combat threats to integrity of football. The task force consisted of three separate working groups, one on Competitions, one on Political Matters and one on Financial Matters. This financial working group had to "discuss and propose possible solutions to problems involving corruption, ownership of more than one football club by a single individual or organisation, betting on football, money-laundering and the flow of money during player transfers, developments in the transfer market and players' agents".

108. It was the first time that FIFA officially referred to money laundering. As part of its efforts to safeguard the integrity of the game of football, FIFA set up the following measures based on the proposals from the Task Force.

Player transfer matching system

109. The transfer matching system is a web based system for data exchange operated by a legal entity owned by FIFA. Applicable to international transfers of professionals, the system is firstly a contract

matching system to ensure that all parties agree on the details of the transfer, secondly a contract validation system to ensure that the terms of a transfer are correct and thirdly a payment recording (settlement) system. The advantages are twofold: it facilitates transfers and shows where the money is coming from and going to, with the aim of making transfers more transparent[29]. The system will become the source for all international transfer certificates for professional players by September 2010[30], and in future it will become a clearing house (timeline to be determined).

FIFA Club Licensing Regulations

110. After UEFA had a positive experience with club licensing regulations, FIFA sought to implement a global licensing system, in collaboration with national associations and confederations. FIFA Club Licensing Regulations were thus drafted based on the *UEFA Club Licensing manual*. The principles were approved by the 57th FIFA Congress in May 2007.

111. The club licensing system has the following overall objectives: safeguarding the credibility and integrity of club competitions; improving the level of professionalism within the football family; ensuring sporting values in accordance with the principles of fair-play; ensuring safe and secure match environments and ensuring transparency in the finances, in the ownership and in the control of clubs.

Players' Agents Regulations

112. The most recent FIFA Players' Agents Regulations were approved by the FIFA Executive Committee on 30 October 2007 and came into force on 1 January 2008. The new features include licences for players' agents being renewable as opposed to having lifetime validity, with the aim of making sure that agents are up to date with the rulings that are in force. Disciplinary measures against agents with dishonest intentions have also been significantly strengthened, and players will also have to pay their agents themselves in order to increase the transparency of the various transactions. In concrete terms, agents will receive payment exclusively from the client who engages them.

Early warning system on betting activities (EWS)

113. The early warning system is an independent subsidiary of FIFA aimed at protecting football from match-fixing derived from sports betting by highlighting any irregularities which occur in betting on football at a sufficiently early stage. This preventative alert system was tested during the 2006 FIFA World Cup Germany™. It monitored all 302 events of the 2008 Olympic Games in Beijing on behalf of the IOC. The FIFA Congress decided at the end of May 2007 to institutionalise the system and will use it to monitor gambling activities related to qualifying and tournament matches for South Africa 2010.

---

[29] As part of a valid transfer, clubs will have to provide the following combination of details: counter club information; counter clubs association (ITC management); player name; type of transfer (permanent, loan); total transfer amount (plus solidarity and/or training compensation if any); transfer type (single-payments, instalments); club agent and commissions if any; player agent if any; payment details of source bank (from club) and destination bank (to club), amount and value date.

[30] From May 2008 to April 2009, 47 countries began the implementation of the system. Phase 1 (since May 2008): Belarus, Belgium, Brazil, Chile, China, Côte d'Ivoire, Greece, Hungary, Kenya, Mexico, the Netherlands, Norway, Paraguay, Poland, Portugal, Spain. Phase 2 (since November 2008): Argentina, Australia, Austria, Bulgaria, Cameroon, Canada, Colombia, Croatia, Czech Republic, Congo, France, Germany, Japan, Lithuania, Morocco, New Zealand, Nigeria, Peru, Puerto Rico, Romania, Russia, Slovakia, South Africa, South Korea, Switzerland, Trinidad & Tobago, Turkey, Ukraine, Uruguay and the United States.

114. The EWS has signed contracts with more than 400 bookmakers worldwide. These bookmakers report any suspicious betting behaviour to EWS. In the event of suspicious betting patterns, FIFA is immediately informed, in accordance with the established emergency plan. EWS offers its infrastructure and its know-how to FIFA member associations and is establishing a common database for all relevant information in relation to match-fixing.

Other measures

115. Concerning the protection of minors, FIFA increased training compensation for 12-15 year old players and introduced the control of academies. In addition FIFA Transfer Matching System will also have an effect on the protection of minors. Concerning the anti-doping policy, in January 2009, a new world anti-doping code and FIFA anti-doping regulations came into force. This includes individual case management, flexibility in sanctions and possible whereabouts for teams.

International Olympic Committee (IOC)

116. The IOC Ethics Commission, created in 1999, is charged with defining and updating a framework of ethical principles, including a Code of Ethics, based upon the values and principles enshrined in the Olympic Charter of which the Code forms an integral part. In addition, it investigates complaints raised in relation to the non-respect of such ethical principles, including breaches of the Code of Ethics and, if necessary, proposes sanctions to the IOC Executive Board.

117. On the question of resources, the IOC Code of Ethics provides that the use of the Olympic resources, namely the financial support given by the IOC, must be only for Olympic purposes, and that this must be clearly demonstrated in the accounts. Regarding the question of the risk to the integrity of the Olympic Games posed by irregular betting activities, the IOC decided to monitor all the betting activity on the 28 sports during the Olympic Games in Beijing. Furthermore, the IOC was in contact with Interpol during this period. Fortunately, during the Olympic Games in Beijing, no irregular activity was noticed. However, the IOC has decided to continue such monitoring of betting activities during future Olympic Games.

Union of European Football Associations (UEFA)

118. UEFA has become remarkably explicit in its concerns on money laundering through football and expressed its concerns that money laundered from various criminal activities is moving into football. In 2005 UEFA has asked the European Union to investigate the origins of some of the hundreds of millions of pounds coming into football due to growing fears that criminals may be using clubs as a vehicle for money laundering. UEFA also urged MEPs from the European parliament known as the "Friends of football" to ask the FATF to examine suspicious investments in the sport.

119. In June 2006 William Gaillard, UEFA's director of communications, stated that "there is no doubt European and Latin American football could be a channel for dirty money to be laundered in major economies. […] Dirty money hurts the game".

120. In a presentation given to Transparency International's conference in November 2006, Henri Roemer, an advisor to UEFA's Executive Committee, explained in more detail what makes football so vulnerable to organised criminal organisations, who amongst other things, use clubs to launder their money. Roemer also outlined a number of steps that football bodies can take with partners outside sport to

combat the problems. Roemer mentioned FATF as the first most appropriate institution to collaborate with.[31]

121. Concerning the betting and match-fixing issues, UEFA stated during a UEFA disciplinary workshop in January 2009 that "an increasing challenge for football comes from betting and possible match manipulation – an area endangering football's integrity". UEFA's determined response to the challenge posed is, among other things, the reinforcement of UEFA's disciplinary services by improving the UEFA fraud detection system, through the recruitment of additional staff, in particular with specific experience in criminal investigation and sports betting. UEFA is also co-operating with a number of specialist partners in monitoring betting on UEFA matches, and the systematic collection of live official data from UEFA matches will help the monitoring process in the future. UEFA's fraud detection policy provides for comprehensive investigation of any alleged cases, and disciplinary action will follow against offenders. An UEFA delegation met recently with the largest bookmakers in Asia to find a way of efficient reporting of irregular betting patterns related to European matches.

122. From the season 2009-2010, UEFA will run a Europe-wide Fraud Detection System including the monitoring of all European domestic top 2 division matches and national cup fixtures of all 53 national associations affiliated to UEFA. These national associations will be informed about irregular betting patterns for their matches and guided in the subsequent disciplinary proceedings.

123. A recent example of UEFA's initiative can be illustrated by the decision taken by the UEFA in April 2009 regarding a club from the former Yugoslav Republic of Macedonia. This club was banned from UEFA competitions for eight years for match-fixing. The UEFA Control and Disciplinary Body added that the club president and a player have also been banned for life as a result of the investigation. Charges were brought against the club due to reports of irregular betting patterns and statements from a number of witnesses.

Football Associations

124. In December 2007 English Football Association came up with an extensive guidance for football clubs "Money Laundering and The Proceeds of Crime Act"[32]. This document was prepared in response to requests from professional and semi-professional clubs for more guidance in this area. The document sought to provide clubs with an overview of the main UK legislation concerning money laundering and the proceeds of crime on legislation; to set out steps a club might take in the event of a suspicious transaction; and to summarise some preventative measures that clubs might take to protect themselves.

125. According to this guidance, there are many transactions that take place within football clubs which have the potential to involve money laundering, no matter how reputable the other party may be in the transaction. Consequently, clubs should ask themselves various questions when carrying out transactions, for example: "Do you know exactly whom you are dealing with?", "Have you properly identified and verified the persons that you are doing business with?", "Do you know how the purchaser/investor/trader/agent has found the funds to pay you?"

126. The guidance also highlights that the repressive anti-money laundering legislation is applicable to sporting clubs. At a preventive level, even though clubs are not directly subject to AML legislation, some of their activities fall within the scope of the law which applies to "relevant businesses" defined in the Regulations such as accountants, banks and solicitors, as well as other that carry out activities that clubs may be involved in such as accepting deposits, dealing in investments and dealing in goods of any

[31] Roemer, H. (2006).

[32] The Football Association (2008).

description (including for example player transactions) by way of business whenever a transaction involves accepting total payments of EUR 15 000 or more.

127. If a club has a "nominated officer", any disclosure should be made to him or her in the first instance. The nominated officer should in turn report to the FIU. If there is no "nominated officer" the disclosure should be made direct by to FIU by the person who has the information or by a member of the club's senior management (assuming that the information is passed onto them).

128. To guard against the risks associated with potential money laundering or the handling of the proceeds of crime, clubs should review their existing systems and procedures and, where appropriate, consider implementing various measures. These measures include:

- Appointing somebody within the club's senior management to be responsible for money laundering issues.
- Making staff aware of the money laundering legislation and training staff that may be involved in transactions that could involve money laundering.
- Ensuring that there are internal controls on your business transactions so that only employees with the appropriate authority can bind the club.
- Ensuring that up to date and accurate records are kept of all business transactions, especially those that may involve money laundering.
- Ensuring that the identity is known of those that the club is dealing with and carry out appropriate enquiries before entering into transactions with them.
- Monitoring customer activity so that if it changes you can evaluate why it may have changed (for example, a customer with a history of making payment through the electronic banking system suddenly starts paying in large sums of cash); and reporting any suspicious activity.

129. The FA works closely with law enforcement authorities. Since 2007, the FA has also set in place a monitoring team which oversees and scrutinises the player transfer market and payments to football agents. One of the mechanisms that allows the FA to undertake this work is the "clearing house" function that the FA operates, whereby all monies paid by English clubs to overseas clubs in respect of player transfers and all monies paid by English clubs to agents must be processed through the FA's dedicated bank account.

CHAPTER 6: POLICY IMPLICATIONS

130. This study of typologies aims to help identify the weaknesses or loopholes in the prevention systems currently in place and may lead to the setting up or development of measures to protect the sector from money laundering linked to criminal activities, thus avoiding its becoming an attractive destination for money obtained from criminal sources.

Key findings

131. Criminals have shown adaptability in finding new channels to launder the proceeds of their illegal activities and there are concerns that various legitimate sectors are at danger of being misused for money laundering.

132. With the growing economic importance of sports during the last two decades, including the increasing profits that can be made out of sports, money gradually started to exert a strong influence on the world of sports. The influx of big money into sports has positive effects, but there are negative consequences. There is a higher risk of fraud and corruption given the amount of money at stake. Sport also can be used as a channel to launder dirty money.

133. As the biggest, truly global, high value sport, football seems to be confronted with various forms of crime and corruption - including money laundering. Football has undergone an accentuated growth and commercialisation since the early 1990's. The influx of big money, in combination with some specific factors has made football one of the many sectors that can be attractive for criminals to launder proceeds of crime.

134. The report identifies three areas of vulnerabilities.

135. The first area relates to the structure of the sector: the market is easy to penetrate, there is a multitude of stakeholders and money flows, different types of legal entities are at stake and management of clubs often lacks professionalism.

136. The second area of vulnerabilities regards the sector's finance. Clubs have large financial needs and considerable sums are often involved, especially in the international transfer market, often with an apparently irrational character, whereas control of origins or destination of payments is weak or even absent.

137. The third area relates to the sector's culture: a certain social vulnerability of some players (in particular younger players) making them vulnerable, the societal role of football making people reluctant to shatter sports' illusion of innocence and finally the opportunity for acquiring social status in the local community and gain entry to the establishment. A complex of financial and non-financial motives could make investments in football attractive for criminals seeking legitimate social status.

138. After analysis, money laundering through the football sector is revealed to be more complex than originally understood.

139. There are cases that illustrate the use of the football sector as a vehicle for laundering the proceeds of criminal activities. A variety of money flows involving various financial transactions increase the risk of money laundering through football. These are related to the ownership of football clubs or players, the transfer market and betting activities. Other cases show that the football sector is used as a vehicle for perpetrating criminal activities, and thus creating dirty money. Those criminal activities mainly refer to illicit trafficking in human beings, corruption, drug trafficking (doping) and tax crime.

140. The money laundering techniques used vary from very basic to complex and sophisticated techniques, including the use of cash, cross border transfers, tax havens, front companies, PEP's and the misuse of non-financial professionals.

141. Connections with other well-known money laundering typologies were identified such as trade-based money laundering, the use of non-financial professionals and NPOs for money laundering purposes, money laundering through the security sector, the real estate sector and the gaming sector.

142. Concerning this last point, it appears that betting in sport has reached new levels of sophistication with various operators involved across several countries and continents and new offshore betting companies being established. The use of the Internet for online betting further also increases the risk of money laundering.

143. Various initiatives are taken by international and national actors in order to combat threats to the integrity of football, including money laundering, in particular with the aim to control the ownership of clubs; to obtain information related to player transfers; to improve the situation surrounding players' agents and to combat illicit betting activities.

Issues for consideration

144. Looking ahead, there appear to be a number of areas that could be considered to improve the capacity to cope with the money laundering risks associated to the football sector.

145. **Building a better awareness**: while criminals use creative schemes to exploit the football sector, lack of awareness of money laundering risks associated to football could contribute to the problem. Very often there is a lack of awareness amongst some key players about their responsibility in the process of fighting illicit activities. Creating an understanding of the money laundering risks associated to the football sector amongst government bodies and the private sector, including financial institutions, is critical. Awareness-raising may prove to be very useful. This would require resources for outreach, training or other cooperative activities, but may result in enhanced information exchange.

146. **Imposing good governance and improving financial transparency:** With the growth in the number of international transfers and the increase in the sums of money paid per transfer, there are more managers and more intermediaries involved, including new parties of dubious background. Promoting healthy financial management is therefore crucial. One could imagine that, alongside monitoring the transfer system for possible abuses, structural measures could be taken to reduce the attractiveness of the transfer system to money laundering.

147. **Exploring industry best practices**: Some countries mentioned reporting obligations of money laundering to the national FIUs. In most cases there are no such obligations for football clubs. The adoption by the football sector of a code of best practices, such as the British football association guidance, could be helpful.

148. **Cooperation with the private sector**: various initiatives are taken by sports organisations (FIFA, UEFA, IOC) in order to safeguard the integrity of football and achieve the greatest possible degree

of transparency. To be successful, these measures could be developed further in cooperation with the FATF.

149. **Imposing similar regulations**: Given the international character of football, it is important to impose similar regulations to avoid choosing countries with the poorest regulations. In this context, there is a need to recognise the sporting industry as a robust industry (requiring financial transparency, proper external accounts, adequate financial management, and an effective regulatory framework).

150. **International co-operation is a key factor**: Difficulties in international exchange of information and the use of tax havens are a major stumbling block in the detection and prosecution of money laundering through the football sector. International co-operation and information sharing are key factors in the fight against money laundering given the international dimension of the football sector. Countries need to work cooperatively to identify and combat the use of the football sector for money laundering purposes.

151. **Internet gambling.** There is a risk associated with internet gambling related to sports in general. This issue could be investigated in a separate FATF typology study.

REFERENCES

- Arnaut, J.L. (2006), *Independent Review of European Sport 2006*.
- Assemblée Nationale française (2007), *Rapport d'information n° 3741 de M. Dominique Juillot déposé en application de l'article 145 du Règlement par la Commission des affaires culturelles, familiales et sociales sur les conditions de transfert des joueurs professionnels de football et le rôle des agents sportifs*, Assemblée Nationale française, Paris.
- Belgian Senate (2002), *Rapport concernant la traite des êtres humains dans le sport*, session 2001-2002, 2-1132/1, Belgian Senate, Brussels.
- Belgian Senate (2005), *Rapport concernant la problématique du dopage dans le sport*, session 2004-2005, 3-366/1, Belgian Senate, Brussels.
- Commission of the European Communities (2008), *Report from the EU Sport Forum* organised by the European Commission in Biarritz on 26-27 November 2008, Brussels.
- Commission of the European Communities (2007), *White Paper on Sport*, COM(2007) 391 final, Brussels.
- Dimitrov, D., C. Helmenstein, A. Kleissner, B. Moser, and J. Schindler (2006), *Die makroökonomischen Effekte des Sports in Europa*, Studie im Auftrag des Bundeskanzleramts, Sektion Sport, Vienna.
- Deloitte (2008), *Annual Review of Football and Finance*, Deloitte.
- *The Economist*, www.economist.com, research tools, economics a-z.
- European Parliament (2007), *Report on the future of professional football in Europe* (2006/2130(INI)), Committee on Culture and Education, European Parliament.
- FATF (2002), *FATF Report on Money Laundering Typologies 2001-2002*, FATF, Paris.
- FATF (2006), *FATF Report on trade-based money laundering*, FATF, Paris.
- FIFA Task Force Report (2005), *For the Good of the Game*, FIFA, Zürich.
- Frick, B. (2009), "Globalization and Factor Mobility, The Impact of the 'Bosman Ruling' on Player Migration in Professional Soccer", *Journal of Sports Economics*, Volume 10, Number 1, Sage Publications, Thousand Oaks, CA, pp. 80-106.
- Glenny, M. (2008), *McMaffia*, The Bodley Head Ltd, London.
- Hill, D. (2008), *The Fix*, McClelland & Stewart, Toronto.

- Johnson, G. (2006), *Football and Gangsters*, Mainstream Publishing, Edinburgh.
- KPMG (2004), "Preventieve doorlichting bedrijfstak betaald voetbal", *Fair play op en rond het veld*, KPMG Integrity & Investigation Services 2004, KPMG, Netherlands.
- Robert, D. (2006), *Le milieu du terrain*, Editions Les Arènes, Paris.
- Roemer, H. (2006), contribution to the workshop "The business of sport and corruption" at the 12th International Anti-Corruption Conference, Guatemala City, 17 November 2006.
- Rosen, S. (1981), "Economics of Superstars", *The American Economic Review*, Vol. 71, No. 5, American Economic Association, Pittsburgh, pp. 845-858
- SCPC [Service central de la prévention de la corruption] (2003), *Rapport du Service central de la prévention de la corruption 2003*, Ministère de la Justice – SCPC, Paris.
- The Football Association (2008), *Money Laundering and the Proceeds of Crime Act: Guidance for Football Clubs*, The Football Association, London.
- World Sports Law Report (2007), http://e-comlaw.com/wslr/index.asp, issue 12, Cecile Park Publishing Ltd, London

ANNEX – FATF QUESTIONNAIRE

1. Do you consider the football sector in your country to be vulnerable to money laundering? If yes, please describe the vulnerabilities?

2. Do you have cases of the misuse of football clubs and their networks to launder the proceeds of crime (such as money laundering through player transfers, investment of illegal funds in clubs, gambling on football competition, through sponsorship, talent pools, business clubs)? If yes, describe these cases in as much detail as possible and provide information on the persons or networks involved.

3. Football clubs and their networks can also serve as a vehicle for perpetrating illegal activities such as fraud, corruption, bribery, illegal gambling. Sporting clubs can therefore also be seen as a source of 'dirty money'. Do you have any cases illustrating this kind of illegal activity? If yes, please describe the schemes used.

4. By which means money laundering cases through football clubs have been detected (*i.e.* STRs, police investigations, newspapers)? If any, please provide the number of STRs relating to football and sporting clubs.

5. Please provide an estimate of the amount of money laundering in each of the case you have described. Do you consider the cases illustrative (common) or exceptional (uncommon) for laundering the proceeds of crime through football?

6. Please give a substantiated estimate of the overall size of money laundering through football in your country (in absolute numbers or related to the overall money laundering problem or compared to other money laundering schemes)?

7. Do individual clubs, football associations, federations or public authorities take measures to prevent money laundering and other illegal activities (see question 3) through football, including on the basis of international measures? If yes, describe these measures and if possible, provide the text of these measures. What kind of measures could be useful to prevent money laundering through football?

8. Which other sporting activities are notably vulnerable to money laundering in your country? Please describe some typical money laundering schemes through sporting activities other than football. Give a substantiated estimate of the overall size of these money laundering schemes.

FATF/OECD
July 2009

www.fatf-gafi.org

Appendix NN:

FATF, *Proliferation on Financing Report* (Paris: FATF, 2008).

Financial Action Task Force

Groupe d'action financière

PROLIFERATION FINANCING REPORT

18 June 2008

TABLE OF CONTENTS

INTRODUCTION

1. The Proliferation Finance Typology Project develops an understanding of the issues surrounding proliferation financing and provides information that can be used by the FATF to assess the need for policy measures to counter proliferation financing.

2. Pursuant to the FATF's Guidance of 29 June 2007, "Further study of broad-based measures to combat WMD proliferation finance under United Nations Security Council Resolution 1540 (2004) "S/RES/1540 (2004)", the project identifies and analyses the existing threat of proliferation financing; examines existing measures used to counter this threat; and outlines a series of options that could be considered by the FATF to counter proliferation financing, within the framework of existing S/RES/1540 (2004) and S/RES/1673 (2006).

There are financial provisions within paragraphs 2 and 3(d) of S/RES/1540 (2004)'s mandatory Chapter VII obligations that merit further examination by the FATF.

> *2. Decides also that all States, in accordance with their national procedures, shall adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them;*
>
> *3. Decides also that all States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall:*
>
> *(d) Establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services relate to such export and trans-shipment such as financing, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations;*

S/RES/1540 (2004) defines a non-state actor as an "*individual or entity, not acting under the lawful authority of any State in conducting activities which come within the scope of this resolution.*"

S/RES/1673 (2006) reiterates the requirements of S/RES/1540 (2004) and emphasizes the importance for all jurisdictions to implement fully that resolution, including provisions regarding the financing of WMD proliferation.

The FATF, while taking into consideration the work of the United Nations 1540 Committee, will conduct further study to:
(a) identify the threat of the financing of WMD proliferation;
(b) analyse the effectiveness of existing measures to counter the threat of the financing of WMD proliferation, and
(c) identify measures (*e.g.* criminalisation measures, broader sanctions, activity-based financial prohibitions or controls or examining the use of financial intelligence) that could be considered in combating WMD proliferation finance within the framework of existing UNSCRs, such as S/RES/1540 (2004).

3. This report has incorporated, *inter alia*, the following into its analysis: 1) jurisdictions' responses to the Proliferation Financing Questionnaire; and 2) the findings of the November 2007 Joint FATF / APG Experts' Meeting on Money Laundering and Terrorist Financing Typologies. The report has also benefited from the discussions that took place at the May (Ottawa) and September (Rome) 2007 WGTM Intersessional Meetings. The Project Team[1] has had opportunities to discuss proliferation financing issues with some representatives of the private sector. Private sector representatives participated at the November 2007 Joint FATF / APG Experts' Proliferation Financing Workshop. The issue of proliferation financing was also discussed at the December 2007 FATF – Private Sector Expert's Meeting on Typologies.

1. ASSESSING THE THREAT OF PROLIFERATION FINANCING

4. The threat of proliferation is significant and the consequences are severe. Proliferation has many guises but ultimately involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programmes, including delivery systems; it poses a significant threat to global security. If appropriate safeguards are not established, maintained and enforced for sensitive materials, technology, services and expertise, they can become accessible to individuals and entities seeking to profit from the acquisition and resale, or for intended use in WMD programmes.

5. They can also find their way into the hands of terrorists willing to employ WMD in acts of terrorism. There is evidence that terrorist organisations continue to pursue chemical, biological, radiological or nuclear (CBRN) capabilities, and it is worrying that their efforts are increasing.[2] In such circumstances, terrorism financing as it relates to providing financial support to terrorist organisations that endeavour to acquire and/or deploy CBRN weapons is then by its nature also contributing to proliferation.

6. Proliferation financing is an element for the movement of proliferation-sensitive items and as such, contributes to global instability and potential catastrophic loss of life if WMD are developed and deployed. Similar to international criminal networks, proliferation support networks are using the international financial system to carry out transactions and business deals.

7. This paper does not seek to define proliferation or proliferation financing. In considering the challenges posed by proliferation financing, this report has looked at issues wider than those set out in S/RES/1540 (2004), strictly defined. The following is a broad working definition of proliferation and proliferation financing for this report only.

> *Proliferation is the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials.*
> *This could include, inter alia, technology, goods, software, services or expertise.*
>
> S/RES/1540 (2004) further defines the following:
>
> *Means of delivery: missiles, rockets and other unmanned systems capable of delivering nuclear, chemical, or biological weapons that are specially designed for such use.*
>
> *Related materials: materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for*

[1] The following FATF delegations participated as members of the Project Team: Belgium; Canada; Denmark; France; Germany; Hong Kong, China; Italy; The Netherlands; Switzerland; United Kingdom; United Nations and United States.

[2] *www.cia.gov/library/reports/general-reports-1/CBRN_threat_wo.pdf*
www.csis-scrs.gc.ca/pblctns/prspctvs/200110-eng.asp

the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery.
Proliferation financing is providing financial services for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials.

It involves, in particular, the financing of trade in proliferation sensitive goods, but could also include other financial support to individuals or entities engaged in proliferation.

For the purpose of this report, no distinction is made between witting and unwitting actors.

8. The proliferation challenge faced by governments includes the direct technology transfers by governments through nuclear, chemical, biological and missile cooperation or espionage into clandestine efforts to build and acquire WMD capabilities. While there can be legal or other restrictions on information sharing given the sensitive nature of proliferation investigations and intelligence gathering, the report does identify a number of proliferation financing cases. Determining, for example, that a high, medium or low number or value of international financial transactions are facilitating proliferation may be impractical, however, the cases identified in the report show several instances where the international financial system has been used to facilitate proliferation. While it is fact that financial institutions were involved in these transactions it does not per se indicate that they should have been in a position to detect the true nature of the transaction and prevent it.

9. Governments have established numerous multilateral arrangements to detect and prohibit proliferation including the Nuclear Non-Proliferation Treaty[3]; however, as indicated later on in the report, traditional arrangements have not focused on proliferation financing. The detection of even a few proliferation related cases should raise concern, in particular, given the consequences that the use of or threat of using a biological, chemical, radiological or nuclear weapon can have on the international community, including the international financial system.

10. Governments have worked to establish and maintain extensive export controls and safeguards to prevent the acquisition of the required goods, services, technology and expertise by proliferators or their supporters. These controls, including safeguards such as the registration, licensing and pre-approvals for the manufacture and export of a broad range of designated goods, are fundamental in preventing proliferators from acquiring important goods, services, technologies and expertise. However, these controls are not uniform across jurisdictions, and some jurisdictions have yet to implement the requirements mentioned in several international treaties to detect and restrict trade in proliferation sensitive goods and items.

11. In addition, trade globalisation and steady advances in technology are providing fresh challenges for the maintenance of effective export controls. Trade volumes continue to rise and trade patterns are less discernable. Further, there is a growing range of goods and technology that have commercial applications as well as applications for WMD and WMD delivery systems (*i.e.* "dual-use" goods), and while proliferators previously attempted to buy or sell whole manufactured systems with the effective control systems, there is a growing trend to purchase or sell more elementary components. Proliferation networks continuously seek out and exploit weaknesses in the global export control system and international financial system.

12. Export controls are used to *inter alia* prevent dual-use and other sensitive goods (listed and unlisted) from being exported to known individuals and entities that are involved in WMD proliferation-related activities. However, it is challenging for authorities to designate and monitor trade in all relevant "dual-use" goods.

[3] The full range of multilateral arrangements is described in some detail in Annex 4.

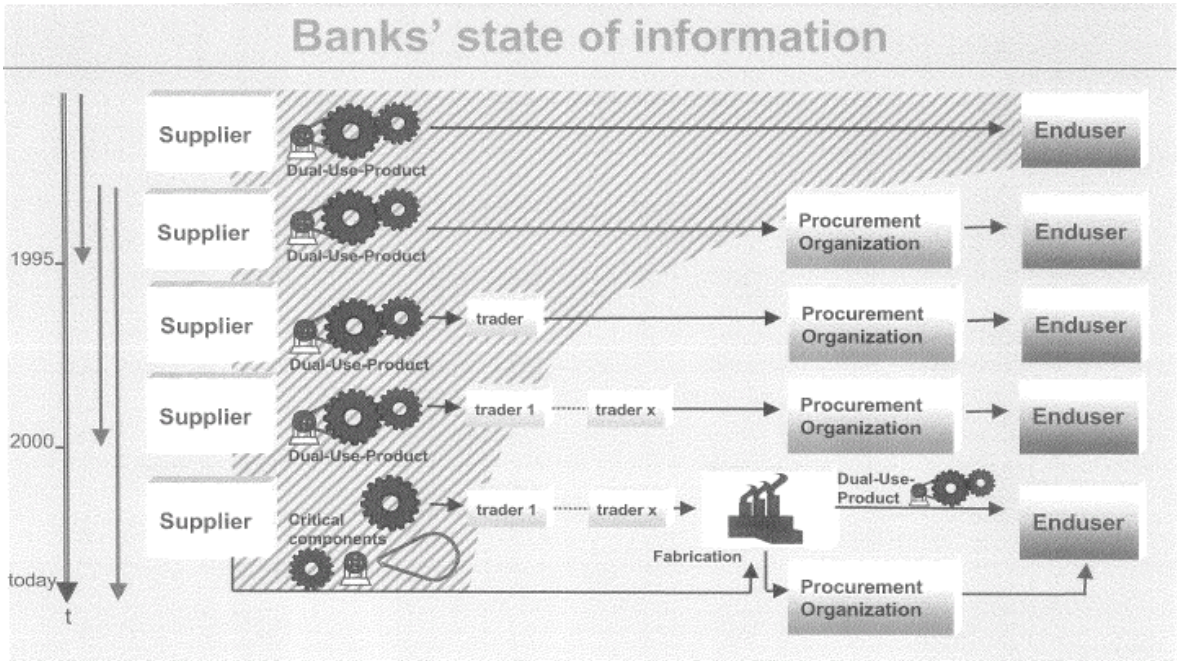
13. Governments are continuously working to further develop these controls while proliferation networks, individuals, entities and countries of concern continue to adapt, using front companies, illicit brokers and illicit means to obtain goods, services, technology and expertise.

14. The multilateral financial prohibitions contained in S/RES/1540 (2004)[4] introduce an additional tool that complement existing counter-proliferation regimes. The diagrams in Annex 2 demonstrate the growing complexity of the procurement process. One or two decades ago financial institutions were in a better position to collect and scrutinise information regarding the ultimate end–use of potentially sensitive proliferation items. However, procurement networks have become more complex over time, increasing: *i)* the number of actors involved; *ii)* the trade in sub-components; and *iii)* the indisputable probability that the true end-users of proliferation sensitive goods will avoid detection. This implies, *inter alia*, the acquisition of technology with the aim of shifting the production capacity to their own country or to generally unwitting production facilities in other countries.

15. With changes to the procurement process and a significant increase in the number of normally innocuous items that now have potential proliferation sensitive applications, it has become far more difficult to assess with a sufficient degree of certainty whether an item will truly be used for civilian purposes. While information that is potentially held by intelligence services has not changed significantly, information held by other entities, including suppliers and financial institutions is greatly diminished. For example, it is common today for suppliers to only have information on intermediary players in the procurement chain. Suppliers deliver dual use products and other critical items that are often not subject to export controls, to traders, brokers and other entities responsible for forwarding on the items as inputs to other facilities where proliferation sensitive goods are then produced.

16. Today, financial institutions have far less information about end-users and ultimate end-uses of items underlying financial transactions. Apart from information that is collected concerning their clients, information in transactions that describe items is generally too vague and/or would require a significant amount of technical knowledge to determine if they were sensitive or not.

17. The following diagram shows the information that is usually available to financial institutions.[5]



Source: Germanv.

4 And subsequently S/RES/1718(2006), S/RES/1737(2006) and S/RES/1747(2007).

5 See Annex 2 for further detail.

The scope of proliferation financing

18. Defining the scope of proliferation and proliferation financing for the purposes of this report is both critical and challenging. The report seeks to present the types of proliferation activities that often involve proliferation financing.

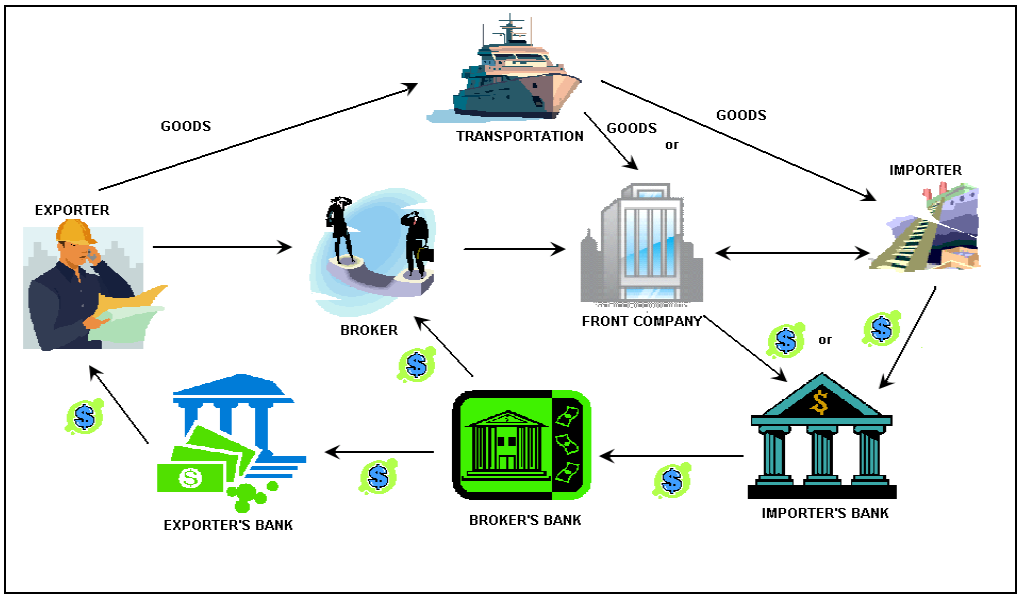
19. Proliferation networks operate globally. Advances in economic integration and in the volume and speed of international travel and trade, facilitate the global transfer of sensitive items by proliferators. Proliferators mask their acquisitions as legitimate trade. They exploit global commerce *e.g.* by operating in countries with high volumes of international trade or utilising free-trade zones, where their illicit procurements and shipments are more likely to escape scrutiny. However, in reaction to this phenomenon, jurisdictions with a highly developed and efficient export control system make enhanced efforts to control these transactions.

20. The following diagram illustrates a basic foreign trade pattern which is routinely used in export financing. Proliferators may abuse this typical trade pattern to disguise their real intentions. It is a starting point for subsequent illustrations and cases that provide a more dynamic snapshot of individuals, entities, products, and documents proliferators may use and exploit, as well as the financing mechanisms they use to facilitate their trade.

OVERVIEW OF A FOREIGN TRADE PATTERN ABUSED FOR PROLIFERATION

An importer may arrange for the shipment of goods directly with an exporter or could use a front company, broker or both a front company and a broker.

Similarly, payments may be settled with a manufacturer's bank either: directly; using a Front Company; using a Broker; or the manufacturer may arrange for payment using Letter of Credit or other payment method.



Source: Canada.

21. Proliferators rely on support structures[6] that exploit a number of channels to facilitate the purchase, sale, export or import of sensitive goods. As with most illicit trafficking, proliferation networks work to conceal the end-user of traded goods, the goods themselves as well as the entities involved and associated financial transactions.

6 More information provided in the section "Witting and Unwitting Actors".

22. To ensure that authorities do not detect the real end-use of sensitive goods being exported, networks may use intermediaries and front companies to arrange for the trade and export of goods by witting or unwitting companies. However, the use of intermediaries is not in itself an indication for proliferation financing. Exporters employ intermediaries for legitimate purposes. When exporting out of or through jurisdictions with well-developed export control regimes, intermediaries and front companies may use fraudulent documents, such as false end-use certificates, forged export and re-export certificates. Couriers or other facilitators may be used to ensure that the transfer of goods, in particular at main transit points, avoids inspection to ensure safe entry of the goods by land, sea, or air.

Activities relevant to this report

23. Weapons of mass destruction proliferation, including the transfer of complete systems or the transfer of components; dual-use goods, services, technology, expertise and training, that could be used to develop weapons or delivery capability is the primary focus of this report. The theft of high value materials from authorised storage facilities with the intention of resale should also be considered a proliferation-relevant activity.

Dual-use goods

24. Proliferators purchase dual-use items, many of which are controlled under international export control regimes. In contrast to trafficking in nuclear or radiological material, these purchases are mostly settled using a range of financial transactions, normally through the formal financial sector.

25. Dual-use goods are items that have both commercial and military or proliferation applications. This can include goods that are components of a weapon, or those that would be used in the manufacture of a weapon (*e.g.* certain machine tools that are used for repairing automobiles can also be used to manufacture certain component parts of missiles).

26. Export control systems are continuously updated and expanded to incorporate new goods and technologies. This has forced proliferators in some cases to adopt a different strategy to select, where feasible, elementary components rather than complete subassemblies[7] to elude authorities. However, a high level of technical expertise is often required to integrate various elementary goods into a full assembly, and as such, proliferation networks may continue to attempt to illegally purchase subassemblies or complete systems. They may even attempt to acquire the manufacturing company.

27. Dual-use goods destined for proliferation use are difficult to identify even when detailed information on a particular good is available. Regardless of the amount of information provided for a particular good, highly specialised knowledge and experience is often needed to determine if a good may be used for proliferation. The table below includes a small subset of the kinds of items – with only minimal information – that are often classified as dual-use by jurisdictions, it is by no means an exhaustive list of dual-use items, as national dual-use goods lists often contain hundreds of items, as well as the technology used to design, manufacture or use such items. Dual-use items can be described in common terms with many uses – such as "scrubbers" – or in very specific terms with more specific proliferation uses – such as metals with certain characteristics. Further, many of the goods listed in this table are only regarded as dual-use if they measure-up to very precise performance specifications.

[7] A subassembly is defined as a major subdivision of an assembly consisting of a package of parts, elements, and circuits that perform a specific function.

Table 1. Select examples of general dual-use items

Nuclear	*Chemical*	*Biological*	*Missile and delivery*
Centrifuges	Scrubbers	Bacterial strains	Accelerometers
High-speed cameras	Mixing vessels	Fermenters	Aluminium alloys
Composites	Centrifuges	Filters	Aluminium powders
Maraging steel	Elevators	Mills	Gyroscopes
Mass spectrometers	Condensers	Presses	Isostatic presses
Pulse generators	Connectors	Pumps	Composites
X-ray flash apparatus	Coolers	Spray dryers	Maraging steel
Pressure gauges	Precursors	Tanks	Homing devices
Ignition	Pumps	Growth media	Oxidants
Vacuum pumps	Reactors		Machine tools
	Heat exchanges		

Source: "Proliferation of weapons of mass destruction", Report from the Swedish Security Service.

Transhipment and diversion

28. Transhipment centres, commonly known as 'hubs' are cargo-sorting and redistribution destinations through which much international trade is routed. Examples of major international hubs include the Netherlands (Rotterdam), the UK (Felixstowe), Hong Kong, Singapore, and Malaysia (Port Klang). Free trade zones are destinations where goods pass through on route to their final destination. Free trade zones, while not always transhipment hubs, are sometimes used by exporters as the landing post for goods destined for end-users in nearby jurisdictions. Examples include the United Arab Emirates (Jebel Ali free port), Malta and Cyprus.

29. Routing goods through transhipment hubs offers a number of advantages to those seeking to facilitate international trade. It is common practice amongst cargo shippers and helps lower shipping costs by reducing the number of ship movements required. Although transhipment routes are often highly complex, with goods travelling through many hubs, they provide the opportunity to link up with other vessels going directly to the end-user destination and do not require specially charted ships to be commissioned or to travel empty – cutting the cost to the importer. Goods travelling through a hub may be small volume – single packages or containers. Many hubs, like free trade zones, have the additional advantage of being close to their eventual cargo destination.

30. For the procurer of illicit goods seeking to avoid detection, the advantages of Free Trade Zones and Transhipment Hubs are that less stringent export controls are often applied by states to goods being transhipped or routed through free trade zones than to goods entering their territory through other means. As goods do not officially enter the economy in question they may be beyond effective customs and police control. The final journey may be by smaller cargo vessel or it may be completed by land or air. Although certain destinations maintain accurate data for cargo passing through their ports for commercial reasons the constant rerouting of goods can make effective tracking of cargo difficult.

31. Diversion occurs when the supplier, broker or end-user deliberately tries to conceal the eventual destination of a particular shipment. For instance, when diverted goods pass through a third country, an individual in that country who is aware of the true destination of the goods seeks to establish himself as a false end-user. Entities or persons seeking to conceal the true end-user have the best chance of doing so by diverting or routing goods through third countries with weak (or non-existent) controls. Diversion points used by proliferators will often be ports where national shipping carriers call and where goods can be passed on to other cargo shippers on route to their final destination.

32. While transhipment and diversion make traditional counter-proliferation controls harder to enforce it can result in a financial intelligence trail for investigators and customs authorities to follow breaches of export control law. Financial flows required to move goods from one place to the next could provide authorities with supplementary information to link up entities of concern with transport routes and ultimate end-users.

Proliferators' use of the formal financial sector

33. Some elements of proliferation support networks may operate for financial gain and the formal financial sector can be abused by networks to carry out transactions and business dealings worldwide. Apart from transaction and business activities in the informal financial sector, proliferation financing can involve traditional trade finance products and transactions.

34. There have been incidences where proliferation-related transactions are settled through opaque cash or "barter-like" settlements involving goods such as oil, sensitive military goods or other proliferation sensitive goods. Cash may be used by proliferators to avoid detection by financial monitoring systems. Further, the cash used in payments may have been obtained through illegal activity. Cash payments for goods do not create financial (paper or electronic) trails and therefore do not contribute financial information that may be useful in identifying and combating proliferation activity.

35. However, it is important for proliferators to have access to the international financial system under most circumstances. Purchases must appear to be legitimate if proliferators are to elude suspicions and they often exploit commercial companies with legitimate businesses.

36. While there are cases where proliferators have exchanged suitcases of cash, this is not cost effective or efficient and is certainly suspicious. Companies being used unwittingly are aware of the sensitivities surrounding their products and are often required to exercise due diligence with purchasing parties. It would be quite suspicious, for example, if an individual tried to purchase a piece of machining equipment with cash.

37. International trade has well established instruments to facilitate imports and exports while mitigating business risks, including the general level of trust between parties engaged in a transaction. Trust is exploited by proliferators to ensure the minimum amount of scrutiny. Traditional trade financing contracts clearly define the specific terms of trade and ensure each party that the other will follow through on their end of the arrangement. The most common payment methods include open account payment, pre-payment, documents against payment and letters of credit. Trade can also be financed through more direct means via credit. These are discussed in more detail below.

38. Proliferation networks also use financial flows to pay intermediaries and suppliers outside the network. Similar to actors that supply proliferation networks, financial institutions are usually unwitting facilitators of proliferation, as a consequence of the complexity of dual-use goods, the involvement of illicit intermediaries, front companies and illegal trade brokers.

Survey results on disrupting and deterring proliferation and proliferation financing[8]

39. Some jurisdictions raised the following general risk factors which might make a jurisdiction vulnerable to proliferation financing, in response to the Proliferation Financing Questionnaire (the survey). The most significant risk factors include: laws or enforcement capacity, its size, openness, industrial make-up and volume of trade with respect to the economy and/or geography. Specific factors raised in the survey responses include:

[8] A survey was sent to all jurisdictions on 1 October 2007 and this report reflects the responses of 20 jurisdictions.

- Weak AML/CFT controls and/or weak regulation of the financial sector.
- Weak or non-existent export control regime and/or weak enforcement of existing export control regime.
- Non-party to relevant international conventions and treaties regarding the non-proliferation of weapons of mass destruction.
- Lack of implementation of relevant UNSCRs.
- The presence of industry that produces WMD components or dual-use goods.
- A relatively well-developed financial system or an open economy.
- The nature of the jurisdiction's export trade (volumes and geographical end-users).
- A financial sector that provides a high number of financial services in support of international trade.
- Geographic proximity, significant trade facilitation capacity (*e.g.* trade hub or free trade zone), or other factors causing a jurisdiction to be used frequently as a transshipment point from countries that manufacture dual-use goods to countries of proliferation concern.
- Movement of people and funds to or from high-risk countries can provide a convenient cover for activities related to proliferation financing.
- Lack of working coordination between the customs authority and the export licensing authority of a specific jurisdiction.
- A jurisdiction that has secondary markets for technology.

40. Most jurisdictions responded that any financial services related to international trade, including through products such as letters of credit, could be abused to finance trade in proliferation-sensitive goods. Financial institutions providing trade finance services are at risk of being abused for proliferation financing with financial services and products such as letters of credit (or documentary credits), loans and electronic funds transfers. It was noted that *hawala* and money remittance services and the insurance sector were at risk for proliferation financing and identified that proliferation networks may use cash couriers to finance proliferation.

41. A number of jurisdictions indicated that general risks, such as having a highly developed industry and financial sector, will increase vulnerabilities should no efficient export control system exist. When asked to assess the effectiveness of export controls in their own jurisdiction, respondents generally considered their system to be adequate.

2. WITTING AND UNWITTING ACTORS

42. Proliferators abuse typical trade structures to facilitate their activities, which include supporters, financiers, logistical support, front companies, assets, shippers and facilitators. Entities that are knowingly engaged in proliferation, such as a front company, may also be involved in legitimate business. Other actors used by a network may knowingly support proliferation, be "wilfully blind" that they are being used for illicit purposes, or are truly unwitting actors. When an entity is engaged in both legitimate and illicit trade it may be less likely for financial institutions to suspect illegal activity.

Front and Other Companies

43. In individual cases, proliferation networks have employed companies to conceal the true end-use or end-user of traded goods. Most front companies are sensitive to public exposure and disruption of legitimate activities.

44. Front companies established by proliferators conduct transactions similar to those of companies engaged in legitimate business. Front companies used by proliferators may be similar to those established by money launderers. As is the practice of other criminal organisations, proliferators create companies for a seemingly legitimate commercial purpose and commingle illegal funds with funds generated by legal commercial activity. In some cases, front companies established by proliferators do not engage in any legal activity at all. Front companies may use fraudulent accounting practices and establish various offshore entities in jurisdictions with lax controls to disguise illegal operations.[9] Proliferators are also known to change the names of front companies, or to use multiple names for the same front company, to prevent the detection of the companies' association with proliferation – or other illicit activity.

45. Front companies used by proliferators are often located in a major trading hub of a foreign jurisdiction with lax export controls but may also be found in jurisdictions with more established controls. They can be shell corporations with a fictitious business and physical location or can have normal commercial and industrial operations.

46. Front companies can arrange shipping services, routing or re-routing goods acquired by the importer or its intermediary. The same and/or additional companies can also be located in jurisdictions with weak financial controls, enabling related financial transactions to settle the underlying trade without detection.

47. In exceptional cases, front companies may seek complicity within a particular jurisdiction's government for signoff by national authorities, by production of false cargo manifests to misdirect customs, law enforcement, and intelligence as to the true nature of the goods being exported and their end-use.

Brokers

48. Brokers are involved in the negotiation or arrangement of transactions that may involve the transfer of items (often between 3rd countries) or who buy, sell or arrange the transfer of such items that are in their ownership. In addition they may also become involved in ancillary activities that facilitate the movement of items such as, but not limited to: *i)* providing insurance; *ii)* marketing; *iii)* financing; and *iv)* transportation / logistics. Illicit brokers illegally participate in proliferation by circumventing existing controls and obfuscating trade activities.

49. Brokers used by proliferation networks are often individuals relying on simple commercial structures, who are very mobile (financially and geographically) so that they can operate from any jurisdiction.

Other Intermediaries

50. Intermediaries may include companies and individuals that purchase or sell sensitive goods for further manufacture or redistribution. Intermediaries may have a particular knowledge of a jurisdiction's commercial infrastructure. Intermediaries that are knowingly engaged in proliferation will use this knowledge to exploit vulnerabilities in export control systems to the advantage of the proliferator.

Financial Institutions

51. Proliferation networks may use financial institutions to hold and transfer funds, settle trade and pay for services. Proliferation networks may use both private and public financial institutions for international transactions. States seeking to acquire WMDs may also use foreign branches and subsidiaries of state-owned banks for proliferation finance-related activities, giving these institutions

[9] FATF (2003), FATF (2006).

the responsibility of managing funds and making and receiving payments associated with proliferation-related procurement or other transactions. These subsidiaries may be engaged in both legitimate and illegitimate transactions.

Financial institution settlement of international trade transactions[10]

52. Financial institutions support international trade in three main ways:

- A financial institution's products and services are used to settle international trade transactions. These products and services range from payment transfers[11] from the importer to the exporter to more sophisticated financial products, such as a letters of credit[12], documentary collections and guarantees.
- The financial sector provides export finance to bridge the time between the need of funds for production, transportation etc. and the payment for such products by the importer. Banks and other export credit agencies provide loans and credit to traders to enable them to purchase and resale goods or equipment.
- The financial sector may provide insurance against certain risks involved in the trading process. Insurance instruments can protect exporters against the non-payment of buyers and insure against non-compliance by the seller and risks arising from government policy changes (*i.e.* political risk).

53. The role of financial institutions in trade finance is not limited to the provision of financial products. In addition, financial institutions provide valuable information to investors and traders depending on the financial service they provide to their client. They may inform their clients about present and future money and capital market conditions. And they operate through established international banking relationships with correspondents, which give their clients greater assurance about the legitimacy of their trading partners. While correspondent banks are used to facilitate trade transactions, the use of these banks does not provide legitimacy to the commercial parties to a transaction. Depending on the trade finance process used, it may provide a greater assurance of payment, however, it does not account for the legitimacy of a trading partner. This role feeds directly into the provision of the three groups of products and it will not be discussed separately.

Trade Settlement

54. In all business transactions, there is some commercial risk. However, in the international context, this risk can be magnified, as information about foreign companies (*e.g.* importers, foreign banks, economic conditions and foreign laws) would likely be less familiar to the exporter and his bank, than in respect of domestic clients. This applies equally to both exporters and importers.

55. For the exporter, commercial risks include the importer not accepting the merchandise or not paying for it once it is accepted. The importer risks that the exporter does not deliver the products at the agreed quality and time. In both cases, the capital invested in the purchase or sale – be it out of companies' own funds or through a credit facility – is at risk.

56. A key consideration in mitigating commercial risk is the choice of trade financing instrument. Traders typically choose from three main methods for settling trade transactions, depending on the extent of commercial risk: *i)* Clean Payments (open account and payment in advance), *ii)* Documentary Collections, and *iii)* Letters of Credit.

---

10 This section significantly relies on information by Hinkelman, E. G., (2002b)

11 This would include wire payments.

12 The term letter of credit is a broad term that includes both Commercial Letters of Credit (typically used for the purchase and sale of goods and services) and Standby Letters of Credit (used for various purposes to guarantee a payment and commonly used to guarantee the purchase and sale of goods and services).

57. It is estimated that about 80% of global trade is conducted not using the traditional process of letters of credit and collections and may be simply clean payments processed through financial institutions. Of the remaining 20% of global trade it is estimated that as much as ten percent may be transacted completely outside the traditional financial system.[13]

58. The following is a description of the three main methods of settling trade transactions.

(i) Clean Payments

59. Clean Payments are typically limited to transactions between well-established, ongoing trading partners or other partnerships where significant trust exists between the importer and exporter. In clean payment transactions, the role of the financial institutions is limited to the transfer of funds. Documents, such as title documents and invoices, are transferred between trading parties without a financial institution acting as the intermediary. Clean payments may be used for any purpose and are not specific to transactions between an importer and exporter.

60. As mentioned, the use of open account transactions by entities engaged in international trade is most commonly used. The decline in use of letters of credit or other trade finance vehicles is in relation to the overall growth in world trade. The actual transaction volume for letters of credit has remained relatively stable over time while the volume of world trade has grown.

61. A significant advantage of clean payments is that the administrative costs, including the time required to settle the transaction and the fee paid to a financial institution, are minimal.

62. The two most common types of clean payments are open account and payment in advance.

(i)(a) Open Account

63. An open account transaction involves the exporter shipping the goods and sending the trade documents directly to the importer. Once the goods are received, the importer arranges through its financial institution to forward payment to the exporter. In this arrangement, the exporter bears all risk and, in the absence of other financial arrangements, cannot access the funds until payment is received from the importer.

(i)(b) Payment in Advance (full or partial)

64. A payment in advance transaction reverses the order of an open account transaction. The first step involves the importer providing payment to the exporter as agreed. Once the exporter receives payment, the goods are shipped and the documents sent to the importer. In this arrangement, the importer bears all risk. In addition, there is an opportunity cost to the importer of using the funds prior to the goods being received.

65. Financial institutions participating in open account transactions will monitor transactions in accordance with domestic anti-money laundering and counter-terrorist financing regulations. This typically involves undertaking the appropriate customer due diligence (CDD) and record keeping as outlined in FATF recommendations and local regulatory requirements.

66. The level of scrutiny and information available on the underlying transaction will depend on the financial institution's exposure to credit and reputation risk associated with the nature of the customer relationship or its participation in the transaction. For example, because an institution's risk exposure when participating in an open account transaction is low, it would not likely scrutinise (or even see) the documents supporting the transaction (*e.g.* bills of lading or invoices).

[13] International Chamber of Commerce

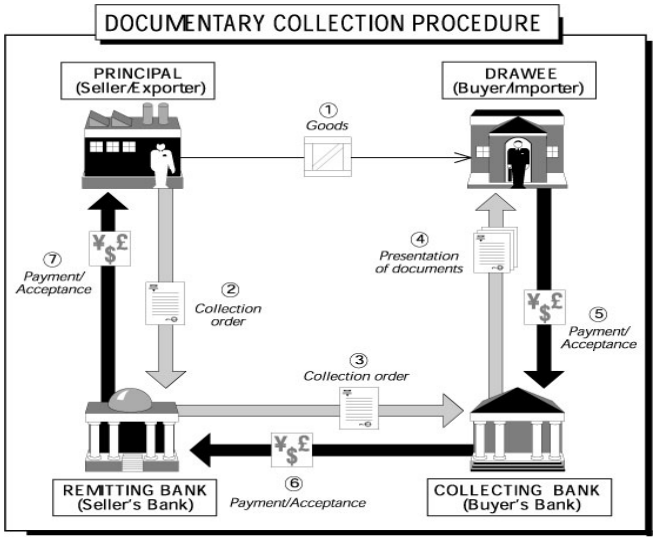
(ii) Documentary Collections

67. Documentary Collections involve the exporter transferring documents (such as an invoice and transportation documents) through exporter's bank to the bank designated by the importer. The importer is able to retrieve the documents once it has made payment or accepted drafts for future payment and obtain release of the goods. In simple terms, banks act as intermediaries to collect payment from the buyer in exchange for the transfer of documents that enable the holder to take possession of the goods. In a typical collections transaction, the bank does not have title or control over the goods.

68. As in the case of an open account transaction, there is a risk of non-payment by the importer, because financial institutions involved in the transaction do not guarantee payment or assume credit risk. The role of financial institutions is to act as an intermediary to forward documents from the exporter to the importer upon receipt of payment (Documents against Payment) or the importer's promise of payment at a later date (Documents against Acceptance). The banks are under no obligation to authenticate documents.

Documentary Collection Process

69. The documentary collection procedure involves the step-by-step exchange of documents giving title to goods for either cash or a contracted promise to pay at a later time. The diagram following the description below illustrates by way of example only each numbered step.



Contract for the purchase and sale of goods – The Buyer and Seller agree on the terms of sale of goods: (a) specifying a documentary collection as the means of payment, (b) naming a Collecting Bank (usually the buyer's bank), and (c) listing required documents.

(1) Seller ships the goods – The Seller ships the goods to the Buyer and obtains a transport document from the shipping firm/agent. Various types of transport documents (which may or may not be negotiable) are used in international trade and only where required by the underlying transaction is a negotiable document used.

(2) Seller presents documents to Remitting Bank – The Seller prepares and presents a document package to his bank (the Remitting Bank) consisting of: (a) a collection order specifying the terms and conditions under which the bank is to hand over documents to the Buyer and receive payment, and (b) other documents (*e.g.* transport document, insurance document, certificate of origin, inspection certificate, etc.) as required by the buyer.

(3) Remitting Bank sends documents to Collecting Bank – The Remitting Bank sends the documentation package by mail or by courier to the Collecting Bank in the Buyer's country[14] with instructions to present them to the Buyer and collect payment.

(4) The Collecting Bank reviews and provides documents to Buyer – The Collecting Bank (a) reviews the documents making sure they appear to be as described in the collection order, (b) notifies the Buyer about the terms and conditions of the collection order, and (c) releases the documents once the

[14] While a collecting bank may be in the buyer's country it need not be.

payment or acceptance conditions have been met. Acceptances under documentary collections are known as "Trade Acceptances" which, when accepted (by the Buyer), only carry the obligation of the buyer as opposed to a "Bankers Acceptance' commonly used under a letter of credit which carries the obligation of a bank.

(5) Buyer provides payment to Collecting Bank – The Buyer (a) makes a cash payment, or if the collection order allows, signs an acceptance (promise of the Buyer to pay at a future date) and (b) receives the documents and takes possession of the shipment.

(6) Collecting Bank provides payment to Remitting Bank – The Collecting Bank pays the Remitting Bank either with an immediate payment or, at the maturity date of the accepted bill of exchange if it receives payment from the Buyer.

(7) The Remitting Bank pays the Seller.

70. See Annex 7 for a description of the document that accompany a Documentary Collection transaction.

(iii) Letters of Credit

71. A letter of credit (also known widely as a documentary credit) is the written and almost always irrevocable[15] promise of a bank to pay a seller the amount specified in the credit, subject to compliance with the stated terms. The fact the seller is relying on the promise of a bank rather than the buyer for payment is the biggest distinction between a letter of credit and a documentary collection transaction.

72. Documentary credits provide a high level of protection and security to both buyers and sellers engaged in international trade. The seller is assured that payment will be made by a bank so long as the terms and conditions of the credit are met. The buyer is assured that payment will be released to the seller only after the bank has received the documents called for in the credit and those documents comply with the terms and conditions of the credit.

73. Although documentary credits provide good protection and are the preferred means of payment in many international transactions, they do have limitations. They do not, for example, ensure that the goods actually shipped are as ordered. It is up to the parties to settle questions of this nature between themselves. Documentary credits will also have higher transaction costs than other settlement methods. A letter of credit is an international established practice offering the best level of legal / contractual certainty, and therefore constitutes one of the most reliable payment methods for international transactions. A core element of the letter of credit is the concept that banks deal with documents and not with goods, services or performance to which the documents may relate[16] and banks examine documents presented under letters of credit "on their face"[17] in compliance with international standards banking practice.[18]

74. While this covers the traditional commercial letter of credit, standby letters of credit and bank guarantees are often frequently used for the purchase of goods and services internationally.

---

15 Revocable credits are rarely used today and are no longer included in international rules such as the International Chamber of Commerce Unified Customs and Practise (UCP).

16 UCP 600 Article 5.

17 UCP for Documentary Credit, Article 14(a).

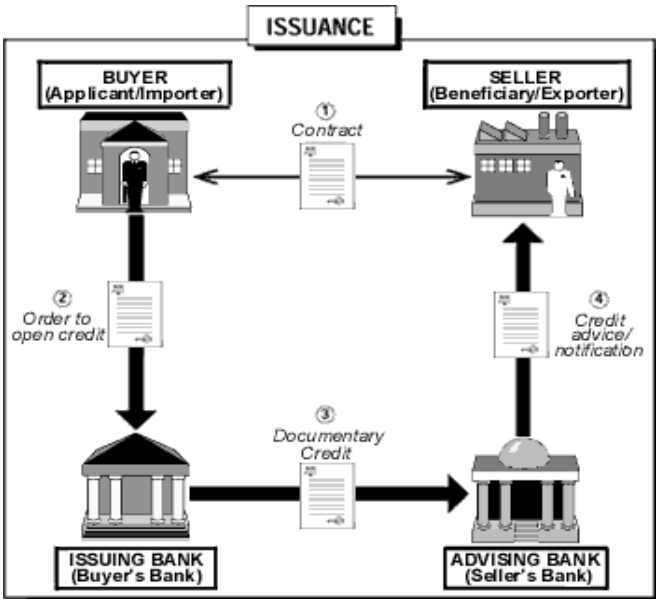
18 UCP Article 14 (d).

Basic Documentary Credit Procedure

75. The documentary credit procedure involves the step-by-step exchange of documents required by the credit[19] for either cash or a contracted promise to pay at a later time. There are four basic groupings of steps in the procedure: (a) Issuance; (b) Amendment, if any; (c) Utilisation; and (d) Settlement. A simplified example follows:

(a) Issuance

76. Issuance describes the process of the buyer's applying for and the issuing bank opening a documentary credit and the issuing bank's formal notification of the seller either directly or through an advising bank.



(1) Contract – The Buyer and Seller agree on the terms of sale: (a) specifying a documentary credit as the means of payment, (b) naming an advising bank (usually the Seller's bank), and (c) listing required documents. The naming of an Advising Bank may be done by the buyer or may be chosen by the issuing bank based on its correspondent network

(2) Issue Credit – The Buyer applies to his bank (Issuing Bank) and the issuing bank opens a documentary credit naming the Seller as beneficiary based on specific terms and conditions that are listed in the credit.

(3) Documentary Credit – The Issuing Bank sends the documentary credit either directly or through an advising bank named in the credit. An advising bank may act as a bank nominated to pay or negotiate (nominated bank) under the credit or act as a confirming bank where it adds its undertaking to the credit in addition to that of the issuing bank. Only in those cases where an advising bank is not nominated to negotiate or confirm the credit is the role of that bank simply an advising bank.

(4) Credit Advice - The advising, nominating or confirming bank informs (advises) the seller of the documentary credit.

(b) Amendment

77. Amendment describes the process whereby the terms and conditions of a documentary credit may be modified after the credit has been issued.

78. When the seller receives the documentary credit, it may disagree with the terms and conditions (*e.g.* the transaction price listed in the credit may be lower than the originally agreed upon price) or may be unable to meet specific requirements of the credit (*e.g.* the time may be too short to effect shipment).

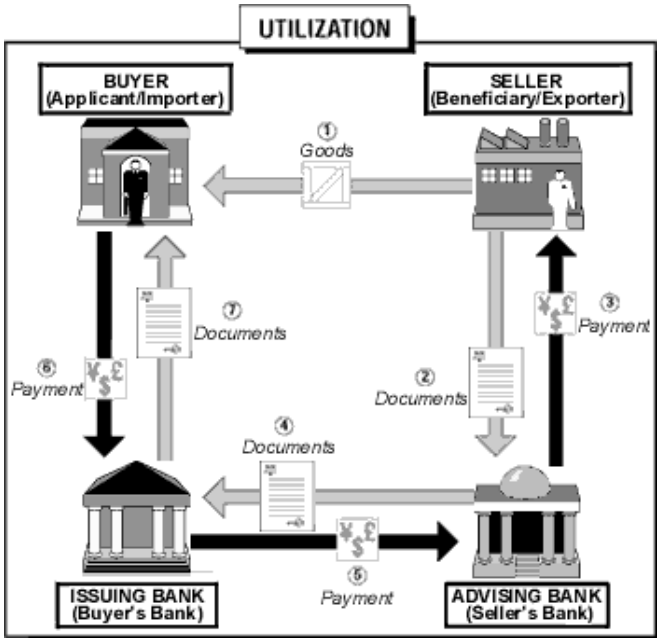
79. If the seller wants to amend the terms prior to transacting, the seller can request these from the buyer. It is at the discretion of the buyer to adopt the proposed amendments and request an amendment to be issued by the issuing bank. An amended letter of credit would be issued by the issuing bank to the seller through the same channel as the original documentary letter of credit.

[19] Title only transfers if a document of title is required under the credit.

Amendments to a letter of credit require the agreement of the issuing bank, confirming bank (if any), and the beneficiary to become effective.

(c) Utilisation

80. Utilisation describes the procedure for the seller's shipping of the goods, the transfer of documents from the seller to the buyer through the banks (presentation), and the transfer of the payment from the buyer to the seller through the banks (settlement). For example:



(1) Seller ships goods – The seller (beneficiary) ships the goods to the buyer and obtains the documents required by the letter of credit.

(2) Seller presents documents to Advising or Confirming Bank or directly to the Issuing Bank – The seller prepares and presents a document package to his bank (the advising or confirming bank) consisting of (a) the transport document if required by the credit, and (b) other documents (*e.g.* commercial invoice, insurance document, certificate of origin, inspection certificate, etc.) as required by the documentary credit.

(3) Nominated or Confirming Bank reviews documents and pays Seller - The nominating or confirming bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit and (b) pays the seller (based upon the terms of the credit) which may mean that payment does not occur until after (5). An advising bank does not normally examine the documents, but simply forwards them on to the confirming or issuing bank for their examination.

(4) Advising, Nominated or Confirming Bank transfers documents to Issuing Bank – The Advising, Nominated or Confirming bank sends the documentation by mail or by courier to the issuing bank.

(5) Issuing Bank reviews documents and reimburses the Nominated or Confirming Bank or makes payment to the beneficiary through the Advising Bank – The Issuing Bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit, under advice to the Buyer that the documents have arrived, and (b) pays the beneficiary through the advising bank or reimburses the nominated or confirming bank (based upon the terms of the credit) and,

(6) Buyer reimburses the Issuing Bank – The Buyer immediately reimburses the amount paid by the issuing bank or is granted a credit by the issuing bank allowing it to reimburse the issuing bank at a later date.

(7) Buyer receives documents and access to goods – The Issuing Bank sends the documents by mail or courier to the buyer who then takes possession of the shipment.

(d) Settlement

81. Settlement describes the different ways in which payment may be effected to the seller from the buyer through the banks. The form of payment is specified in the original credit, and must therefore be accepted by the seller. The following are common settlement methods:

- The Sight Credit (Settlement by Payment) – In a sight credit, the value of the credit is available to the exporter as soon as the terms and conditions of the credit have been met (as soon as the prescribed document package has been presented to and checked by the issuing, nominated or confirming bank and found to be conforming to the terms and conditions of the credit) or once the advising bank has received the funds from the issuing bank (unconfirmed). Payment may be affected directly by the nominated bank or confirming bank upon their examination of the documents and they are reimbursed for that payment by the issuing bank.
- The Usance Credit (Settlement by Acceptance) – In a Usance Credit, the beneficiary presents the required document package to the bank along with a time draft drawn on the issuing, nominated or confirming bank, or a third bank for the value of the credit. Once the documents have been found to be in order, the draft is accepted by the bank upon which it is drawn (the draft is now called an acceptance) and it may be returned to the seller who holds it until maturity.
- The Deferred Payment Credit - In a deferred payment credit the issuing bank and/or the nominated or confirming bank accepts the documents and pays the beneficiary after a set period of time. The issuing, nominated or confirming bank makes the payment at the specified time, when the terms and conditions of the credit have been met.
- Negotiation is the term used where a bank other than the issuing bank agrees to advance funds or discount drafts to the exporter before the issuing bank has paid. Discounting an accepted draft has the same effect.

82. A letter of credit will normally require the presentation of several documents including a Draft[20], Commercial Invoice, Transport Document, Insurance Document, Certificates of Origin and Inspection, Packing and Weight Lists. Annex 7 provides some detail on the kinds of information that may be contained in each of these documents.

Export Financing

83. Through a variety of sources and structures, exporters can obtain financing (working capital) to facilitate their trading activities and bridge the time from which they spend money on an export activity (for example, securing an export order) until the moment of payment. Working capital financing can be applied to the manufacture and development of goods prior to shipment, or be applied to business activities following shipment but prior to receipt of payment.

84. The following section briefly describes the following types of trade finance:

(a) Direct Loans or general credit facility.
(b) Note Purchases (also known as forfaiting).
(c) Factoring.
(d) Guarantees.

(a) Direct Loans

85. Acting independently or as part of a syndicate, financial institutions and other entities offer loans to facilitate export transactions. There are two basic types of loans. Buyer credit involves an arrangement to finance exports generally related to a specific contract. Supplier credit transactions are structured to provide the exporter with the ability to provide its buyer with extended payment terms. These loans may also be backed by export or buyer credit guarantees provided by the governments of the countries involved.

[20] Drafts are not always required by a credit.

(b) Note Purchases / Forfaiting

86. Financial entities can purchase promissory notes or bills of exchange issued by foreign buyers to exporters for the purchase of goods and services, freeing up cash for the exporter.

(c) Factoring

87. In international trade, factoring is the purchase or discounting of a foreign account receivable for cash at a discount from the face value. While factoring is primarily undertaken by non-bank financial entities, banks may participate in factoring if the exporter has obtained accounts receivable insurance that guarantees the liquidity of the accounts.

(d) Guarantees

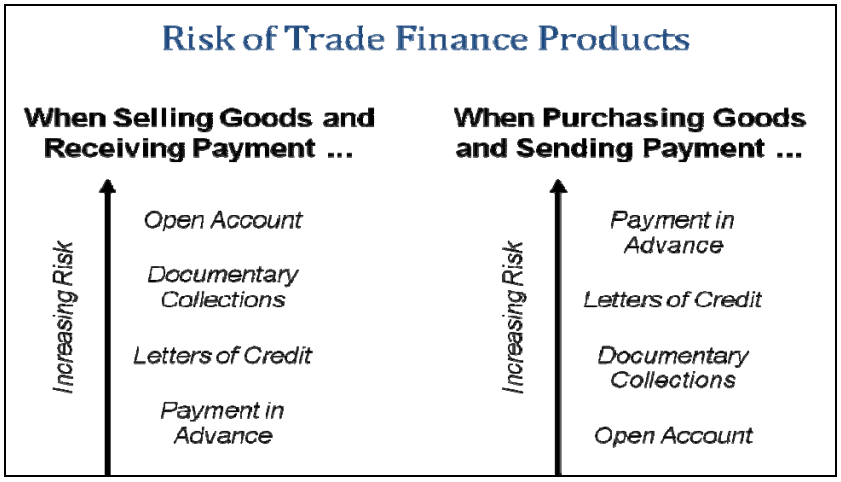
88. Guarantees are provided to or by financial institutions on behalf of exporters. Two popular types of export guarantees are pre-shipment and performance guarantees.

- *Pre-shipment Guarantees* encourage other financial institutions to advance pre-shipment loans to fund the upfront costs associated with an export contract.
- *Performance Guarantees* providing contract performance cover to buyers on behalf of the exporter.

89. It should be noted that both guarantees and standby letters of credit may be used in various ways to generate the purchase or sale of goods or services. In those cases many of the documents outlined in the steps above may or may not be utilised as part of the transaction.

Transaction risks for importers vs. exporters

90. The graphic below shows the different types of core trade finance products available, and positions each in terms of transaction risk, from the importer's and from the exporter's perspective. Importers and exporters consider these transactional risks in conducting legitimate trade transactions. The product choice will depend on the level of trust between the buyer and seller. Proliferators will also consider transactional risks when deciding how to sell/purchase and receive payment for/send payment for goods.



Source: Canada.

Risk Management and Customer Due Diligence (CDD)

91. All financial institutions involved in trade finance, no matter what their business line, have both commercial incentives and legal obligations to conduct CDD and potentially account monitoring. But the nature and depth of CDD undertaken, and how it is organised, can vary significantly between financial institutions, from transaction to transaction and based on the regulations in the local jurisdiction.

92. Some elements of CDD are universal: CDD processes include the identification and, in a risk-based manner, the verification of the identity of customers and reasonable measures to identify and verify the identity of beneficial owners, obtaining information on the purposes and intended nature of the business relationships and conducting ongoing due diligence. Of these components, the identification and verification of identity of customers are requirements that need to be completed in all situations.

93. The implementation of other components of CDD is variable, depending on the risks associated with the transaction and the legal requirements in the jurisdictions involved. A reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanism used to meet these standards.[21] The CDD process that a financial institution will perform before they act or an international trade transaction will be dependent upon a number of factors, these include:

- Specific regulatory requirements or guidance to which it is subject.
- The role which it will be required to perform in the transaction.[22]
- The institution's own exposure to financial or reputational risk through the transaction.
- Its assessment of the risk posed by the country in which the instructing party is based or operates.
- Its assessment of the risk nature of the underlying trade business (*i.e.* the goods, products or services being traded.).
- Whether any other higher risk parties appear to be involved as owners or intermediaries.

94. Appropriate CDD measures, relying in particular the factors above, are a critical first step for a financial institution to mitigate the risk of proliferation financing.[23]

95. Where the financial institution is granting any form of credit to the party from whom instructions are expected, then more extensive information would be requested as part of the CDD process, focused particularly on the client's financial standing, credit risk, and ability to repay. Equally where the financial institution assesses a customer to be higher risk then it may well employ "enhanced CDD" to the extent that a risk-based approach is allowed by the relevant regulatory authority.

---

21 FATF (2007)

22 In a letter of credit transaction, for example, financial institutions view different parties in the transaction as their customers for CDD purposes. As an issuing bank the applicant of the credit will be their customer, as an advising, nominating or confirming bank the issuing bank will be their customer. In some cases the beneficiary of a credit may be the customer of the advising, nominated or confirming bank and they may have done CDD on that beneficiary, however in most transactions the banks look to the issuing bank as their customer.

23 Customer Due Diligence is, depending on the type of internal organisation, conducted at the relationship management area rather than in the trade operations. This area may be a specific relationship manager, a relationship management group, a client coverage area, a compliance group or other area designated by the bank. Depending on the bank's internal policies and procedures the actual point of review, investigation, notification, determination, decision or reporting may vary.

96. Each financial institution has its own organisational structure for conducting CDD, an element of which may include outsourcing to employees that are located in different countries and undertake transactions that are not local to them. The same obligations for CDD apply no matter what arrangements are in place for implementing them.

Correspondent Banks

97. In the context of trade finance it is important to note that no one financial institution will undertake all aspects of CDD related to a specific transaction; and as discussed, different financial institutions will be responsible for individual elements depending on their role.

98. Since financial institutions in foreign countries do not necessarily have a presence in all countries or a relationship with all financial institutions, financial institutions are sometimes used as correspondents in the payment chain. Payment transactions are ordered in a foreign country, transit through one or more financial institutions and finally are received by the beneficiary located in a second foreign country. Such transactions may also occur when designated financial institutions in a country are prohibited from conducting financial transactions with institutions from another country, and therefore a correspondent financial institution in a third country is used as an intermediary.

99. With banks undertaking international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence, correspondent banks must rely on the respondent bank's due diligence and monitoring controls. However, a financial institution would not normally initiate a transaction on behalf of a party it does not know.

100. A primary objective for any financial institution when agreeing to accept instructions from a correspondent will be to ensure that the correspondent conducts satisfactory CDD on its own customers. Establishing a correspondent relationship might involve an understanding of the customer and documenting that the associated CDD obligations are undertaken.

101. As part of due diligence which is performed on a potential correspondent it is critical for the financial institution to agree and establish the types of accounts, if any, they will operate and the means of exchanging authenticated (bank to bank) messages. These mechanics are necessary for the handling of international trade transactions.

102. Although many financial institutions have procedures to ensure that the respondent institution's controls are adequate to mitigate the risk of money laundering and terrorist financing,[24] most do not specifically assess whether a respondent institution has adequate controls to detect and prevent proliferation financing. Such assessments may rely on information that is not currently reviewed as part of correspondent banking procedures[25], such as information related to a respondent financial institution's trade finance controls or its association with a state proliferator.

103. For more information in the risks related to money laundering and terrorist financing by correspondent banking, see the FATF Report on Money Laundering Typologies 2001-02.

Reviewing and monitoring transactions

104. Financial institutions manage a wide range of risks in the processing of international trade business. In practice risk management will normally include credit risk, including cross border or country risk, and the operational risk. Exposure to money laundering and terrorist financing form part

[24] For more information in the risks related to money laundering and terrorist financing by correspondent banking, see FATF (2002).

[25] Customer Due Diligence for correspondent banks is usually conducted in a centralised relationship management area within financial institutions. This area may be a specific relationship manager, a relationship management group, a client coverage area, a compliance group or other area designated by the bank.

of the overall risk management process. Such risk management processes will influence what arrangements are in place for reviewing documents and monitoring transactions.

105. If there is potential exposure to proliferation financing, financial institutions consider whether parties involved in payments are named in UN or relevant local sanctions lists or are considered to pose other risks. For example, if the transaction is subject to any export licensing requirements or trade embargoes.

106. All financial institutions are expected to have a form of financial transaction monitoring in place. The form of monitoring varies between (and within) institutions, including automated or manual checking, or a mixture of both, in order to monitor the transactions handled. This may involve reviewing customers' accounts or patterns of activity.

107. The information presented to a financial institution will vary according to the nature and complexity of the transaction. The extent to which this information needs to be verified will also vary. In general a financial institution will normally examine trade instructions received to establish whether:

- They have CDD on the instructing party;
- The instruction is consistent with what would normally be expected from the instructing party.

108. Financial institutions will also check the documents presented to them in accordance with relevant International Chamber of Commerce (ICC) rules and accepted banking practice. Furthermore, where letters of credit are concerned, the vast majority of transactions will be subject to commercial expectations and ICC standards which determine the time allowed for processing the various stages during the lifespan of the letter of credit.

109. It should be noted that in processing trade finance transactions, financial institutions deal with documents, not the physical goods to which they relate. Any physical inspection of goods will only occur in exceptional circumstances and would tend to relate to wider credit issues where the underlying goods are pledged as security. However, commercial parties to the underlying transaction may use other agencies to independently verify a particular shipment. Consequently inspection and verification measures in relation to physical goods are relatively rare as the vast majority of trade transactions are conducted legally between parties who willingly disclose all the information needed to conclude such transactions.

110. However, some existing transaction monitoring controls currently employed by financial institutions may result in the detection of proliferation finance. Financial institutions may currently detect transactions associated with proliferation activity by screening transactions against proliferation-related United Nations sanctions lists, such as the list of individuals and entities designated pursuant to S/RES/1737 (2006), or other local proliferation sanctions lists, to detect the presence of an individual or entity involved in proliferation in the transaction. In some cases, financial institutions may also attempt to verify whether a transaction is subject to any export licensing requirements or trade embargoes by requesting additional verification or documentation, such as export control licenses.

Identifying Suspicious Activity

111. There are several points in the trade finance cycle at which financial institutions could potentially detect suspicious activity if provided sufficient information by their customer and/ or relevant government authorities. For example, CDD processes can establish risks: whether a customer is a producer or buyer of goods or services which the institution regards as high risk, including ongoing monitoring of transactions, as described above, can also identify activity which may be intended to obscure the ultimate counterparties to the transaction or the eventual destination of goods.

If suspicious activity is suspected, the role of financial institutions is not to determine the underlying criminal activity; but to report suspicious activity in line with their domestic legal framework and relevant local regulations (including data privacy laws).

112. Financial institutions rely on export control regimes and customs authorities to police the activities of exporters which are its customers, in part as financial institutions are unlikely to have staff technically qualified to understand whether an apparently legitimate or innocent trade transaction is subject to such a control or whether in any event it is actually part of a proliferation finance scheme.

113. The ability of financial institutions to detect suspicious activity in their trade finance operations is constrained by several factors:

- The description of goods may be too vague and/or technical for a financial institution to determine if it is proliferation-sensitive or not.
- The fragmented nature of the trade cycle and the involvement of different financial institutions in a single transaction.
- The systems used to monitor transactions and volume of transactions will also influence the ability to review information and identify potential suspicious activity. Even where only a single financial institution is involved in a transaction, the organisational complexity of the institution may mean that no one individual examines all elements of CDD and monitoring associated with a transaction. This can make it difficult to identify complex or large-scale patterns which might indicate suspicious activity.
- The detection of fraud or money laundering by financial institutions is based on well-understood indicators and profiles, developed from a substantial case history. Proliferation financing has only recently garnered attention and consequently has not been incorporated into financial institutions' due diligence processes – whether through profiles or staff training programmes - to the same degree. Indicators or "red flags" invariably only become evident after the event when a transaction has already been completed.
- The availability of specific information regarding suspicious or high-risk entities is critical, as the factors noted above limit financial institutions' capacity to detect generic patterns associated with proliferation financing. Therefore, the ability of a financial institution to detect and identify potential proliferation financing is dependent on clear guidance or specific intelligence provided by authorities.

Money Services Businesses

114. Apart from supervised payment services, illegal, informal or registered money services businesses or alternative remittance systems (*e.g.* Hawalas) can also be used to transfer funds. Entities involved in proliferation financing activity may also use this sector if there is strong detection or monitoring measures in place for financial institutions in the formal sector.

Authorities relevant for export control

115. A jurisdiction's export control policy is usually implemented by a number of agencies that have varying responsibilities. The main authorities, which contribute to the implementation of the export control policy, are as follows:

- Licensing authorities
- Law enforcement and customs authorities
- Intelligence services (as a part of their general duties)

116. In accordance with their specific responsibilities, licensing authorities, law enforcement and customs authorities and intelligence services each play a major role in the prevention of proliferation. Licensing authorities decide whether the export of an item is subject to licensing or is exempt. They are also responsible for making licensing decisions – and for informing exporters of the decisions they have made. Normally, in adherence to their international obligations under relevant multilateral arrangements, jurisdictions will require an export licence application for controlled goods.

117. Items covered by national and international lists usually range from weapons, ammunition and related production facilities via material, plants and equipment for nuclear, biological and chemical purposes, high-grade materials, specific machine tools, electronic equipment, computers, telecommunications up to specific chemical units and chemicals. In addition to the licensing requirements for listed items, there are often licensing requirements for non-listed items depending on the use they may be put to. Experience shows that unlisted items are playing an increasing role in proliferation activities. Export control systems may incorporate "catch-all" clauses, to restrict trade in such items that in circumstances could be used for proliferation purposes. However, these catch-all clauses are usually only triggered when the destination and end-user is known to be of proliferation concern, unless there is evidence that the destination / end-user has established front companies elsewhere to try and circumvent controls. In cases concerning sensitive jurisdictions, technical assistance as well as the trafficking and brokering of items particularly from 3rd countries to those destinations may also be subject to additional controls.

118. National export control regimes usually provide that the exporter is liable for compliance with the restrictions and licensing requirements in force. Therefore, licensing authorities often reach out to industry in order to make them aware of their responsibilities. Ideally, licensing authorities and exporters work together to ensure compliance with this legislation.

119. Law enforcement and customs authorities monitor and control trade in order to detect deliberate offenders who illegally export or divert strategic proliferation-sensitive goods, software and technology. Law enforcement and customs authorities decide whether the exporter or importer wishing to export, import or transit their jurisdiction respects national and international regulations. Focus is most often placed on the verification of exports through selective risk-based examination. In the case of exports to jurisdictions of concern, efficient systems will often require all exports to be examined in this way. Surveillance procedures are used in the first instance to identify targets using documentation provided prior to export. The assessment of this information may lead to the targeting of particular shipments for physical examination. In some instances customs authorities may regularly decide to subject all cargo being shipped from a particular port or airport to such a destination to a physical examination.

120. Law enforcement and customs authorities are in a position to examine whether the description of the items in the export license match the items actually being exported. Customs authorities have the ability to physically inspect the goods, use their expertise and that of others within government with specialist knowledge of dual-use and other proliferation sensitive goods, to decide if export control requirements have been met.

121. If available, an intelligence service will provide specific information to enhance the monitoring by licensing and customs authorities. The intelligence function is a critical component for collecting, evaluating, collating, analysing and disseminating information on actual, suspected and potential export violations and trends. Intelligence is crucial in identifying suspected or known violators and ultimately unravelling complex networks. Intelligence is important in uncovering illegal procurement tactics such as diversion through false description of goods or the use of front companies. Intelligence is also used to detain and seize goods and may in certain circumstances be used by prosecutorial authorities. Provision of information on proliferation activities by intelligence is therefore a key element to prevent proliferation.

122. The exchange of information between customs and the wider export control enforcement community such as law enforcement, defense and export licensing authorities is imperative for an effective export control system. Licensing and customs authorities are in the best position to detect non-compliance with export control requirements, including criminal acts such as forgery of export documents and other related materials. However, financial information may provide another intelligence stream to supplement or reinforce existing channels in the fight against proliferation.

3. CASE STUDIES

123. The following 18 case studies illustrate some common techniques used by proliferators to transfer and export technology, goods, services or expertise that contribute to the proliferation of weapons of mass destruction.

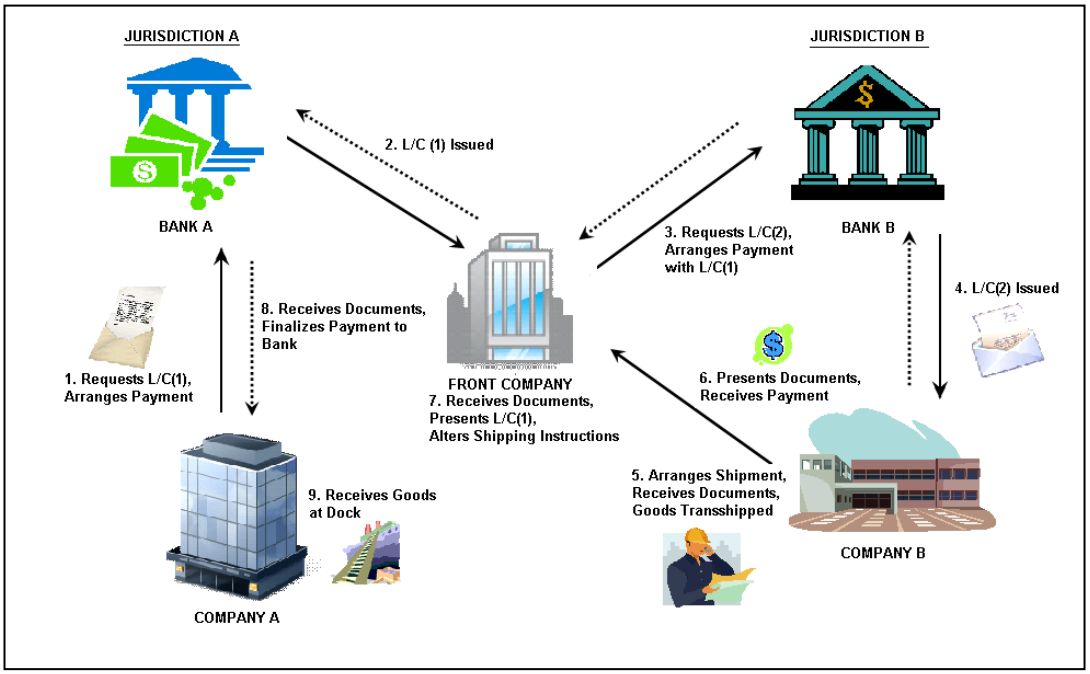
124. The cases also indicate that the international financial system is being used to facilitate proliferation. In many of these cases proliferators use letters of credit to settle trade in sensitive goods. In some there are more simple examples of wire transfers and large cash transactions that are used to move funds in efforts to facilitate proliferation. Annex 3 contains additional cases with no proven link to the financial sector, but that provide useful context.

125. While the majority of the cases mentioned in the report illustrate traditional means of trade financing such as letters of credit, there is no evidence that suggests that these financial instruments are more susceptible to potential abuse by proliferators. It would have been very difficult for the financial institution to detect proliferation financing based on evidence provided in the cases that illustrate links to the international financial system.

126. It is likely that proliferation background is more difficult to detect if other financial instruments, such as clean payments, are used. These cases studies describe features of the transactions, which were discovered through subsequent investigation, which would not at the time have provided a meaningful basis for financial institutions to report suspicions. They nevertheless can illuminate the financial features associated with the underlying acts of proliferation.

Cases involving letters of credit

Case 1: Letters of credit and front company



1. In **Jurisdiction A**, **Company A** requests that Bank A draw up Letter of Credit (1) and arranges payment for goods from a **Front Company**.
2. **Bank A** issues Line of Credit (1) to the **Front Company**.
3. The **Front company** then requests Letter of Credit (2) from Bank B in Jurisdiction B and arranges payment using Letter of Credit (1).
4. **Bank B** issues Letter of Credit (2) to Company B located in Jurisdiction B.
5. **Company B** arranges for shipment of goods to Front Company, arranges documents and transhipps goods.
6. **Company B** presents documents to **Bank B** and receives payment.
7. Front Company receives documents from **Bank B**, presents for Letter of Credit (1) and alters shipping instructions.
8. **Front Company** gets documents and finalizes payment to **Bank A**.
9. **Company A** receives goods at port.

Source: United States.

Case 2: Purchase of magnets through front companies and intermediaries

A proliferator set up front companies and used other intermediaries to purchase magnets that could be used for manufacturing centrifuge bearings.

False declaration
Front Company 1 signed documents with the foreign jurisdiction's manufacturing company concerning the manufacturing and trade of magnets, however, it was not declared in these documents, nor was it detected by authorities, that these components could be used to develop WMD.

Diversion
The magnets were transhipped through a neighbouring third jurisdiction to Front Company 2. This jurisdiction was typically used as a "turntable" for goods *i.e.* goods are imported and re-exported. The proliferator used an intermediary to arrange for the import and export of the magnets in this third jurisdiction. The intermediary had a sound understanding of the jurisdiction's export and commercial controls and used this knowledge to conceal the nature of the goods.

Using banks with poor AML/CFT controls
The intermediary also conducted financial transactions to settle trades. The intermediary had accounts with several banks in the third jurisdiction and used these banks to both finance the acquisition of goods and launder the illegal funds used for these transactions. A combination of cash and letters of credit were used to pay for the trade of the magnets, which totalled over 4 million USD.

Source: Gruselle, Bruno, (2007).

Case 3: The Thyratron case in Halmstad

In the spring of 1999 the Swedish Customs found out that a person (P) in Halmstad, via a pizzeria, had exported a thyratron to Iran that was classified as a strategic product and therefore was subject to export control. After an audit and interview with P, suspicions grew that it was a question of smuggling.
A search was made in the apartment of P and a seizure of a thyratron was made at Arlanda Airport. It was on its way to a jurisdiction of proliferation concern. Earlier another thyratron was already exported.
P stated that he had been contacted by his cousin in the jurisdiction of proliferation concern in the spring of 1998 who worked at a university in that jurisdiction. The cousin wanted P to get a thyratron to the university. The producer in the United States directed P to the branch in Sweden. P stated he would use it as a degree project at a Swedish university. He forged an end user statement in order to buy the thyratron.

P paid the company 22 000 SEK and delivered the product to Halmstad. P contacted a forwarding company in order for them to export the thyratron to a university in the jurisdiction of proliferation concern. P wrote a pro forma invoice in the name of the pizzeria. The buyer was the university in the jurisdiction of concern. The thyratron was then exported.

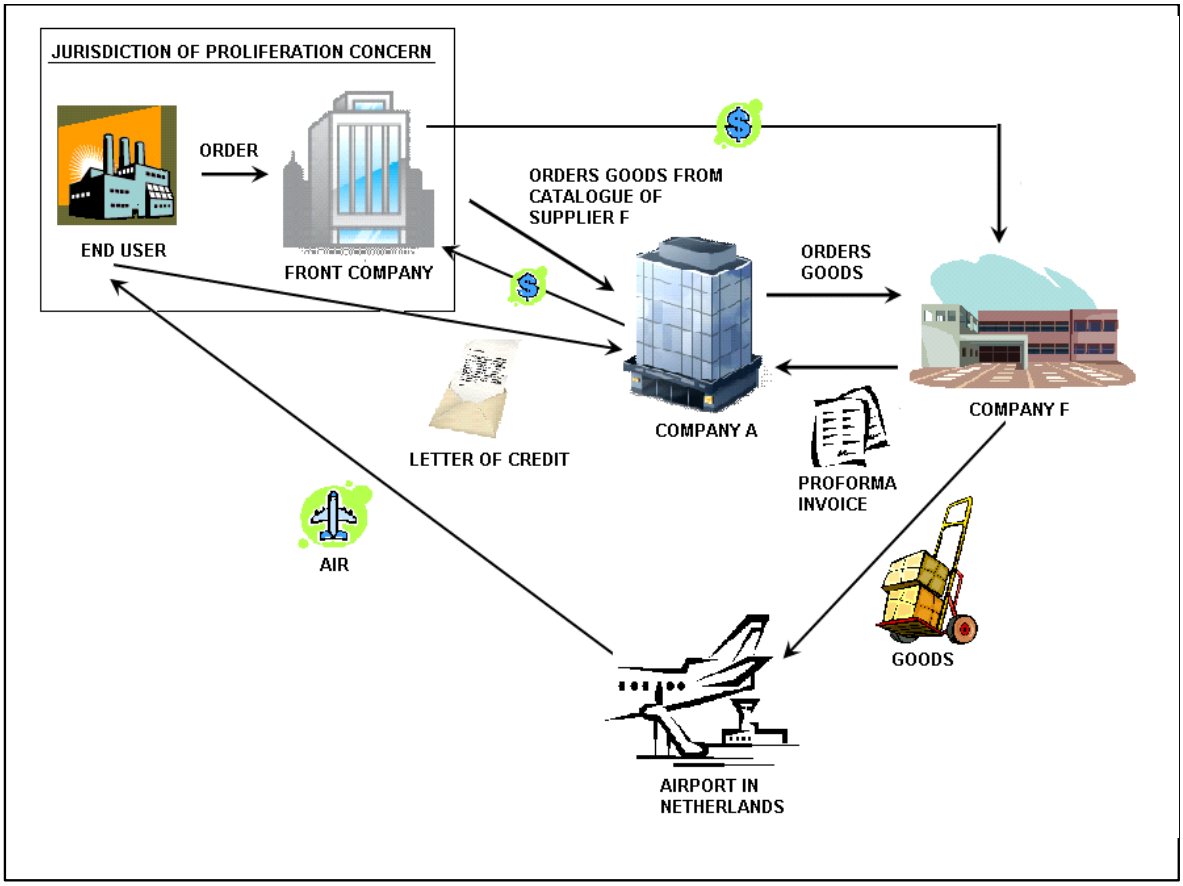
In November 1998 P ordered one more thyratron after an order from another university in the jurisdiction of concern. P paid the delivery and in 27 May 1999 the thyratron was delivered to P in Halmstad.

The forwarding company got an assignment to send it to the jurisdiction of concern. The product was not exported because P had not paid the forwarding company for the cost of the freight terminal. P had the impression that Iran Air would once again be responsible for all expenses like last time.

During the preliminary investigation the Swedish Customs found documents like dispatch notes for payment from abroad, inter alia, from the jurisdiction of proliferation concern.

Source: Sweden.

Case 4: Letter of credit and front company



A **Front Company** in a Middle-Eastern jurisdiction of proliferation concern, used the following method in order to obtain goods. The **Front Company** represents several large companies located in the jurisdiction of concern that are also established in Europe and other Western countries. The **Front Company** stands surety for the delivery of the needed goods to the companies in the jurisdiction of concern and executes eventual after sales services. The **Front Company** has the first contact with the true **End User** in the jurisdiction of concern.

The **End Users** order the needed goods from the **Front Company**. The **Front Company** orders the goods of the different Western companies from " **A**", that is to say, only on the basis of the article numbers in the catalogue and informs "**A**" about the supplier the goods have to be bought from. At request a L/C is opened in favour of "**A**". It also happens that "**A**" itself has to look for a supplier on the basis of an article number or article description. This happened worldwide. "**A**" orders the goods after having received the order (pro-forma invoice) from **F** and the L/C from the Middle Eastern client or end user. The goods that were bought outside the Netherlands came in transit to the airport of Schiphol and were delivered at a forwarding agent. The goods were sent from Schiphol airport to the jurisdiction of concern. "**A**" did not see the goods itself.

"**A**" placed the payment received from the end users through the L/C at the disposal of **the Front Company** by means of a bank account with a Dutch bank and after deduction of a commission. The suppliers were paid by the **Front Company**.

Source: The Netherlands.

Cases 5 to 8: State-owned entities

Three known instances of procurement for WMD programmes routed through state-owned banks whose overseas branches and correspondent banking partners facilitate business with foreign suppliers:

Case 5: Company A, a well-known front company for one of the entities responsible for country Z's ballistic missile programme, in order to buy 'special items' from country X, opened a Letter of Credit at a branch of a state-owned bank in Z's capital. The London branch of the same state-owned bank was named as the Advising Bank and in due course transferred payment to the supplier of the 'special items'.

Case 6: A branch of the same state-owned bank in another European capital was instructed to transfer over $100,000 to the account of a company in country U, a near neighbour of Z and a known diversionary destination. The company is owned by a well-known procurement agent who asked for the money to be transferred to a specific UK bank in order to cover the purchase of goods associated with a Letter of Credit opened with a branch of the same state-owned bank in Z's capital.

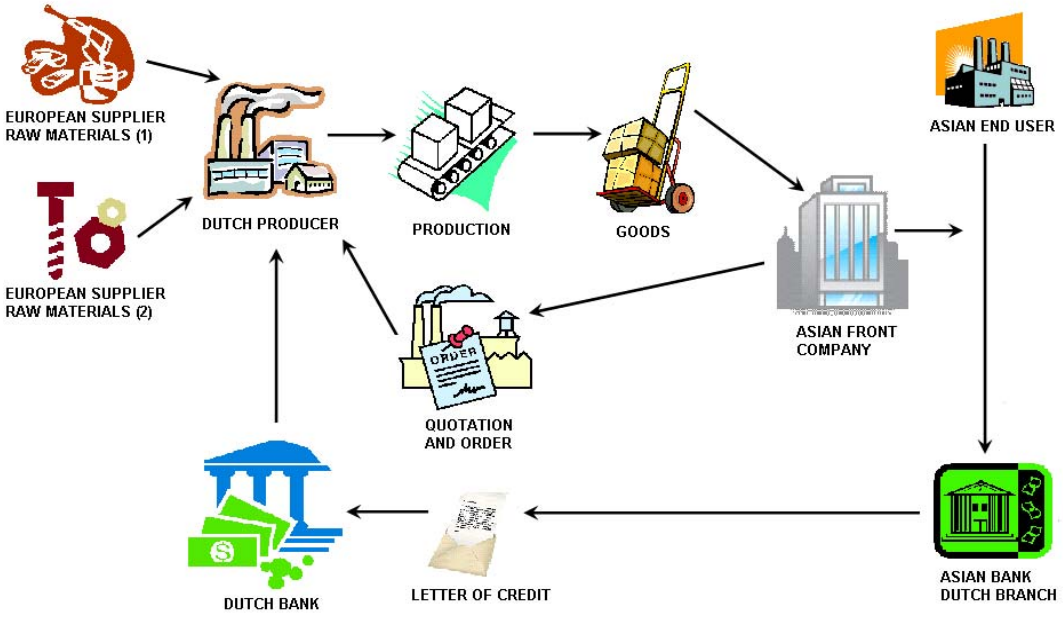
Case 7: In country Y, a state-owned bank known as the X Commercial Bank is known to have close relations with country Y's main arms exporters. In the past it has routed transactions through European banks. Recently it has sought correspondent bank relationships with several banks in a large Asian country, seeking to open Euro and US dollar accounts.

Use of a UK bank in a Diversionary Destination

Case 8: Trading company B in country Z deals in laboratory test-equipment for university and research centres and also for the energy sector. It is known to have procured dual-use items for country Z's WMD programmes.
Company B has bank accounts in a number of countries and has a UK account with a UK bank in country U, a known diversionary destination.

Source: United Kingdom.

Case 9: Infringement of export controls and Letter of Credit



This case concerns the infringement of export controls. Strategic goods were exported without the obligatory authorization. The Dutch producer was contacted by a Front Company, in an Asian jurisdiction of proliferation concern, to provide certain strategic goods, carbon fiber with special characteristics. The Dutch producer ordered the materials from two suppliers in other European countries. Payment took place through a Letter of Credit. The bank of the true Asian end user actually issued the letter of credit to the Dutch bank of the producer.

Finally the prosecutor decided to no longer pursue this suspect, since during the pre-trial the testimony of the expert stated that after the specific production performed by the Dutch producer, the end result of the carbon fibre no longer contained the characteristics for which it qualifies as a strategic good.

Source: The Netherlands.

Case 10: ASHER KARNI

Overview
Asher Karni was the principal in an import/export business known as Top-Cape Technology. In July 2003, agents from the U.S. Commerce Department (Commerce) and the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement learned that Karni was in the process of acquiring 200 triggered spark gaps from a company in Massachusetts and that he planned to have the triggered spark gaps sent to Top-Cape in South Africa, from where the items, at his instruction, would be re-exported to Pakistan. Triggered spark gaps are high-speed electrical switches that are capable of sending synchronized electronic pulses. They can be used as detonators of a nuclear device.

Investigation and outcome
U.S. export laws and regulations require the issuance of a license for the export of triggered spark gaps to Pakistan. At the request of investigating agents, the manufacturer agreed to disable the triggered spark gaps before they were shipped to Karni's company in South Africa through a broker.

In October 2003, Karni's company illegally sent the triggered spark gaps to Islamabad, Pakistan via Dubai, UAE. Karni was arrested on Jan. 1, 2004, in Denver, CO, when he arrived for a ski vacation. He was detained pending trial. In September 2004, Karni pled guilty and cooperated. Karni acted as a middle man for Khan, a Pakistani, in illegally shipping both triggered spark gaps and oscilloscopes to Pakistan. Khan was indicted in April 2005. Karni received credit for his cooperation and was sentenced to 36 months in prison in August 2005.

Financial elements
The triggered spark gaps shipment was financed via letter of credit opened by Khan at the National Bank of Pakistan with the Standard Bank of South Africa.

Source: United States.

Case 11: Thiodiglycol

US Immigration and Customs Enforcement, Office of Investigations, through its predecessor agency the United States Customs Service, conducted an investigation into the illegal export of thiodiglycol, which is a precursor for sulfur-containing blister agents found in Mustard Gas. Thiodiglycol is a Chemical Weapons Convention schedule 2 chemical used in the production of sulfur-based blister agents such as mustard gas.
http://en.wikipedia.org/wiki/List_of_Schedule_2_substances_%28CWC%29

The investigation had revealed that Alcolac International, a United States based company, was shipping large amounts of thiodiglycol out of the Baltimore Port of Entry to several transshipment countries with a final destination to Iran. During the investigation, agents encountered a large shipment of thiodiglycol with a declared final destination to a "Far East country." Agents substituted the chemical with water and tracked the shipment from the United States through two transshipment countries and ultimately to Iran.

The investigation led the agents to multiple bills of lading for shipments to other companies with one marked "Transshipping is allowed." A review of the financial documents and related bank records revealed multiple Alcolac Letters of Credit noting preference for immediate payment in cash. Agents also discovered that subjects attempted to open new accounts under shell companies in the US to facilitate the exportation through a letter of credit.

Alcolac International pled guilty to two counts related to the illegal export of thiodyglycol. As a result the company was fined $437,594. Several additional individuals who took part in the illegal exportation of thiodyglycol were also found guilty.

Source: United States.

Cases involving other payment methods such as wire transfers and cash transactions

127. The following cases show how proliferators use wire transfers and cash transactions to support their activities. Case 13 also provides an example where a proliferator under-valued shipment in efforts to disguise the true nature of the goods being transferred.

Case 12: Sponsoring of students by a known WMD procurement entity

Voluntary information received from a Canadian intelligence agency indicated that **Individual 1**'s education in Canada was sponsored by a known WMD procurement entity located in **Country X** and that **Individual 1** was possibly a procurement agent.

Analysis of FINTRAC's information revealed that **Company A**, located in **Country X**, sent Electronic Funds Transfers (EFTs) to **Individual 1** and three other individuals (**Individuals 2, 3 & 4**). For some of the EFTs, the transaction was noted to be for "cost of study". All EFTs were sent to personal bank accounts and totalled about $140,000 US.

Other than all receiving funds from **Company A**, no apparent connections between the four individuals were identified. **Individuals 1 & 2** were found to be located in two different Canadian provinces, while no address was found for either **Individual 3** or **Individual 4**.

During the same period, a Large Cash Transaction Report (LCTR) received from a depository financial institution indicated that **Individual 2** also deposited about $10,000 US into his/her personal account. The LCTR further indicated that **Individual 2** was a student.

It is unknown why **Company A** would be funding the education of these four individuals. However, the research field in which **Company A** was involved indicated a possible association to a WMD program. In addition, at the time, **Country X** was known to sponsor students who agreed to study overseas in science and engineering programs. It was suspected that **Country X**'s objectives were to gain knowledge and expertise in some areas that could be useful for its WMD program.

Source: Canada.

Case 13: AMLINK

Overview

R. David Hughes was the president of an Olympia, Washington-based company, AMLINK. AMLINK was a medical supply company, but was involved in export of commodities that did not match its business profile.

In June 1996, the U.S. Customs Service began an investigation of the exportation of nuclear power plant equipment by Hughes and AMLINK from the Port of Seattle to Cyprus. According to a confidential source, the nuclear power plan equipment was to be shipped from Cyprus to Iran via Bulgaria, in violation of the U.S. embargo on Iran.

Investigation details

The equipment in question was nuclear power plant equipment that had been purchased in an auction by a Washington company, LUCON. The origin of the equipment was a Washington-based power company that led a consortium in the 1970s to develop a nuclear power station in Burlington, Washington. The power plant was cancelled in 1983, and the equipment was sold. Hughes worked with another individual, a Lebanese national with permanent U.S. resident status, Habib T. Abi-Saad to purchase the equipment from LUCON, export it to Cyprus and attempt to find buyers for the equipment. Hughes used a freight-forwarding company to assist in arranging the shipment.

The equipment was transported in three shipments from Seattle in 1995, which transited Rotterdam, before arriving in Cyprus. Although the documentation regarding the shipment did not indicate it included nuclear equipment, Cypriot authorities who inspected the cargo determined that it was nuclear-related equipment. The equipment was controlled by the Nuclear Regulatory Commission and required a license to export. Hughes did not request or receive such a license. Further, documentation/bills of lading were marked “for re-export only,” but there was no end destination or consignee was provided and the exporter provided vague/incomplete information to the freight forwarder on commodities involved.

Hughes was indicted and convicted of export of nuclear equipment without a license.

Financial elements

Payment was made via wire transfer from Abi-Saad into Hughes U.S. bank account; Hughes then paid for the equipment with a cashier’s check. The declared value of the shipment was under-valued with ten containers being exported with a declared value at $20,000, even though it would cost $2,000 to ship an empty container out of the country.

Source: United States.

Case 14: Use of financial information in a case of an attempted procurement

Information sent to the Canadian FIU identified individuals and entities that were suspected of being involved in the procurement of technology that could be possibly used for WMD programs.

It was alleged that **Company 1**, located in Country Z, received a request from Foreign **Individual X** for price information regarding a magnetostrictive sensor instrument for guided wave research, and declared Foreign **Company X** as the end user. **Company 1** informed Foreign **Individual X** that it could not sell the equipment due to Country Z's export restrictions. The equipment utilizes wave propagation and acoustic emissions to detect defects in piping systems. It is not specifically export-controlled, however, according to its design engineers it could have both nuclear and military applications. The following day, **Company 1** received a similar request for the same equipment from **Individual A** as a representative of **Company A**, located in Canada.

Company 1 noticed that **Company A** was copying Foreign **Individual X** on a series of e-mail exchanges.

Foreign **Individual Y**, the head of Foreign **Company X**, had created **Company A** and was listed as its General Director, while other Foreign **Company X** personnel occupied other executive positions within **Company A**.

Financial Elements
Analysis of the Canadian FIU's information revealed that a short time after that inquiry by **Individual A**, Foreign **Company X** ordered EFTs totalling over $100,000 US for the benefit of **Company A** over a period of about two months. The total amount appeared to cover the controlled item price plus an additional amount, possibly a commission for **Company A**'s services.

A few weeks later, **Company A** ordered one EFT, which appeared to have been an initial deposit, for the benefit of **Company 1**. One month later, **Company A** ordered another EFT for the benefit of **Company 1**, which covered the balance of the guided wave equipment price.

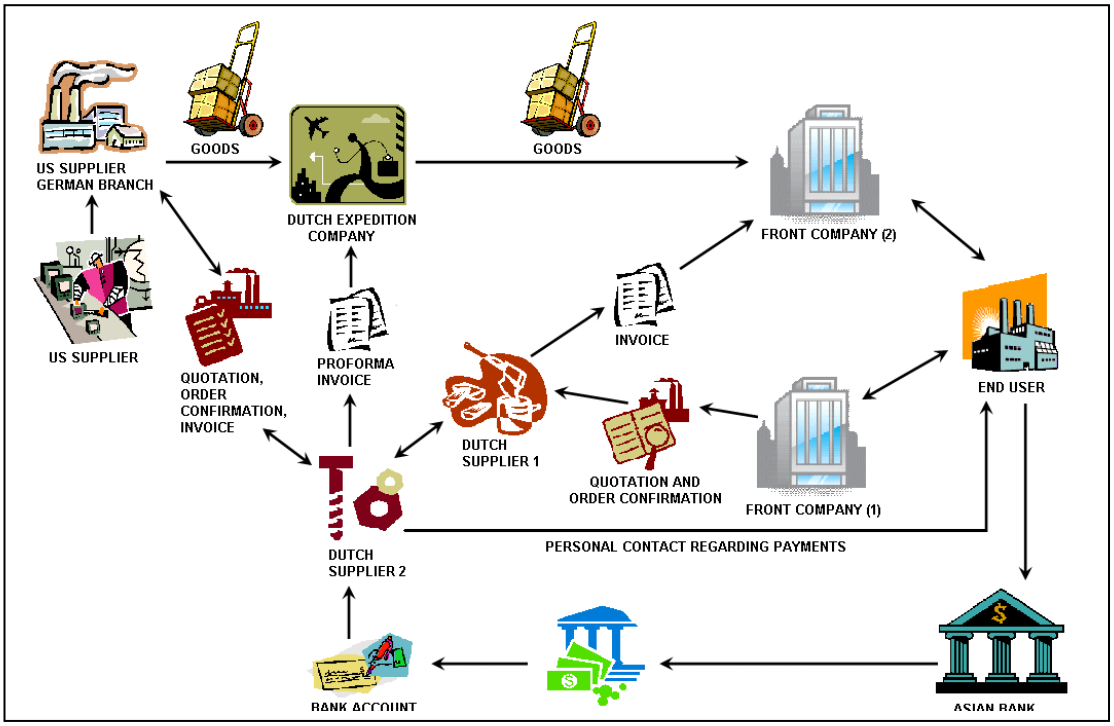
Investigation
An investigation revealed that Canadian **Company A** had been established by Foreign **Individual Y** specifically to market foundry software developed by Foreign **Company X.** Foreign **Individual X** is a member of the Research and Development department of Foreign **Company X** and was directing the purchase of the equipment through Canadian **Individual A**. Foreign **Company X** is a private research center and independent testing laboratory in the field of materials engineering, and is also involved in the development of materials engineering software for the foundry industry.

Individual A was described as "Management Executive", and operated **Company A** on behalf of Foreign **Individual Y**. This made it possible to distribute Foreign **Company X**'s foundry software to customers in Country Z as a means of circumventing its regulations.

Individual A and Foreign **Individual Y**, together with a third representative of Foreign **Company X**, were arrested while traveling to Country Z to receive training on the guided wave sensor.

Source: Canada.

Case 15: BANK BRANCHES



The case study clearly shows the difficulties in discerning the true purpose of trade when an authorization request is separated from the actual delivery of the goods.

The Dutch **Supplier 1** was contacted by two separate front companies, both located in an Asian jurisdiction of proliferation concern. The invoice was sent to one **Front Company A** in the jurisdiction of proliferation concern but the Dutch **Supplier 1** received the quotation and the actual confirmation of the order from another front company, **Front Company 2** (**Front company 1** and Dutch **Supplier 2** had personal contact with the **End User** in the jurisdiction of concern about the orders and payments.
This could be deducted from administrative information (emails and other documents) found at a research investigation at Dutch **Supplier 2**.

Dutch **Supplier 2** also contacted and confirmed that it could acquire goods form an additional supplier, **Supplier 3**, a branch located in Europe. The goods were then shipped directly by a regular Dutch expedition company to **Front Company 2**. The Dutch expedition company was unaware of the order confirmation and the invoice that was sent to the **US Supplier**, since it received a proforma invoice of Dutch **Supplier 2** directly.

The payments were received via wire transfers form the **End User's Bank** in the jurisdiction of concern, through a separate branch on the bank account of **Dutch Supplier 2**.

By using different companies (both in The Netherlands as in the jurisdiction of concern) that acted separately in different phases of the process, parties tried to disguise the actual circumstances of the trade transaction.

Source: The Netherlands.

Case 16: FRENCH CUSTOMS (EXAMPLE 1)

A French businessman is contacted by Pakistani nationals for the supply of dedicated electronic equipment for missile and/or drone tracking and guidance. He will acquire this equipment from an American intermediary, who will in turn order the components from an American manufacturer. Exportation of this sensitive equipment from the United States to France is authorised, provided that the latter country is the final destination. This operation is therefore subject to a prohibition on re-exportation from France.

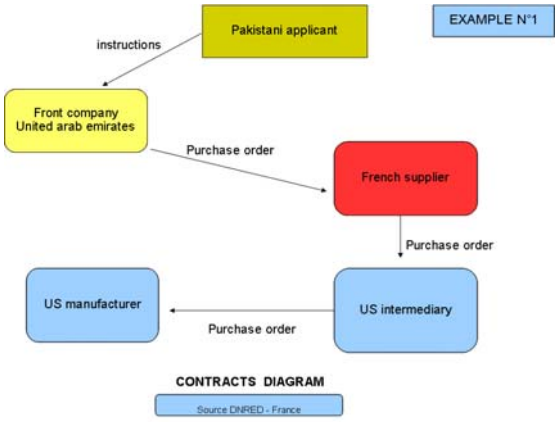
The equipment will not even be cleared from customs on arrival in France but remain in transit until immediate re-exportation to the United Arab Emirates, destined for a local front company acting on behalf of the Pakistani principal, which is affiliated with the Department of Defence (DoD) in Islamabad.

Contracts

A Pakistani purchasing network operating on European territory contacts a French industrialist to acquire electronic components that could be incorporated into tracking – ballistic control equipment for missiles or drones.

The French industrialist, who does not carry such equipment, contacts an American intermediary, which in turn places an order with an American electronic equipment manufacturer. On receipt, the intermediary decides to export the equipment to France, taking advantage of an export authorisation subjected to a restrictive condition prohibiting re-exportation from France.

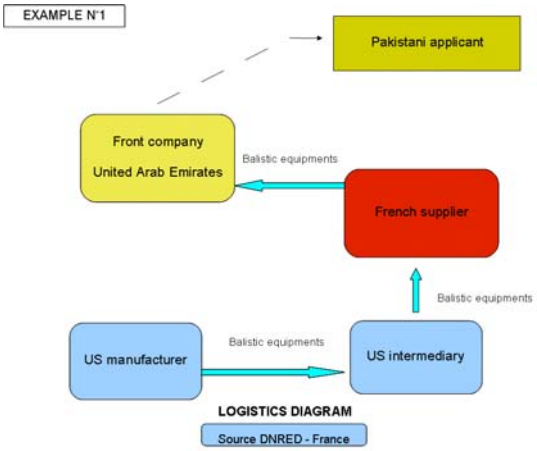
Meanwhile, a front company based in the United Arab Emirates, acting on behalf of the Pakistani principal linked with the Department of Defence, officially places an order with the French supplier.



Logistics

The equipment leaves the U.S. for France by express air freight.

It will not be cleared through customs in France. While in transit in Marseille, it is immediately re-exported to the front company in the United Arab Emirates, which assumedly then delivers the equipment to Pakistan.



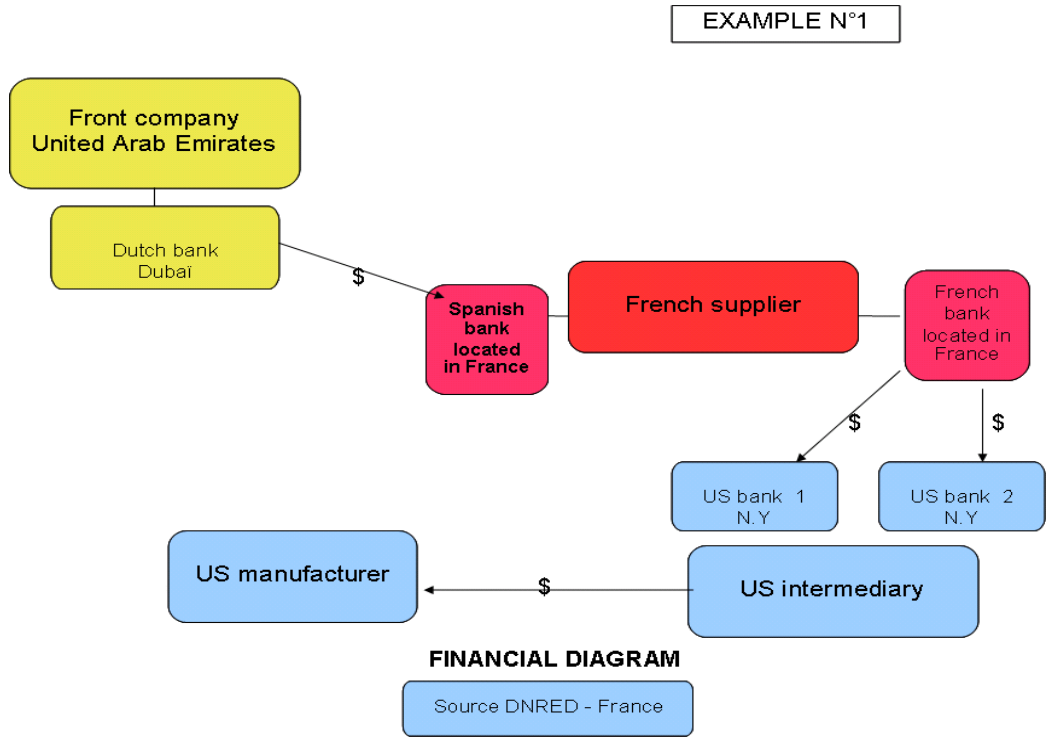
Case 16: (Cont'd)

Financial elements

This involves a direct financial transfer from Dubai (branch of a Dutch bank) to one of the French company's two banks (French branch of a Spanish banking group + branch of a French banking group).

One bank (branch of the Spanish bank) receives the money from Dubai and the other pays the American supplier, which itself has two banks, both domiciled in New York.

The transactions are split, both in France and in the U.S., between two banking institutions, seemingly unrelated because they belong to separate groups.



Source: France.

Case 17: FRENCH CUSTOMS (EXAMPLE 2)

Further to the action described in example 1, the Pakistani intermediaries acting on European territory established contact with a company specialised in designing and selling ballistic testing and programming equipment for missiles and drones.

This firm, very small (3 employees) yet capable of designing and producing high technology customised to satisfy its customers' needs, bought components from a Norwegian manufacturer specialising in the space industry (in which the firm had acquired financial interests) to then incorporate them into equipment exported to Pakistan. The shipments were split up to prevent inspection services from getting a comprehensive picture of the equipment (declared to Customs as electrical testing equipment), its characteristics and its sensitivity.

The equipment was exported without authorisation:

- either directly to Pakistan, destined for an import-export company fronting for the Department of Defence (DoD);
- or via an intermediary company based in the United Arab Emirates.

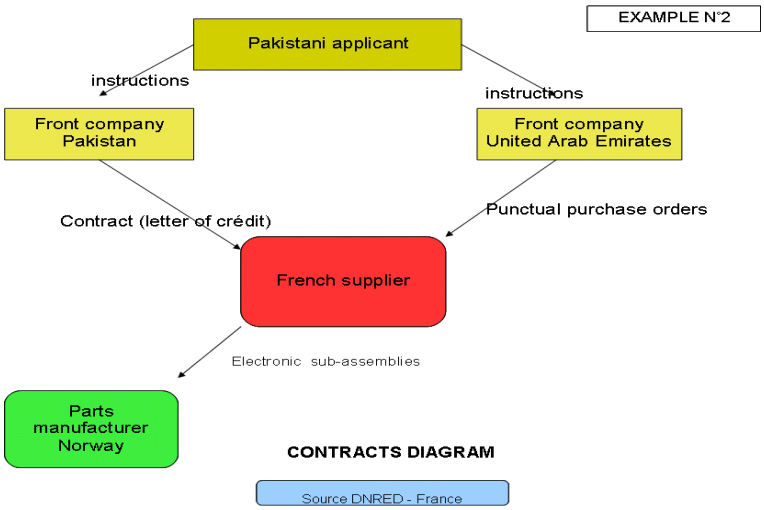
Searches were launched by French Customs at the firm's main office and at its employees' homes after an attempt to export one of the batches of equipment destined for Pakistan was intercepted at Roissy airport. These investigations confirmed the extreme sensitivity of all of the equipment (classified war materiel by the French Ministry of Defence) and the substantial involvement of the French company's director in the operations of the Pakistani military-industrial complex. The French company was declared dormant by its director. A claim was lodged by French Customs with French judicial authorities.

Contracts

The same Pakistani purchasing network (as in example 1), probably hoping to diversify and secure its supply sources in Europe, contacts a French businessman at the head of a small technological innovation firm (three employees) specialising in tracking and fire control equipment (missiles, drones). A contract is concluded concerning a complete calibration and guidance system for drones.

This project is divided into two separate but complementary orders. A first order is placed by a company based in Pakistan (55% of the system). A contract and letter of credit are drawn up for this order. The other part of the contract (45%) will be fulfilled through a succession of single orders by a front company based in the United Arab Emirates.

The two companies (Pakistan and UAE) both act on behalf of the same principal, i.e. Pakistan's Department of Defence (DoD). Down the line, the French integrator will procure part of the components required to develop the system from a Norwegian manufacturer which specialises in aeronautics and space and supplies the Norwegian army. The French integrator secures this procurement by taking a share in the Norwegian supplier's capital.

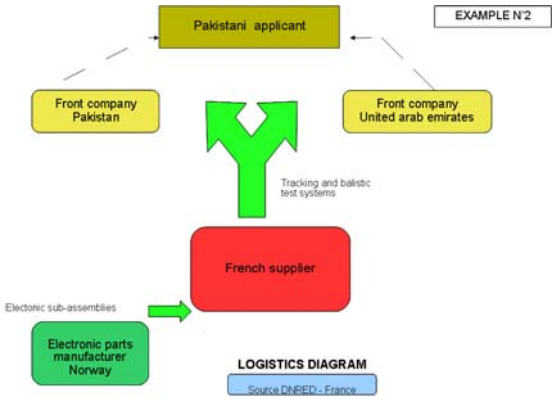


Case 17: (Cont'd)

Logistics

Upstream, the Norwegian manufacturer delivers its electronic subsystems to its French customer, which exports them directly in its name, one part to Pakistan and the other to the United Arab Emirates.

It is worth pointing out that, as is generally the case in such affairs, the real nature of the goods and their sensitivity were obscured by the innocuous-looking commercial wording of the customs declaration (e.g. electrical equipment).

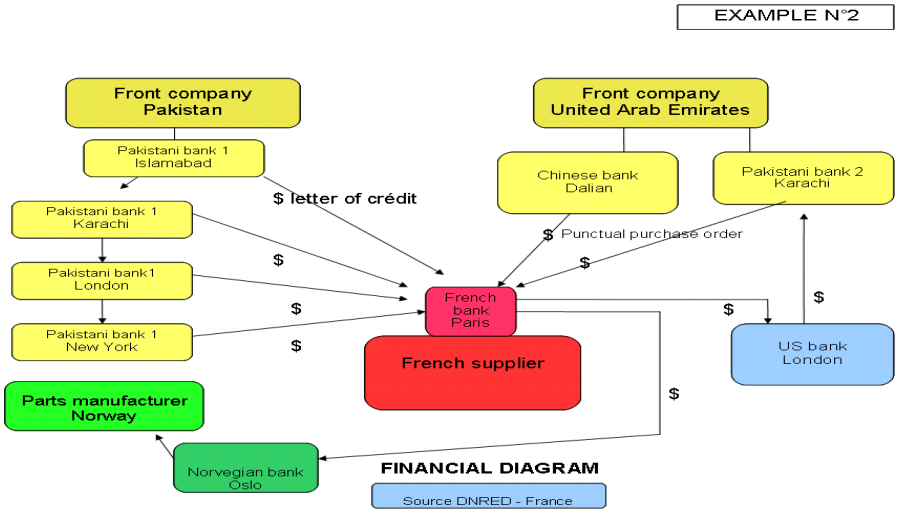


Financial elements

The financial diagram is highly instructive, because it shows the range of financing possibilities behind an act of organised proliferation. The Pakistani principal will go through two separate financing networks: 1) (right-hand side of the diagram) One network will put money into its front company in the United Arab Emirates and funnel the payments for single orders through a Chinese or Pakistani bank. Interestingly, the Pakistani customer indicates to the French seller that an American bank in London is to receive the kickback payments; and 2) (left-hand side of the diagram) The Pakistani buyer will use the letters of credit destined for a single French bank, where the French seller has domiciled its accounts.

These letters of credit will transit through four branches of the same Pakistani banking group (other that the one used by the front company in the United Arab Emirates) located in Islamabad, Karachi, London and New York, respectively.

The advantage of this scheme divided into two distinct parts is that the left hand doesn't know what the right hand is doing. However, all of the operations (left hand and right hand) were linked to a single French bank, a linkage that facilitated the French Customs' investigations. In addition, this French bank effected the payment of the electronic component orders placed with the Norwegian manufacturer via a Norwegian bank in Oslo.



Source: France.

Case 18: FRENCH CUSTOMS (EXAMPLE 3)

Information passed on by a French intelligence service reported visits by interns of country A to the main office of a French company based near Paris. This extremely dynamic company was headed by an independent industrialist, also the director of another firm. The two companies specialised in designing and manufacturing very high-tech dedicated products for ballistic applications. Concerned here were calibration tables for missile guidance systems that only found their equivalent at a Swiss supplier and an American supplier. In other words, the French industrialist headed one of the three specialists world-wide in that area.

The following facts also attracted the service's attention:

- This equipment was systematically declared free for export (neither licence nor authorisation for war materiel exports) under such surprising customs descriptions as electrical cabinets or kinaesthetic apparatuses.
- The buyers of this equipment were located in Pakistan, in country A and in country B.

French customs officers conducted an "in the act" (*flagrant délit*) interception at Paris' Orly Airport, with the support of their specialised counter-proliferation intelligence and investigation service. A machine was seized for examination at the time of the attempted export. The examination immediately confirmed at a minimum the dual civil and military nature of the equipment, whose destination was a ballistics research institute located in country A.

The searches conducted on the company's premises revealed that:

- Several machines had been exported illegally to those sensitive countries, either directly by one of the two French industrialist's companies or through the intermediary of a front company that received a commission for appearing to be the official seller of certain machines destined for various institutes of country A. The front company was also mentioned on the contracts, the letters of credit and the customs export declarations, whereas everything had been negotiated and organised by the French industrialist.
- Analysis of the equipment's technical characteristics found that it classified either as war materiel (therefore subject to a war materiel export authorisation) or as a product on the list of dual-use items (export licence - category 2B1 of the European Union's Community regime regulation).
- Hearings of the implicated companies' executives underlined the French industrialist's deliberate intention of circumventing existing export restrictions for his sensitive goods, whose strategic and military nature he knew perfectly well. In view of the potential buyers of the equipment, the industrialist knew that he could not obtain the necessary authorisations from French authorities. That was why the equipment was falsely declared in customs at exportation and why a front company in France was used in order to mask the real seller.
- As for the financial side of these sales, apart from the country A or Pakistani buyers' direct payments to the industrialist's companies by conventional letter of credit, most of the transactions were effected via the front company, the intermediary through whose accounts the money merely passed before the total, after an average 3% commission was skimmed off, was paid into the industrialist's companies' various accounts and then finally transferred to a financial structure belonging to the industrialist.

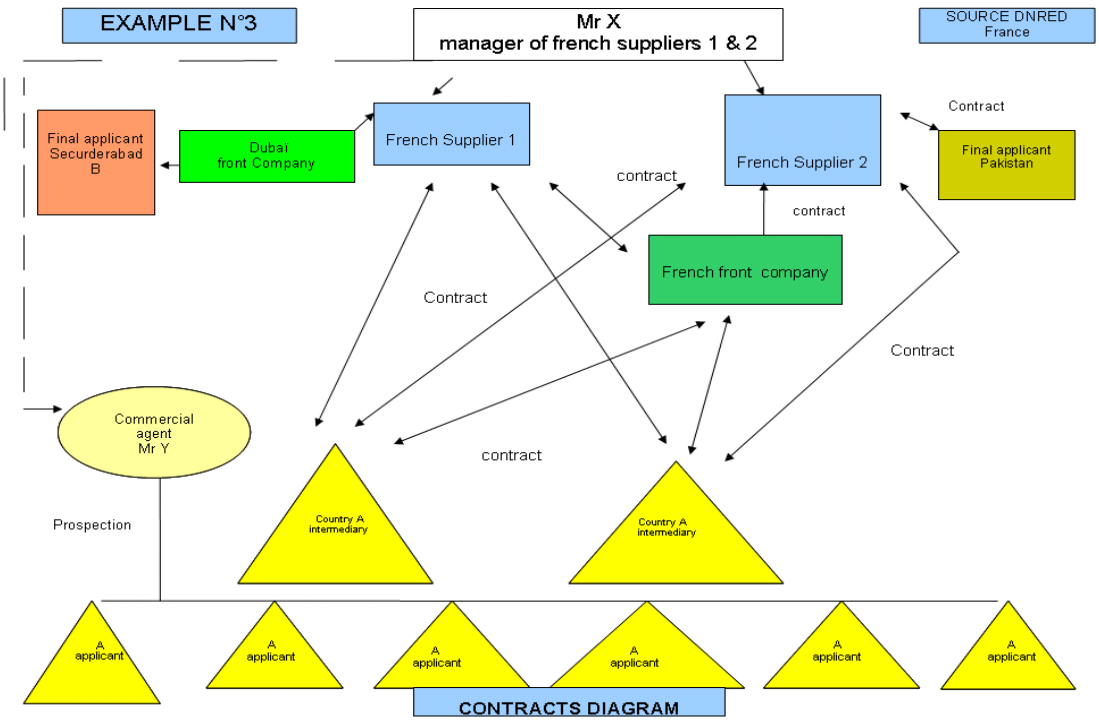
Case 18: (Cont'd)

Contracts

A French industrialist decides to set up business in at-risk countries – Iran, Pakistan, country A and country B – for which he knew he could not obtain the French authorities' authorisation to export sensitive equipment.

The investigation uncovered two kinds of commercial relations: 1) sales contracts entered into directly, with no intermediary (diagram upper right: Pakistani contract); or 2) contracts via various types of intermediaries:

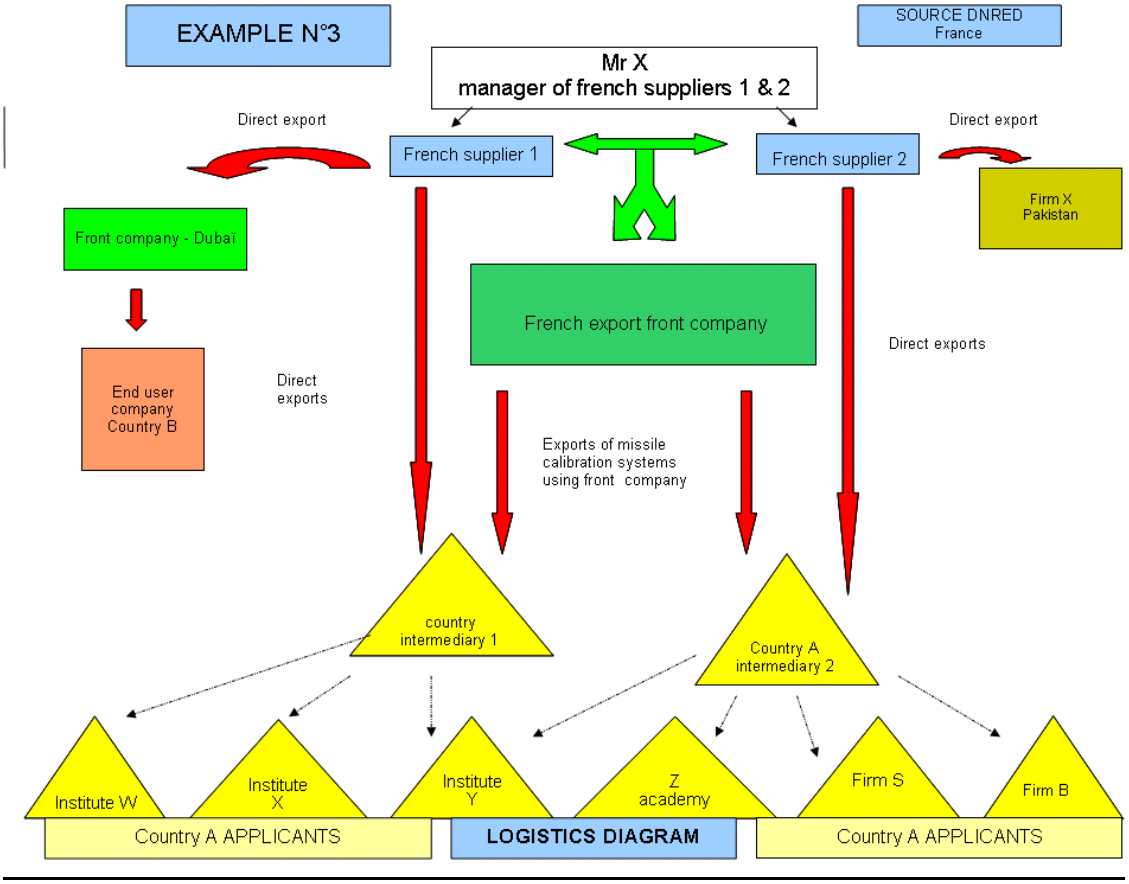
- Contracts via a commercial agent of country A canvassing the end users.
- Contracts via intermediary companies of country A disguising the real end customer (country A intermediaries diagram).
- Lastly, the most complex variant: use of a buffer company in France (French chain company diagram) to substitute for the industrialist and his company as the declared exporter of the sensitive goods.
- Another interesting point: a one-shot circuit for a B customer via a front company in the United Arab Emirates (diagram upper left).



Case 18: (Cont'd)

Logistics

The logistics diagram mirrors the contracts diagram. Direct exports by the companies controlled by the French industrialist to Pakistan and the United Arab Emirates, as well as to two A trading groups (intermediaries), responsible for forwarding the equipment to the final customers. The main exportation scheme used passes through a French front company mentioned on the customs declarations as the official exporter.



Case 18: (Cont'd)

Financial elements

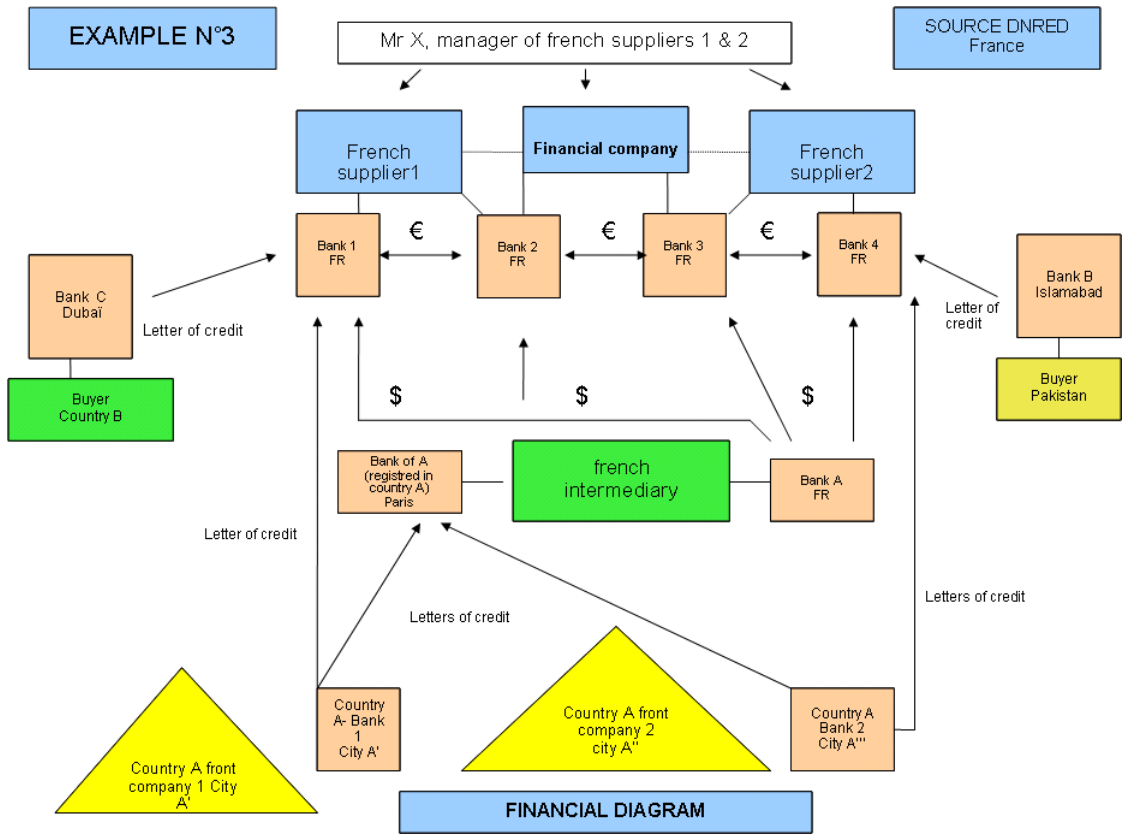
The financial diagram is highly enlightening as to the "left hand/right hand" model, in which the left hand doesn't know what the right hand is doing.

In general, it operates by letters of credit opened:

- Either directly by the foreign customer – Pakistani via an Islamabad bank or B using a Dubai bank – in the French companies' favour (suppliers 1 & 2).
- Or by A intermediaries in favour of the French front company (French chain company).

For the A operations, all of the letters of credit for the French front company are opened by two A banks at the Bank of A in Paris. This establishment then has those sums transit through a merchant bank in Paris, after skimming off an average 3% commission. The merchant bank, following instructions from the industrialist who organised the fraud, then transfers the sums to one or the other of his firms (suppliers 1 & 2), through one of their banks (four in all).

Even more interesting, the French industrialist had set up a financial structure (company) in the Paris area, totally independent of his companies, through which he could recycle that money as he wished, to his personal benefit.



Source: France.

4. COUNTER PROLIFERATION PURSUANT TO S/RES/1540 (2004)

128. S/RES/1540 (2004) was adopted unanimously on April 28, 2004 under Chapter VII of the UN Charter, with its objectives reiterated in S/RES/1673 (2006).

129. The resolution is the first international instrument to deal with the non-proliferation of all classes of WMD, their means of delivery and related materials in an integrated manner, and is the first international instrument to prohibit facilitating proliferation via financing. Operative Paragraph (OP) 5 of S/RES/1540 (2004) states that none of its obligations shall be interpreted to conflict with existing treaties. Annex 4 has a description of the most important conventions and other initiatives.

The key requirements of S/RES/1540 (2004)

130. S/RES/1540 (2004) represents the first time that the Security Council adopted a Resolution that broadly addresses the issue of WMD proliferation.

131. S/RES/1540 (2004) obligates States to take a wide range of actions to prevent and counter the proliferation of WMD. The main requirements of S/RES/1540 (2004) are found in OPs 1 to 3.[26] While those paragraphs set out multiple broad obligations, they are not prescriptive in nature, States are required to determine how best to implement the requirements of the Resolution, in accordance with their domestic laws and regulations and consistent with international law.

132. OP 1 prohibits States from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery.

133. OP 2 requires States to "adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them". Of particular importance for the FATF's consideration, States must have in place prohibitions which address WMD proliferation financing activity.

134. OP 3 requires that States establish and enforce effective domestic controls to prevent WMD proliferation, including accountancy and physical protection over related materials, border controls, brokering controls, measures to prevent illicit trafficking, and export controls (including controls over transshipment and re-export, as well as end-user verification). In terms of proliferation financing, it is important to note that OP3 also requires that States put in place controls on providing funds and services related to the export of WMD-related materials, such as financing.

135. OP 8(d). asks jurisdictions to work with industry and the public on their legal obligations under laws implementing S/RES/1540 (2004). This requirement enhances the effectiveness of measures that have been adopted.

---

[26] *Non-State actor*: individual or entity, not acting under the lawful authority of any State in conducting activities which come within the scope of this resolution.

Means of delivery: missiles, rockets and other unmanned systems capable of delivering nuclear, chemical, or biological weapons that are specially designed for such use.

Related materials: materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery.

5. KEY FINDINGS ON THE IMPLEMENTATION OF S/RES/1540 (2004)

136. Based on the survey[27] results and the findings of the 1540 Committee[28], the following information is useful in considering how jurisdictions are implementing their obligations pursuant to S/RES/1540 (2004).

Export controls

137. Export controls are a key feature of, and effective implementation is an essential first step to, countering proliferation. However, the 1540 Committee reported that only 80 jurisdictions had any export controls related to WMD-related items, and only 69 had associated penalty provisions, among nearly 130 States. However, every jurisdiction responded to the FATF survey as having an export control system and most reported as having specific dual-use legislation covering dual-use items and catch-all provisions covering goods known or suspected for WMD end-use but not listed as dual-use items under their export control system. Some jurisdictions have prohibited any support for the development of WMD, including prohibition on financing activities related to it. Annex 5 provides information on some elements that traditionally contribute to effective export controls. In general it does not appear from survey responses that any jurisdiction's export control regime imposes special obligations on financial institutions to detect proliferation financing, a conclusion that is supported by the findings of the 1540 Committee.

138. Reports to the 1540 Committee show that a number of jurisdictions worldwide have not yet implemented lists of controlled goods and end-user controls. A limited number of jurisdictions control the transit, trans-shipment, or re-export of WMD-related items; efficient control may be more difficult in free trade zones. Jurisdictions that responded to the survey indicated the importance of end-user controls, including the examination and verification of end-users by authorities using Embassy assistance, assurances by foreign governments, end-user certificates, international import certificates and pre-shipment audits. Most jurisdictions that responded to the survey use a coding system for controlled goods, including dual-use goods; however, the use of this system presupposes detailed technical knowledge which financial institutions do not poses.

Sanctioning proliferation activities

139. The survey results indicate that one jurisdiction has legislation containing provisions that specifically criminalise proliferation and financial assistance related to proliferation, and that most have taken significant action to implement specific proliferation legislation and controls. Most jurisdictions have not implemented legal provisions that criminalise proliferation financing, indicating in the survey response that specifically criminalisation of the activity of proliferation financing is already covered by complicity provisions in connection with provisions criminalising specific activities related to proliferation. Depending on the breadth of complicity provisions in a particular jurisdiction counter proliferation legal framework, additional legal provisions may be superfluous.

140. No jurisdiction reported any convictions or charges related to proliferation financing. All jurisdictions reported to have asset freeze requirements related to S/RES/1718 (2006) on North Korea and S/RES/1737/1747 (2006/07) on Iran. In addition, some reported having an ability to impose asset freezes for known proliferators beyond their implementation of these resolutions.

---

[27] A survey was sent to all jurisdictions on 1 October 2007 and this report reflects the responses of 20 jurisdictions.

[28] Countries must report on their implementation of S/RES/1540(2004) to the 1540 Committee. The 1540 Committee's report to the Security Council was based on answers from 129 States (136 by August 2007) and the EU. This report, along with country reports are published on the 1540 Committee's website *http://disarmament2.un.org/Committee1540*. A forthcoming report of the 1540 Committee is due by 31 July 2008.

141. While some jurisdictions consider anti-terrorism laws to be sufficient in satisfying their obligations to prohibit proliferation by non-state actors, it should be considered if such legislation is applicable in all cases. For example, the 1540 Committee identified that non-state actors may not necessarily proliferate for terrorist purposes, or their activities may not lead to facilitating a terrorist act[29].

142. The could also be issues concerning the applicability of money laundering legislation when proliferation financing is derived from legitimate sources and is not connected to the proceeds of crime. Terrorism financing legislation may not be applicable if the financing does not ultimately result in contributing to a terrorist act. Again, the 1540 Committee has expressed to the Security Council its concerns with regards to the use of AML/CFT legislation, that it may not be sufficient to fully implement OP 2 requirements[30].

143. The FATF survey indicated that few countries have taken measures to monitor the activities of trade intermediaries, for example trading companies, freight forwarders, etc. One jurisdiction reported having legislative measures against proliferation through brokering and transport. In this example, a broker must obtain a permit for the trade with goods that are or might be destined entirely or in part for the purpose of WMD. One jurisdiction reported that it requires customs brokers, depot and warehouse operators to be licensed by customs authorities. One jurisdiction reported that freight forwarders are subject to a license/registration system.

Enforcement

144. Effective implementation of S/RES/1540 (2004) requires a significant amount of public resources, and it appears that jurisdictions are implementing a legal framework to deter and detect proliferation. However, the effectiveness of enforcement measures may differ from jurisdiction to jurisdiction. In its report, the 1540 Committee identifies a number of issues, and provides its recommendations concerning effectively maintaining and enforcing: border controls; export controls; licensing; controls related to items and controls related to transactions.[31] Annex 6 provides a chart from the 1540 Committee report that indicates that while a number of jurisdictions are enacting the necessary legislation for border and export controls, fewer have implemented appropriate enforcement measures.

145. Survey responses varied concerning the methods used by authorities to address the risks of proliferators diverting goods to circumvent export controls. The most elaborate responses noted the following as key elements used by the responsible authorities for detecting/preventing diversion:

1) Risk assessment.
2) Intelligence and information sharing.
3) Follow-up procedures to ensure products arrived at declared destination.
4) Legislative authority to ask for additional verification measures from an exporter, *e.g.* the proof of delivery through providing documentary evidence.
5) Ad-hoc verification after delivery by competent authorities, *e.g.* to check if goods are used for the intended purpose.
6) Authorisation for export of dual-use goods is followed by a letter informing company about the obligation to immediately notify the competent authority if conditions for the authorisation change, including if the company receives new information about the end-use of the goods, the end-user or re-export of the product.

29 United Nations (2006), Paragraph 40
30 United Nations (2006), Paragraph 41
31 United Nations (2006), Paragraphs 85 to 105

Exchange of information and outreach to private sector

146. Jurisdictions reported that information on proliferation is generally shared among competent authorities both domestically and internationally but on a case-by-base basis. Little mention was given to proliferation financing. Confidential information (names etc.) is exchanged domestically between limited authorities dealing with counter-proliferation and internationally in counter-proliferation forums. Some information is only exchanged between intelligence services. The EU has a system which requires Member States to provide all other Member States with information on denials of export licenses for dual-use goods. As a rule, the private sector is not privy to this information.

147. The survey results indicate that many jurisdictions are disseminating information about export controls publicly. In general, red flag indicators and typologies for manufacturers and/or export control and customs authorities as well as official targets etc, if existent, may be publicly available. This may, in some jurisdictions, include "countries of concern". Some information concerning critical countries, end-users, intermediaries and brokers may be shared with export control authorities (and part of this may be shared with the private sector on a case by case basis) while some of it will only be known by intelligence services.

148. Several jurisdictions indicated that they issue guidance concerning UNSCR-targeted persons and entities and other general information (see publicly available information under export controls) and AML/CFT indicators relevant to proliferation financing, while one jurisdiction doubted in general whether AML/CFT indicators could help detect proliferation financing. One jurisdiction reported that it provides a programme of outreach awareness-raising exercises with the financial sector on issues relating to proliferation more generally. These include seminars that highlight the importance of export controls and the relevance of these to financial institutions.

149. Some jurisdictions also mentioned that transport documents could help detect diversion, including the implementation of a safeguard provision covering competent authorities to receive documentation for goods arriving at the stated place of end-use. Some indicated that information on controlled goods held by international control regimes could be useful information for financial institutions to screen transactions for possible proliferation financing.

Financial measures in more detail[32]

150. Many survey responses suggest that CDD requirements may be the most useful AML/CFT requirements in countering proliferation financing. Some mentioned suspicious transaction reporting systems could be useful, and others referred in addition to the following requirements:

1) Record-keeping requirements.
2) Correspondent banking controls.
3) Prohibition on shell banks.
4) Reporting of large cash transactions.
5) Reporting of electronic fund transfers.

151. One jurisdiction reported that its financial sector would need consolidated information on companies that were denied export licenses. Guidance could help the financial sector in identifying industries deemed high risk that are not self-evident in addition to considering where goods and financial transactions are destined. Additional information concerning high risk individuals, entities and jurisdictions can be very useful for financial institutions.

152. Screening customer databases against lists of names, knowledge of customers' trading activities and knowledge of products, if available, are trade finance controls that could be most useful

[32] The following relies solely on information derived from survey responses.

in detecting and deterring proliferation financing. A financial institution that has some knowledge of the controlled goods lists and export restrictions may be in a better position to request additional information such as export licences, and provide guidance to clients on more complex transactions of trade financing.

153. Under normal circumstances financial institutions do not have a detailed knowledge of the underlying commercial transaction associated with a financial transaction undertaken for a client, in particular where there is no detailed documentary evidence used in the transaction, such as a letter of credit.

154. No jurisdiction reported to have any specific proliferation financing reporting for financial institutions, but several jurisdictions mentioned that reporting is encouraged[33]. However, in addition to electronic fund transfer and large cash transaction reporting, several jurisdictions mentioned that information may be reported under the suspicious transaction reporting system.

155. Jurisdictions generally reported that financial information could help counter proliferation and proliferation financing and provide useful information to ongoing investigations. There was some indication that information on financial aspects has proven to be useful in investigations on the infringement of export controls, and in one example the investigating authority will focus on financial aspects of trade to verify end-use and the true nature of the good. There was some indication of reports having been received by a financial intelligence unit (FIU) concerning entities and/or individuals suspected of being involved in proliferation financing activities. There was some indication that a financial audit had assisted in determining the extent of procurement of non-WMD controlled items and the involvement of others in the supply of dual-use goods.

156. Jurisdictions indicated that, in general, the following types of financial information could be useful to help detect diversion:

1) Information in any associated letter of credit.
2) All information on type of payment (letter of credit, wire transfers).
3) Information on financial transfers associated with commercial transactions, including specific information on parties to the transaction.

6. ISSUES FOR CONSIDERATION

157. The following section addresses the third objective, of the report: to identify measures (*e.g.* criminalisation measures, broader sanctions, activity-based financial prohibitions or controls or examining the use of financial intelligence) that could be considered in combating WMD proliferation finance within the framework of existing UNSCRs, such as S/RES/1540 (2004).

158. This study explains that proliferation financing poses a real and ongoing threat to the international financial system. Proliferators are using trade finance and other bank products to finance trade in proliferation sensitive items. However, proliferators use a variety of techniques, which are described in the report, to hide their true identities and their involvement in proliferation, as well as the true end-use of an item or an item's true end-user. Jurisdictions and financial institutions may remain vulnerable if these risks are not adequately considered.

159. The issues for further consideration by the FATF are presented along four broad categories: *i)* legal systems; *ii)* preventative measures; *iii)* awareness raising; and *iv)* investigations.

160. The analysis and observations contained in previous sections of this report suggests that financial measures could help in overall counter proliferation efforts, but the benefit of these measures

[33] Jurisdictions do require financial institutions to report on targeted financial sanctions pursuant to S/RES/1718(2006), S/RES/1737(2006) and S/RES/1747(2007).

will be very limited if more traditional counter proliferation measures are not effectively implemented and enforced. Effective proliferation financing prohibitions is one of several important elements that contribute to a jurisdiction's effective and comprehensive counter proliferation regime.

161. However, it is important to note that without a thorough implementation of controls to prevent the transfer and export of technology, goods, services or expertise, proliferation financing will be difficult to prevent and financial measures would not be useful.

Legal systems

162. S/RES/1540 requires jurisdictions to prohibit proliferation financing.

- There is limited evidence that jurisdictions have taken additional measures to criminalise proliferation and proliferation financing since the adoption of S/RES/1540 (2004).
- Most jurisdictions rely on complicity provisions and other provisions, such as terrorism financing provisions, to prohibit proliferation financing.
- There may be value in explicit criminalisation, including to:
  - Clarify the obligations on firms and financial institutions to be vigilant to proliferation and proliferation financing.
  - Enhance enforcement against proliferation and proliferation financing, including by establishing appropriate penalties.
  - Address financial activities not otherwise covered by export controls.
  - Provide a basis for financial institutions to report, when necessary, financial information related to proliferation financing to an appropriate competent authority within the domestic legal framework.
  - Provide a basis for competent authorities to receive, analyse and share financial information related to proliferation financing.
  - Properly cover intermediary activities, *i.e.* brokers.

163. Some jurisdictions are using targeted financial sanctions to prohibit proliferation financing, however most do not. There may be value to measures that create a domestic legal authority and capacity to implement targeted financial sanctions against individuals, entities and jurisdictions involved in proliferation financing. Such measures can serve to:

- Deprive proliferators of their assets and limit their access to the global financial system.
- Disrupt proliferation networks by publicly exposing designated individuals and entities.
- Provide detailed identifier information on designated proliferators, front companies and other associates, which could be used by financial institutions to effectively detect and prevent proliferation financing.

164. However, the use of targeted financial sanctions against proliferation financing has limitations. Automatic and manual screening through name based designation requires adequate and up-to-date identifier information for designated individuals and entities. This can be challenging for jurisdictions, which can result in false positives and failure to capture individuals and entities working on behalf of designated entities, or designated entities who have changed their names or other identifying information.

Awareness

165. While proliferation networks, including financing arrangements, use creative schemes to exploit unwitting actors, lack of awareness of proliferation and proliferation financing could contribute to the problem.

166. The majority of private sector entities do not knowingly engage in proliferation, want to be good corporate citizens and do not want to be involved in illicit activities. They avoid risks to their reputation and avoid having their assets unknowingly involved in proliferation.

167. Outreach by government to producers, sellers, transporters etc. on proliferation risks is critical, and already takes place to a high degree in many countries.

168. Outreach to the financial sector on proliferation financing risks does not take place to the same degree. When considering if and to what extent measures should be taken the nature of the services provided by the financial sector and the ability to detect proliferation finance must be taken into account.

169. Awareness-raising with authorities and persons/companies/financial institutions etc. may prove to be very useful. This would require a reasonable amount of resources for outreach, training or other cooperative activities, but may result in enhanced information exchange.

170. It may also be beneficial to outreach to those (*e.g.* lawyers, notaries, accountants, auditors) involved in the establishment, incorporation, purchase and audit of companies to make them aware of the use of front companies in proliferation networks.

171. Generally, there are limited educational, licensing, registration or oversight requirements for brokers. Flexibility of business operations enables illicit brokers to avoid restrictions by locating in a jurisdiction with little or no regulation of brokering services.

Preventative measures

172. Effective implementation of existing AML/CFT requirements, in particular CDD, record keeping, transaction monitoring, and due diligence with respect to correspondent banking relationships, are relevant measures for a financial institution to mitigate proliferation financing risk.

173. Given that the sources of funding for WMD proliferation can be legal or illegal, well-known indicators or “red flags” for money laundering may be relevant in cases where the source of funds is illegal. However, the risk of proliferation financing is more likely to be present in cases where the source of funds is legal but the end-user or type of goods involved is intended to be obscured. The structural differences between money laundering on the one hand and proliferation financing on the other hand should therefore be taken into account when considering the applicability of AML/CTF requirements.

174. Using existing AML/CFT controls against the threat of proliferation financing has the benefit to financial institutions of allowing them to rely on familiar concepts, processes and procedures to protect against a newly understood risk There may be value in:

- Considering adjustments to AML/CFT controls to adequately detect and prevent proliferation financing.
- Financial institutions applying AML/CFT controls in a risk based manner across all product lines, particularly trade finance.

- Effective use of CDD information by global trade services representatives engaged in trade finance activities, which may require additional training of these representatives in AML/CFT measures.
- Using any information contained in trade finance documentation to verify the goods that are being traded, the final destination, and the parties involved in the trade.

175. Information sharing is critical in enabling a financial institution to address proliferation financing risks. Government may consider providing additional information on threats and risks to allow financial institutions to assess the risks they face from proliferation financing and, where appropriate, to amend CDD and monitoring systems to mitigate the risk.

- Detailed information on entities designated through targeted financial sanctions can be particularly useful to financial institutions.
- Diversion of trade and financial payments through third parties and/or third jurisdictions.
- Jurisdictions with substandard export and financial controls.
- There may be useful public information for financial institutions that is currently made available by export control authorities.
- Information on high risk persons and entities, including front companies.

Investigation

176. Financial information can be useful in proliferation related investigations and prosecutions and relevant authorities should consider its use as a matter of routine in these cases. In particular, financial information is useful for:

- Contributing to uncovering proliferation activities when complemented by information held by competent authorities and other sources.
- Linking entities of concern together, especially given the increasing use of front companies and transhipment points by the proliferation networks in their attempts to evade export controls.
- Demonstrating diversion or infringement of export controls.

177. There are significant amounts of data that are received by financial intelligence units currently in relation to money laundering, terrorist financing and other illicit activity that could contribute to proliferation investigations.

178. There may be some value in reporting suspicions of proliferation financing or other reporting mechanisms.

179. Domestic information sharing mechanisms between government agencies are critical to combating proliferation financing. Given the international dimension of proliferation financing, effective mechanisms to share information between governments is also crucial.

7. BIBLIOGRAPHY

Dolan, John and Walter Baker (2007), *Users' Handbook for Documentary Credits under UCP 600*, No. 694, International Chamber of Commerce, Paris.

FATF (2002), *Report on Money Laundering Typologies*, FATF, Paris, *www.fatf-gafi.org.*

FATF (2003), *Report on Money Laundering Typologies*, FATF, Paris, *www.fatf-gafi.org.*

FATF (2006), *The Misuse of Corporate Vehicles, including trusts and company service providers*, FATF, Paris, *www.fatf-gafi.org.*

FATF (2007), *Guidance on the Risk –Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*, FATF, Paris, *www.fatf-gafi.org.*

Frantz, Douglas and Catherine Collins (2007), *The Nuclear Jihadist: the True Story of the Man Who Sold the World's Most Dangerous Secrets... and How We Could Have Stopped Him*, Twelve (Hachette Book Group USA), New York.

Gruselle, Bruno (2007), *Proliferation Networks and Financing*, Fondation pour la Recherche Stratégique, Paris, *www.frstrategie.org/barreFRS/publications/rd/RD_20070303_eng.pdf.*

Hinkelman, Edward G. (2002a), *A Short Course in International Payments: How to Use Letters of Credit*, D/P and D/a Terms, Prepayment, Credit, and Cyberpayments in International Transactions, 2nd edition, World Trade Press, Petaluma, California.

Hinkelman, Edward G. (2002b), *A Short Course in International Trade Documentation: The Essential Guide to Documents Used in International Trade*, World Trade Press, Petaluma, California and *www.worldtraderef.com.*

Hinkelman, Edward G. (2004), *Dictionary of International Trade*, 6th edition, World Trade Press, Petaluma, California.

Hinkelman, Edward G., K. Shippey and S. Putzi (2002), *Dictionary of International Trade: Handbook of the Global Trade Community*, 5th edition, World Trade Press, Petaluma, California.

ifs School of Finance and the International Financial Services Association (2007), *The Guide to Documentary Credits*, 3rd edition, text for the certified documentary credit specialist certification, ifs School of Finance and IFSA, Canterbury, Kent and Parsippany, New Jersey.

International Chamber of Commerce (ICC) publications, principally:

ICC (2006), *ICC Uniform Customs and Practice for Documentary Credits* (UCP 600), No. 600, ICC, Paris.

Other ICC publications relevant to this report include:

International Uniform Rules for Demand Guarantees (URDG 458), No. 458, ICC, Paris, 1992.

Supplement to UCP 600 for Electronic Presentation (eUCP), No. 500-3, ICC, Paris, 2002.

ICC Uniform Rules for Collection (URC 522), No. 522, ICC, Paris, 1995.

Incoterms 2000: ICC Official Rules for the Interpretation of Trade Terms, No. 560, ICC, Paris, 2000.

ICC Uniform Rules for Bank-to-Bank Reimbursements Under Documentary Credits (URR 525), No. 575, ICC, Paris, 1997.

International Standby Practices (ISP 98), No. 590, ICC, Paris, 1998.

International Standard Banking Practice for the Examination of Documents under Documentary Credits (2007 Revision for UCP 600), No. 681, ICC, Paris, 2007.

Jones, Scott (2005), *Black Market, Loopholes and Trade Controls: The Mechanics of Proliferation*, presentation delivered at the 2005 Carnegie International Non-Proliferation Conference, Washington DC, 8 November.

Palmer, Howard (1999), *Trade Finance Risk: Documentary Fraud & Money Laundering*, Amer Educational Systems.

United Nations (2006), *Report of the Committee established pursuant to resolution 1540 (2004)*, UN Security Council Committee established pursuant to resolution 1540 (2004), United Nations, New York, *www.un.org/sc/1540/committeereports.shtml*.

ANNEX 1: ELEMENTS THAT MAY INDICATE PROLIFERATION FINANCING

The investigative indicators below serve as a starting point to assist financial institutions in understanding the risk that customers, transactions or other account activity may be associated with WMD proliferation. They are not provided as definitive indicators that WMD proliferation is occurring, as a basis for automated screening, further work would be needed to develop such indicators.

Identifying characteristics that are useful to financial institutions as indicators for possible proliferation financing-related activity poses several challenges, for example:

- Given that the sources of funding for WMD proliferation can be legal or illegal, well-known indicators or "red flags" for money laundering may be relevant in cases where the source of funds is illegal. However, the risk of proliferation financing is more likely to be present in cases where the source of funds is legal but the end-user or type of goods involved is intended to be obscured. The structural differences between money laundering and proliferation financing should therefore be taken into account when considering how indicators could be used.
- Specific information on the risk posed by the end-user or counter-party involved, or technical expertise to evaluate the possible WMD use of goods involved, will generally be needed to fully understand the risk of proliferation financing for a transaction or a customer.[34]
- Proliferators use a range of sophisticated schemes to obfuscate their activities. For example the case studies show that proliferators have used layered letters of credit, front companies, intermediaries, brokers etc. However, existing case studies do not enable us to identify any single financial pattern uniquely associated with proliferation financing, though indicators, if available, may help to identify some of the methodologies used by proliferators.

Nonetheless, the typologies working group has endeavoured, as part of its study of this issue to identify, or adapt, possible indicators of proliferation financing.

It should be stressed that in trade individual financial institutions rarely deal with all counterparties involved, and may not be aware of the activities highlighted below. Some of the indicators also presuppose access to information, *e.g.* on customers of concern, which may not be routinely available to financial institutions, or which financial institutions lack the capacity to use. The list includes both indicators which could provoke initial suspicion of a transaction or customer, and also indicators which would be useful to remove "false positives" through further investigation, but which are not themselves a basis for suspicion. Finally, specific indicators might only be useful at particular stages of the transaction process *i.e.* during initial CDD, during transaction processing ("real time screening"), and after the transaction monitoring post transaction review in investigation of already-suspect activity. The opportunities and capacity to use indicators will therefore vary according to when they can be practically used.

[34] Where particular individuals, organisations or countries are the subject of WMD proliferation-finance sanctions programmes or export controls, the obligations on institutions to comply with those sanctions and export controls are determined by countries and are not a function of identifying potential risk. Violations of such sanctions may result in a criminal offence or sanctions in some jurisdictions if funds or financial services are made available to a target, directly or indirectly.

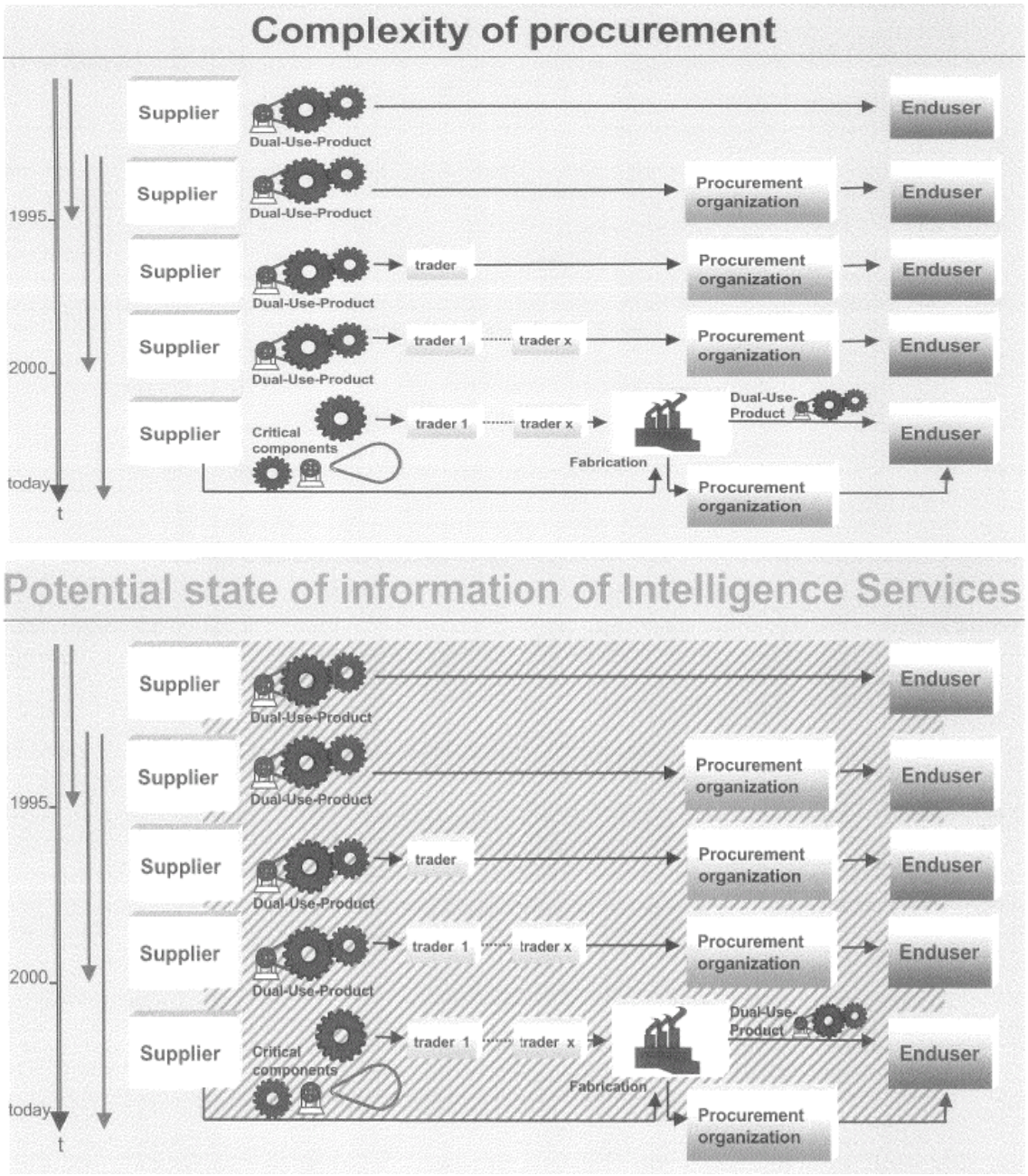
Indicators of possible proliferation financing

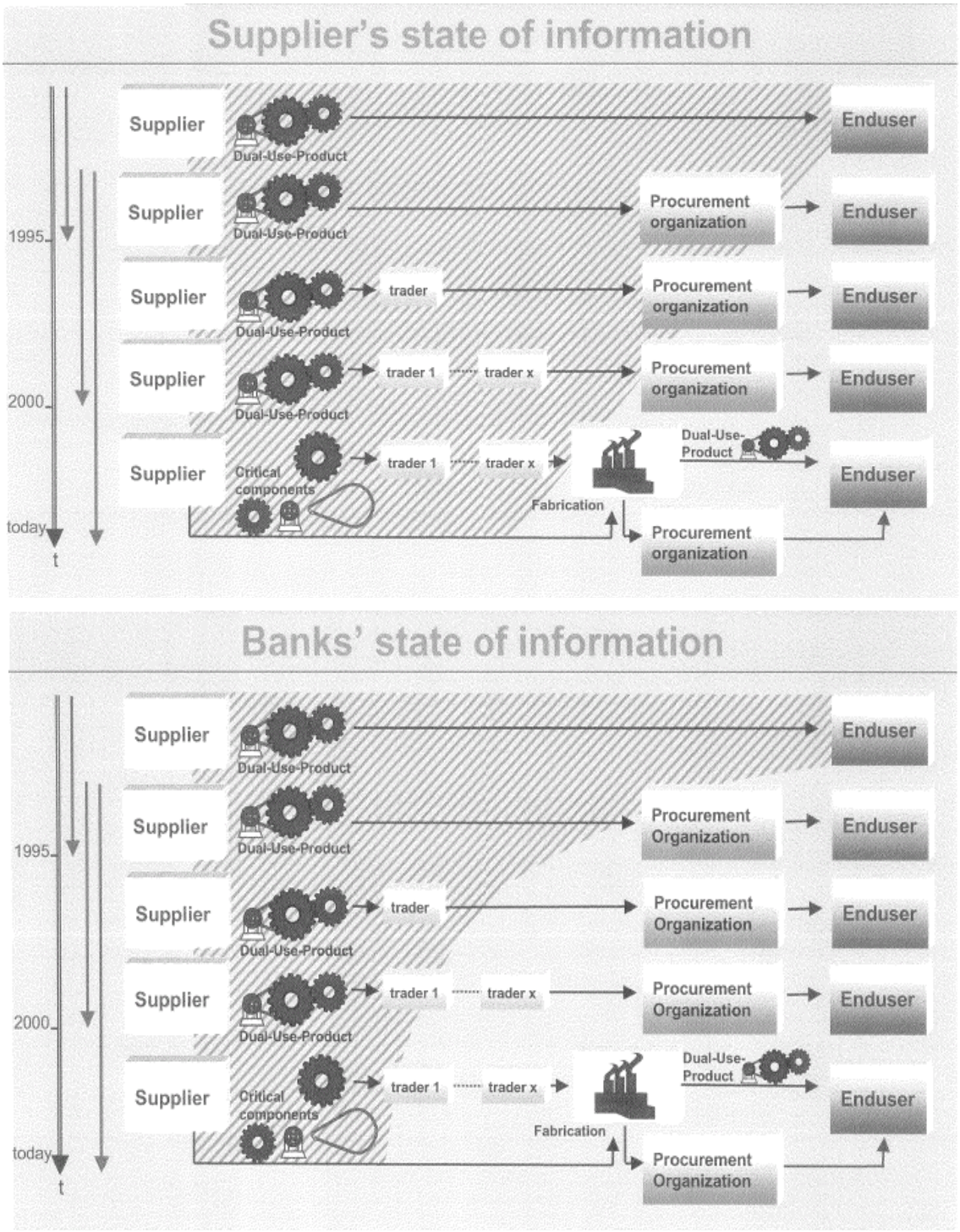
- Transaction involves individual or entity in foreign country of proliferation concern.
- Transaction involves individual or entity in foreign country of diversion concern.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- Transaction involves individuals or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (*e.g.* does the country involved normally export/import good involved?).
- Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (*e.g.* semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Customer activity does not match business profile, or end-user information does not match end-user's business profile.[35]
- Order for goods is placed by firms or individuals from foreign countries other than the country of the stated end-user.[36]
- Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
- New customer requests letter of credit transaction awaiting approval of new account.
- The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
- Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- Transaction demonstrates links between representatives of companies exchanging goods *i.e.* same owners or management.
- Transaction involves possible shell companies (*e.g.* companies do not have a high level of capitalisation or displays other shell company indicators).
- A freight forwarding firm is listed as the product's final destination.
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

[35] This indicator may also be apparent through credit-risk or other know-your-customer assessments, particularly if a customer is moving into a new line of business. At the transactional level, a transaction involving a product whose capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery, should raise concerns.

[36] In many cases, end-users may not be identified in documentation supporting a transaction. Additionally, wholesale companies routinely have this type of activity as a business model. In cases involving wholesalers, geographic or other factors should be considered in identifying risk.

ANNEX 2: THE COMPLEXITY OF PROCUREMENT NETWORKS OVER TIME





Source: Germany.

ANNEX 3: ADDITIONAL CASES OF PROLIFERATION

While the following cases do not provide any proven direct link of proliferation to the financial sector, they do provide some additional context as to the complexity of the detection of proliferation activity in general. For example, case 16 discusses how financial information may have been useful in investigating illicit activities that were disguised by proliferators through the use of cover names, front companies, false end-users and diversion etc.

Case 19: Customs authorities.

A suspected procurement network operating in Canada attempts to supply targeted entities in **Jurisdiction 1** with goods controlled under Canadian export laws. **Jurisdiction 1** is a jurisdiction of proliferation concern. A shipment of "industrial equipment" was presented for export at a major Canadian port by an exporter that was subject to a Canadian Border Services Agency (CBSA) national security/export control lookout due to suspected proliferation activity. Shipping documents were presented to CBSA indicating that the consignee of the equipment was an import/export trading company. Customs officials formally detain the shipment at the Canadian port for examination and export permit verification. The following documents are analysed:

- Export Declaration Form detailing the exporter, the consignee, the commodity, transportation details (routing, carrier) and the value. The exporter had listed the consignee as an Import/Export Trading Company located in **Jurisdiction 2**, a known transhipment hub. The goods are described as "industrial equipment" without further elaboration.
- Bill of Lading provides cargo shipping information.
- Invoice indicates the value of the "industrial equipment" is $500,000.
- Certificate of Origin indicates the goods originate from **Jurisdiction 3**.
- Export Permit is not presented for the goods (*Note*: Depending on the commodity, its origin and its destination, exporters may be required to indicate a General Export Permit number on their export declaration or they may be required to obtain an Individual Export Permit from competent authorities.

The exporter was the subject of a customs authority lookout (targeted shipment) for procurement activity and has a history of export control contraventions. The consignee was a trading company in a known transhipment country.

The description of the goods as "industrial equipment" was not specific enough to ascertain what the goods actually are or what their intended use might be. The value of the goods is high, which may indicate specialized use or high technological content.

Customs officials at the Canadian port are instructed to contact the exporter and obtain technical specifications for the goods and an end-use certificate from the consignee. The technical specifications reveal that the goods are a "five-axis milling machine", which, depending on their cutting capabilities, are controlled nuclear dual-use goods and subject to Canadian export control laws. The end-use certificate states that the goods are to be used in **Jurisdiction 2** at a wood working plant. Furthermore, a trading company is probably not the true end-user since it is likely the goods will be sold or re-exported. Open source searches indicate that the trading company in **Jurisdiction 2** is state-owned by **Jurisdiction 1**. At this stage, customs authorities have concerns that the milling machine is a controlled commodity and that it will be diverted or transhipped to the nuclear industry in **Jurisdiction 1**.

Canadian Customs officials ask export permit authorities what required export permits are required. Goods originating from **Jurisdiction 3** require a general export permit when destined to **Jurisdiction 2**. Since the exporter did not declare that the goods were being re-exported through Canada, customs authorities issue an administrative monetary penalty to the exporter for failing to properly declare this. There was not sufficient evidence to prove that the goods were destined for jurisdiction 2 and therefore the goods were not seized and were released for export despite suspicions on the part of customs officials.

Case 19 *(Cont'd)*

Numerous indicators maintain the concerns of customs authorities as to the true end-use and destination of the goods. Authorities continue to develop an intelligence file on the exporter and consignee. The intelligence file work-up includes reviewing various intelligence, enforcement, and commercial databases (including both open and classified sources). A review of the Canadian exporting company's previous exports revealed that it had already exported 8 five-axis milling machines with a combined value exceeding $4 million. As such, in addition to the current shipment, CBSA would now expand the intelligence probe to better understand the circumstances (*i.e.* end-users, routing, destination, etc.) surrounding all the shipments of five-axis milling machines (possible controlled nuclear dual-use goods).

Customs officials intercepted the Canadian exporter two weeks later at an airport returning from a trip to **Jurisdiction 2**. A secondary examination of his luggage is conducted under the authority of the customs laws and a bill of lading is discovered in his carry-on baggage, which describes the movement of a milling machine from **Jurisdiction 2** to an electronics company in **Jurisdiction 1**. Classified intelligence indicates that the electronics company is a known front company for **Jurisdiction 1**'s nuclear and missile industries.

In this example, CBSA was unable to seize the five axis milling machine, without proof of the true end-use and ultimate consignee in **Jurisdiction 1**. Proof for transhipment to **Jurisdiction 1** might include:

- Letters of credit from Jurisdiction 1's nuclear industry to the Canadian exporter;
- Financial transactions between the Canadian exporter, the trading company in Jurisdiction 2, the front company in Jurisdiction 1, and Jurisdiction 1's nuclear industry.
- Financial intelligence analysing complete financial proliferation networks linking all the various entities involved.

Source: Canada.

Case 20: Accelerometers

The United States Immigration and Customs Enforcement, Office of Investigations, in conjunction with the Defense Criminal Investigative Service (DCIS), conducted an investigation in which led to a federal indictment against a foreign national. The indictment was for conspiracy to commit offenses against the United States in connection to exporting Endevco 7270A-200K accelerometers, which are designated as a defense article on the United States Munitions List and cannot be exported from the United States without permission from the United States Department of State. The Endevco 7270A-200K accelerometer has many military applications including use in "smart" bombs, missile development and the measurement of nuclear and chemical explosives.

From April 2007 through October 2007, ICE agents conducted undercover operations, in which an identified foreign national conspired with agents to export the Endevco 7270A-200K accelerometers in violation of United States Export laws. Undercover agents were advised that if the items were delivered overseas in proper working order, larger orders would follow. Undercover agents along with identified suspects negotiated price, payment, and delivery terms of the accelerometers in furtherance of the conspiracy. Undercover discussions included the delivery of the accelerometers to either a third party country or the country of final destination. Financial terms were discussed between the Undercover agents and the violator utilising the formal financial sector through either an escrow account for payment or making payments through bank wire transfers.

The defendant has been charged under Title 18, of the United States Codes, Section 371, with conspiracy to Commit offenses Against the United States and faces a maximum penalty of five (5) years in prison and a $250,000.00 fine.

Source: United States.

Case 21: Shipping of electronics to a number of countries

Canadian **Individual A** is the sole owner of Canadian **Company A**, whose business includes the shipping of electronics to a number of countries. Canadian **Individual A** contacted Canadian **Company B** to purchase a number of computer chips (power amplifiers) designed for use in radar and satellite communication systems. These goods are dual use with potential military applications and are subject to export controls. **Individual A** reported the end-user as Canadian **Company C** and refused to allow Canadian **Company B** to meet with representatives of Canadian **Company C**. Canadian **Individual A** ultimately cancelled the order entirely.

Significant suspicions were raised on the part of Canadian **Company B** once Canadian **Individual A** refused to coordinate a meeting with Canadian **Company C**. The addresses given by Canadian **Individual A** on the US Traffic in Arms Regulations (ITAR) form for both the purchaser (Canadian **Company A**) and the purported end-user (Canadian **Company C**) were the same.

Further investigation revealed that Canadian **Company C** is actually based overseas, and is also run by Canadian **Individual A** and another person. Had the purchase of computer chips from Canadian **Company B** gone through, the items would have been shipped through Canada overseas.

The following year, an intermediary for the military of a foreign country requested a purchase of US-origin military-grade night-vision cameras from the same Canadian **Individual A**. The cameras have potential dual-use WMD applications in addition to regular military use and are subject to export-controls. Canadian **Company A** placed an order for one camera with US **Company 1**. US **Company 1** notified US authorities, who confirmed that the camera, after arriving in Canada, was then re-exported overseas and is currently located near an important nuclear site in a country of proliferation concern.

In addition, Canadian **Individual A** has been involved in other procurement deals designed to circumvent US export restrictions using Canadian **Company A**. For instance, Canadian **Company A** is now believed to be in the midst of procuring F-5 fighter aircraft spare parts from US **Company 2**, also on behalf of Foreign **Company X**, purportedly for a foreign Air Force. Canadian **Company A** has also attempted to re-label a US-origin airplane propeller as originating in another country in order to avoid prohibitions regarding shipment and re-export of US-origin goods. Although this particular shipment was stopped by Canadian authorities, other similar orders have been carried out. Canadian **Company B** has also fielded requests for other military-related goods, such as helicopter parts and jet fuel, although it is not known if these particular orders have been completed.

Source: Canada.

Case 22: Use of intermediaries to circumvent export restrictions

Canadian **Company A** deals in medical products and laboratory equipment and was in contact with Foreign **Company X** regarding the sale of multiplexers and potentiograph laboratory equipment. Foreign **Company X** is a procurement entity associated with a foreign nuclear programme of proliferation concern. Inquiries revealed that Canadian **Company A** has ongoing business dealings providing potential dual-use goods to a number of foreign enterprises, including Foreign **Company Y**. Foreign **Company X** is known to utilize Foreign **Company Y** as an intermediary, as part of its deceptive practices to avoid revealing the foreign nuclear programme as the end-user of purchased equipment. Goods are instead described as being for "educational purposes".

Further investigation revealed that the proprietor of Canadian **Company A**, Canadian **Individual A** regularly engaged in deceptive practices to conceal the end-user of dual-use equipment. Some deceptive techniques used in this particular case include the following:

- **Individual A** frequently provided the name of a Canadian University as the end-user for US-origin and other goods, despite having no actual connection with the university. The products would then be re-shipped to various foreign countries via commercial courier, with the description "laboratory equipment" or "medical instruments" given on the customs declaration, regardless of the true nature of the product being exported.
- Canadian **Company A** falsified documents in order to hide US-origin goods, re-labelling them as Canadian products manufactured in a south-east Asian country in order to permit export to embargoed countries.
- Canadian **Company A** exploits the fact that a country's export authorities generally do not inspect exported items as rigorously as imported items.
- Canadian **Company A** exploits a loophole in export reporting requirements for goods valued at less than $2,000.00 dollars, by re-invoicing products at a far lower value to avoid having to complete a paper export declaration.
- Canadian **Company A** is also involved as part-owner of Foreign **Company Z**, which it uses as the principal point of transit for goods going from Canada to overseas.

In addition to a number of potential nuclear/WMD dual-use exports to the companies noted above, Canadian **Company A** also conducts business with several other entities of procurement concern. These entities have been connected to procurement activities on behalf of various nuclear/WMD programmes in different countries of proliferation concern. Canadian **Company A** is currently the subject of a joint investigative effort by Canadian agencies aimed at uncovering the nature and extent of its procurement activities on behalf of the nuclear/WMD programmes of several high-interest countries.

Source: Canada.

Case 23: Illicit Brokering

A suspected procurement network operating in Canada aimed to supply entities in a jurisdiction of proliferation concern with controlled and strategic goods.

While executing a search warrant related to an offence of the *Customs Act* and the *Export and Import Permits Act* at the business address of the Canadian exporter, Customs authorities uncover shipping documents and commercial invoices related to a shipment of titanium-stabilized stainless steel tubes with an outer diameter of 750mm and a wall thickness of 2.5mm (controlled under 6-6.C.9 of the ECL). This shipment was not related to the offence being investigated. The documents related to this shipment indicate the tubes were manufactured in a European country; purchased by the Canadian company; moved by rail to a second European country; loaded into a maritime shipping container; shipped to a Free Trade Zone and once there, re-manifested and shipped to the jurisdiction of proliferation concern.

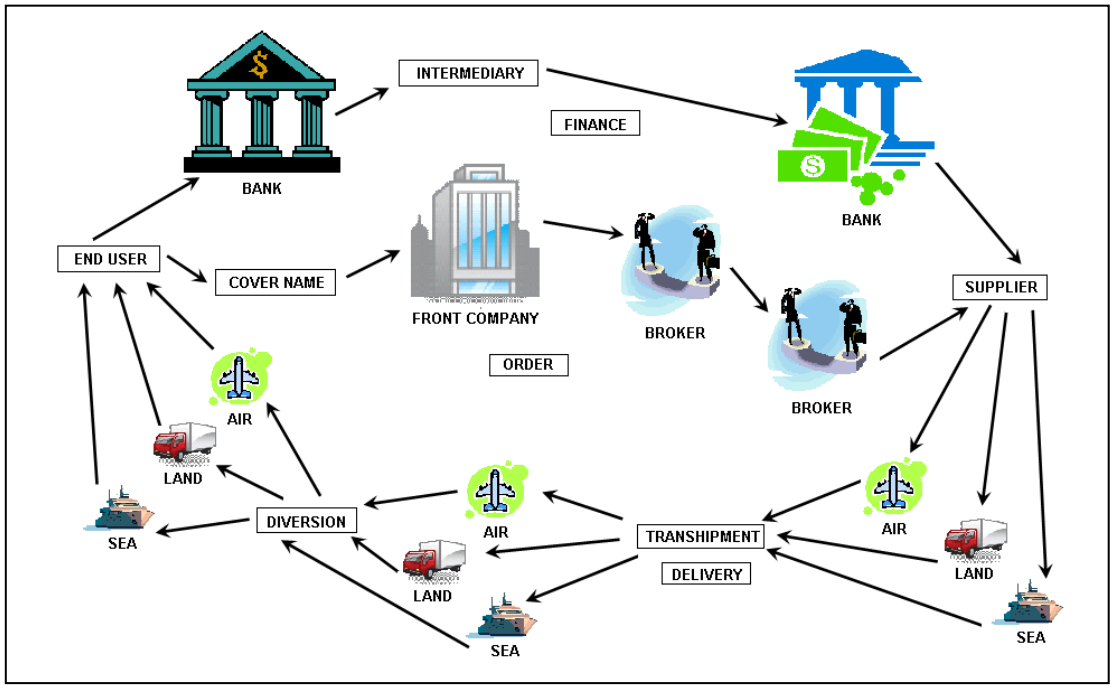
CBSA did not have enough evidence to enable it to act upon this illicit brokering activity. Furthermore, the above example is based on the fact that CBSA authorities had obtained a search warrant on an unrelated matter. If CBSA had not been searching the business records, this infraction would have gone undetected. However, financial information could have formed the basis for an initial investigation.

Source: Canada.

Case 24: Traditional counter proliferation making use of financial information

This diagram represents the procurement process and the start point for an analysis of proliferation networks. Counter proliferation has traditionally focussed on the bottom two aspects of the process.

This model can be used to describe purchases made on the open market and transfers between proliferators.



When purchases are made on the open market only a few entities within the diagram will be aware of what they are doing. In some cases only one entity will know. It is unlikely entities within the delivery or finance part will have sight of what is occurring. For example, it may be that only the end-users and the representative of the front company that are aware of the true destination and end-use for the goods.

When the transfer is between proliferators more of the entities involved will be aware that they are engaged in illicit activity. However these transactions still utilize commercial practises and routes some entities involved in the procurement and transportation may be unaware of that occurring. For example while the entities representing the supplier and end-user – the middle part of the chain would be aware the transfer is associated with a WMD or BM programme. They may choose to transport the goods by commercial carrier who would be unaware of the nature of the transfer.

Source: United Kingdom.

Case 25: Kahn

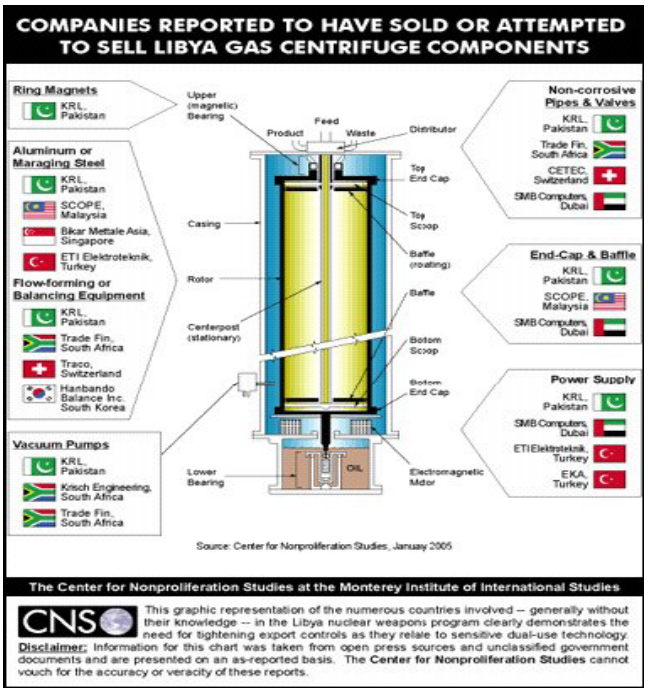
The Khan-case (which consists of several different proliferation cases over a long period) concerned nuclear weapon programs in several jurisdictions of proliferation concern. The process of proliferation for each item to be constructed consisted of many steps in order to disguise the activities of the network and the true nature and end-use of the goods. Many individuals, companies and countries were – knowingly or in good faith – involved. There is not much published concerning the financing in the Khan proliferation networks, but at least the following is mentioned in "Proliferation Networks and Financing" by Bruno Gruselle (Fondation pour la Recherche Stratégique, March 2007):

"Although some operations appear to have been settled in cash, others were settled through international transfers within the framework of duly established contracts. For example, this is the case for the contract made between the *Gulf Technical Industries* (GTI) company and SCOPE, for an amount of 13 million dollars."

"In terms of the financial organization, the few data available highlight two types of transaction:

- Inter bank: for remuneration of agents or suppliers outside the network. In other words, transfers between suppliers, intermediaries and/or front companies. Thus, the contract between SMB and SCOPE appears to have been financed conventionally, probably through letters of credit or bills of exchange.
- Cash transactions within the network and with customers. The amounts thus obtained (possibly in several payments) could then have been deposited in bank accounts of emerging or offshore countries before transactions were made between banks for final beneficiaries. Even if payments were made in cash, some operations could have been made through written contracts between Khan (and/or Tahir) and the intermediary concerned."

An illustration from the Centre for Non-proliferation Studies concerning gas centrifuge components to Libya illustrates the puzzle of proliferation of WMD – and also illustrates why detection is so difficult:



Many centrifuges are needed and a numerous components are required for each centrifuge. Several entities will be involved in the different networks used to acquire the components – including in payments and financing – but if someone sells e.g. 10 vacuum pumps to a country which is not a country of special concern one may not have WMD as the first thought.

Source: Gruselle, Bruno, (2007).

ANNEX 4: RELEVANT CONVENTIONS AND INITIATIVES

1. Nuclear Non-Proliferation

1.1 INTERNATIONAL TREATIES

Treaty on the Non-Proliferation of Nuclear Weapons (NPT)

The NPT aims at preventing the spread of nuclear weapons outside the five States which are recognised by the NPT as nuclear weapon States (NWS): France, the People's Republic of China, Russia, the United Kingdom, and the United States. These NWS have agreed not to transfer nuclear weapons or other nuclear explosive devices and not in any way to assist, encourage, or induce a non-nuclear weapon state (NNWS) to acquire nuclear weapons.

NNWS which are party to the NPT agree not to receive, manufacture or acquire nuclear weapons or to seek or receive any assistance in the manufacture of nuclear weapons. They also agree to accept safeguards by the International Atomic Energy Agency (IAEA) to verify that they are not diverting nuclear technology from peaceful uses to nuclear weapons. In return, NNWS are granted the inalienable right to use nuclear energy for peaceful purposes.

190 States are party to the NPT.

1.2 INTERNATIONAL ORGANISATIONS

The International Atomic Energy Agency (IAEA)

The IAEA is an independent intergovernmental organisation under the aegis of the United Nations and is the world´s centre of cooperation in the nuclear field. The Agency works with its Member States and multiple partners worldwide to promote safe, secure and peaceful nuclear technologies. Three main pillars – or areas of work – underpin the IAEA´s mission: Safety and Security; Science and Technology; and Safeguards and Verification. The IAEA reports annually to the UN General Assembly and, when appropriate, to the UN Security Council. It also works closely with the World Customs Organisation on security and trade issues, the Universal Postal Union on mail security issues, and Interpol and Europol in combating illicit nuclear trafficking.

The IAEA conducts inspections in countries that have safeguards agreements with a view to verifying that those countries are using nuclear material peacefully and providing recommendations on ways to improve the accountability and control of nuclear material. It also provides training at the international, regional and national levels concerning the security of nuclear and radioactive materials. In addition, the IAEA helps countries to obtain the necessary equipment for physically protecting nuclear and radioactive materials, including equipment that assists in the detection of cross-border smuggling of such materials.

In 1997, a model Additional Protocol to the NPT was produced by the IAEA. The adoption of the Additional Protocol is a voluntary measure for non-nuclear weapons states parties, designed to strengthen and expand existing IAEA safeguards for verifying that they only use nuclear materials and facilities for peaceful purposes.

1.3 EXPORT CONTROL REGIMES

The Nuclear Suppliers Group (NSG)

The NSG is one of four informal and voluntary export control regimes. It consists of a group of nuclear supplier countries which create Guidelines for exports of nuclear goods and nuclear related dual-use goods. The NSG Guidelines aim to ensure that nuclear trade for peaceful purposes does not contribute to the proliferation of nuclear weapons or other nuclear explosive devices, and to mitigate the risk of acts of nuclear terrorism. Participants seek to coordinate national export licensing efforts to prevent nuclear proliferation.

The NSG has 45 participants. The European Commission participates as an observer.

The Zangger Committee

The Zangger Committee, also known as the "NPT Exporters Committee", contributes to the interpretation of article III, paragraph 2, of the Nuclear Non-Proliferation Treaty (NPT) and thereby offers guidance to all parties to the Treaty. The main significance of this paragraph is that parties to the Treaty should not export, directly or indirectly, nuclear material and equipment to non-nuclear-weapon States unless the export is subject to International Atomic Energy Agency (IAEA) safeguards. By helping to establish and update control lists of nuclear equipment, the Zangger Committee helps to prevent the diversion of exported nuclear items from peaceful purposes to nuclear weapons or other nuclear explosive devices.

2. Missiles

2.1 EXPORT CONTROL REGIMES

The Missile Technology Control Regime (MTCR)

The MTCR is one of four informal and voluntary export control regimes. It aims to ensure the non-proliferation of ballistic missiles, cruise missiles and other unmanned delivery systems capable of delivering weapons of mass destruction. Partners of the MTCR seek to coordinate national export licensing efforts aimed at preventing the proliferation of these means of delivery by defining Guidelines for the export of relevant systems and related dual-use goods.
The MTCR has 44 partners.

3. Chemical Weapons

3.1 INTERNATIONAL TREATIES

The Chemical Weapons Convention (CWC)

The CWC prohibits all development, production, acquisition, stockpiling, transfer, and use of chemical weapons. It requires each State Party to destroy chemical weapons and chemical weapons production facilities it possesses, as well as any chemical weapons it may have abandoned on the territory of another State Party. The CWC does not prohibit production, processing, consumption, or trade of related chemicals for peaceful purposes, but it does establish a verification regime to ensure such activities are consistent with the object and purpose of the treaty.

The verification provisions of the CWC not only affect the military sector but also the civilian chemical industry, world-wide, through certain restrictions and obligations regarding the production,

processing and consumption of chemicals that are considered relevant to the objectives of the Convention. The most important part of the verification regime, however, are regular inspections which are conducted by the Organisation for the Prohibition of Chemical Weapons (OPCW). The CWC maintains only controls on chemicals, but does not control production technology.

183 States are party to the CWC.

3.2 International Organisations

The Organisation for the Prohibition of Chemical Weapons (OPCW)

The Organisation for the Prohibition of Chemical Weapons (OPCW) is responsible for the implementation of the Convention. The OPCW is mandated to ensure the implementation of its provisions, including those for international verification of compliance with the Chemical Weapons Convention. It also performs monitoring and conducts inspections to verify that declared chemical weapons production facilities have been deactivated and declared weapons stockpiles destroyed. Inspectors also verify the consistency of industrial chemical declarations and monitor the non-diversion of chemicals for activities prohibited under the Chemical Weapons Convention.
To address the threat of chemical terrorism (*i.e.* the use of chemical weapons by terrorists to threaten, injure, or kill people), the OPCW works towards chemical disarmament and to ensure that chemicals which are produced for peaceful purposes are not misused.

3.3 Export Control Regimes

The Australia Group

The AG is one of four informal and voluntary export control regimes which controls chemical and biological substances, as well as production equipment. The Group meets annually to discuss ways of increasing the effectiveness of participating countries' national export licensing measures to prevent would-be proliferators from obtaining materials for CBW programmes.

The AG has 41 participants including the European Commission.

4. Biological Weapons

4.1 International Treaties

The Biological and Toxin Weapons Convention (BTWC)

The Convention bans the development, production, stockpiling, acquisition and retention of microbial or other biological agents or toxins, in types and in quantities that have no justification for prophylactic, protective or other peaceful purposes. It also bans weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.

156 States are party to the BWC.

4.2 Export Control Regimes

The Australia Group (see section 3.3)

5. Conventional Weapons

5.1 EXPORT CONTROL REGIMES

The Wassenaar Arrangement (WA)

The WA is one of four voluntary and informal control regimes and concentrates on export controls for conventional arms as well as related dual-use goods and technologies. The WA contributes to regional and international security and stability and aims at preventing destabilising accumulations of conventional arms. The WA follows agreed Guidelines and Procedures, including the Initial Elements, the founding document of the WA. The 40 WA participating States implement export controls on the basis of WA control lists, agreed guidelines and best practices via national legislation and report transfers and/or denials of specified controlled items (arms and dual-use gods).

The WA has 40 participating States.

6. Other non-binding Measures

The Proliferation Security Initiative (PSI)

The Proliferation Security Initiative (PSI) is an informal network of cooperating nations that are committed to stopping the trafficking of weapons of mass destruction, their delivery systems, and related items to and from states and non-state actors of proliferation concern. The PSI was created in 2003 as an innovative complement to more formal non-proliferation regimes. More than 85 countries have endorsed the PSI Statement of Interdiction Principles (4 September 2003). PSI participating states develop a broad range of legal, diplomatic, economic, law enforcement, and other tools to assist in interdicting shipments of proliferation concern consistent with national legal authorities and relevant international law and frameworks. To date, PSI partner states have conducted over 30 interdiction training exercises involving more than 70 nations. These exercises increase the interoperability of PSI participants, improve interdiction decision-making processes, and enhance the interdiction capacities of participating states.

ANNEX 5: ELEMENTS OF EXPORT CONTROL SYSTEMS

Export control systems can vary from jurisdiction to jurisdiction, including each jurisdictions lists and due diligence for controlled goods. At a minimum, jurisdictions that implement export controls tend to licence the exports of certain goods, as identified by the four export control regimes. A truly comprehensive regime may require catch-all clauses. Many jurisdictions may consider the following elements in their export control systems:

Preventive export control

- International information sharing.
- National open source information (websites, conferences, seminars, etc.).
- Outreach activities to the private sector:
    - Legal basis
    - International sanctions and UN-resolutions
    - Procurement methodology
    - Countries/entities/organisations/persons of concern
    - Red flags
    - End-user/purchaser check

Export control

- Export authorisation.
- Special authorisation for certain products, *e.g.* weapons, chemicals or CBRN-material.
- Customs control – screening:
    - Licenses
    - Certificates
    - Shipping documents
    - Other documents
- Technical assessment of exported items
- Customs control – border:
    - Spot checks
    - Front companies
    - Diversion
    - Trans-shipment and transit cargo

Investigative export control authorities

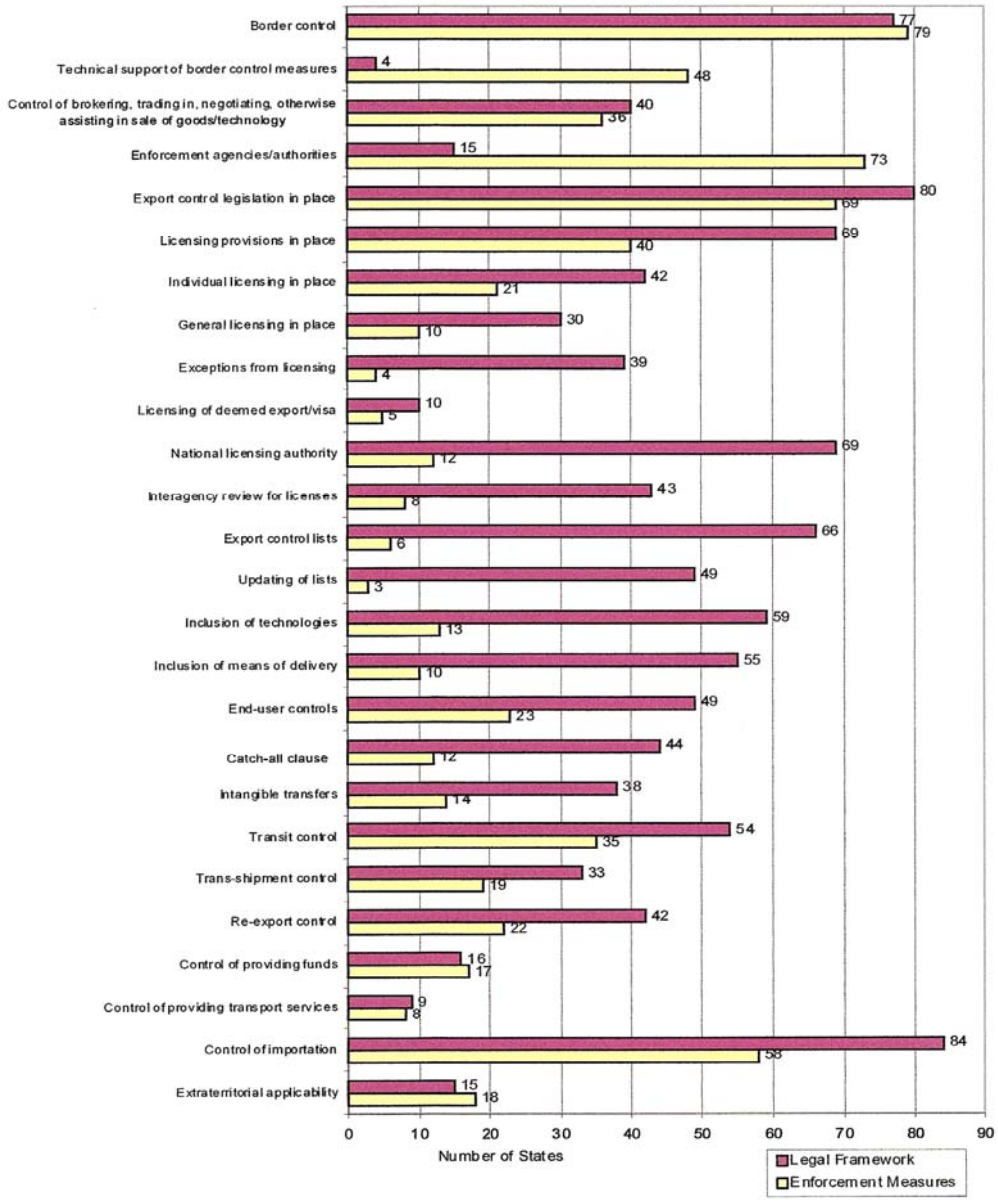
- Licensing authorities:
    - Applications
    - Denials
- Customs:
    - Authorisations
    - Surveillance
- Intelligence
- Security
- Police authorities
- Other public authorities

ANNEX 6: EFFECTIVE BORDER AND EXPORT ENFORCEMENT

Annex IX

States reporting on national legal framework and enforcement measures under paragraph 3 (c) and (d)

Border and export controls



ANNEX 7: INFORMATION IN DOCUMENTS WHICH MIGHT BE CALLED FOR AND PRESENTED UNDER A LETTER OF CREDIT PRESENTED AS PART OF A DOCUMENTARY COLLECTION

Note. Similar documents to those described below may be presented as part of documentary collection order, but unlike the L/C scenario *i)* without any reference to a letter of credit *ii)* the draft should not be drawn on the bank and *iii)* the bank will not be examining the documents for the same detailed consistencies.

The *Draft* or Bill of Exchange (not always required) provides formal evidence of debt under a letter of credit and is presented with all other documents unless stipulated otherwise. A Draft may contain information on:

- Value of Draft, date of payment and payment terms *e.g.* "at sight", "30 days after sight", "60 days after Bill of Lading Date".
- Date Exporter presents documents to the "available with" Bank (not normally required).
- Letter of credit reference number assigned by the Issuing Bank (if required by credit).
- Date the letter of credit was issued (not normally found on a draft).
- Name and address of the Issuing Bank (if the drafts are drawn on the issuing bank).
- Name and address of the bank on which the Drafts are to be drawn.
- Signature of an authorised signing officer of the Company and the Beneficiary's name as shown on the letter of credit.

The *Commercial Invoice* is the accounting document through which the exporter charges the importer for goods and services purchased. The Invoice gives details about:

- Merchandise weight, quantity and price and currency.
- The name and address of Exporter and the Importer.
- The number of copies presented and signed if required.
- The trade term listed, *e.g.* C.I.F., F.O.B etc.

The *Transport Document* (or Bill of Lading, Airway Bill, Railway Consignment Note) is a document issued by the carrier that describes the goods that have been accepted for carriage. In some forms, the Bill of Lading may also act as a document of title to the goods and should include information that is consistent with the letter of credit:

- Information on the merchandise (usually a general description).
- The points of loading and discharge.
- To whom the Bill of Lading is consigned.
- The date of shipment.

The *Insurance Document* is a guarantee in part or in whole (depending on the terms and conditions) by an insurance company, specifying the goods shipped on a named vessel, indicating the applicable coverage, and showing to whom loss is payable.

The *Certificate of Origin* notes the country where the goods were produced. The *Certificate of Inspection* offers an opinion that the specified quality and quantity related conditions have been met. These documents should be dated on or before the Bill of Lading date.

A *Packing List* is usually supplied by the exporting shipper in cases where a diversified shipment is packed in several packages or containers. The list will show the contents of each box or case identified by a specific number. A *Weight Certificate* is supplied by the Exporter, at the request of the Importer. It certifies the weight of each large unit in a shipment or the net and gross weights of packages containing smaller units. It is of particular value when the price of the goods is based on weight and, also, is often used by the carrier in arriving at the weight to be recorded on the Bill of Lading as a basis for the freight charges.

- The quantity of units/weights should match the Commercial Invoice (this may or may not agree based on how the weights are calculated by the various parties involved).
- The breakdown of merchandise/weight per carton, package or container should be shown if requested in the letter of credit.

Appendix OO:

FATF, *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (Paris: FATF, 2008)

Financial Action Task Force

Groupe d'action financière

MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS

18 June 2008

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. Criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. As the Internet becomes more and more a worldwide phenomenon, commercial websites and Internet payment systems are potentially subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist groups.

2. The present study analyses money laundering and terrorist financing (ML/TF) risks associated with commercial websites and Internet payment systems with the focus on mediated customer-to-customer websites as the most vulnerable to abuse because of their popularity, accessibility (to the public), and high volume of cross border trade transactions. The analysis also provides a number of case studies that illustrate how mediated customer-to-customer websites can be exploited for ML/TF purposes.

3. The study highlights the following vulnerabilities of commercial websites and Internet payment systems: non face-to-face registration, possible anonymity of the users, speed of transactions, limited human intervention, high number of transactions, international presence, limited jurisdictional competences, difficulties for traditional financial institutions to monitor and detect suspicious financial transactions with the consequence that their abilities in the detection of suspicious financial transactions, when an Internet payment service provider is used, could be affected.

4. The study indicates that some of the ML/TF risks associated with trade-based money laundering[1] and non face-to-face business and financial transactions also apply to commercial websites and Internet payment systems. The financial transactions that are initiated from a bank account or a credit card (which is the majority of online payments) already involve a customer identification process as well as transaction record keeping and reporting obligations. While low value transactions do not necessarily equate to low risk, these transactions are subject to the regulatory controls already applicable to the financial sector and may be consequently less risky. Regarding the risks associated with the non-face-to-face registration and the possible anonymity of the users, the study highlights the need for online identity verification solutions (the electronic identity card used in certain countries for instance) to help commercial websites and Internet payment service providers mitigate the risk of criminal activity. The report also indicates that if Internet payment service providers adequately monitor the financial transactions of their customers, monitoring for and acting on deviations from the customer transaction profile, the lack of face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem. Online and offline retail merchants and payment services should have comparable AML/CFT obligations.

5. It is also important that efforts to fight ML/TF by commercial websites and Internet payment service providers in different countries not be hampered by divergent privacy legislation, potentially interfering with the amount of customer information that service providers could exchange regarding suspected ML/TF.

[1] FATF (2006b).

6. Although the challenges to identifying terrorist financing apply equally to Internet payment systems (the suspicions being mostly based on name matching with the names provided by the competent authorities), it is not always necessary for Internet payment service providers to identify TF in their suspicious transactions reports (STRs) in order to help counter terrorist financing. Any suspicious activity is important to report regardless of the type of activity. Some Internet payment service providers have put in place systems to detect, monitor and analyse suspicious transactions - even for small amounts.

7. Concerning the risk-based approach to combat ML/TF, we can refer to the June 2007 FATF Guidance which states that : "By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention." Applying this principle to online transactions, the private sector may be allowed to consider low value consumer payments initiated from a financial institution or credit card account (which require customer identification and verification procedures, as well as transaction record-keeping and reporting policies) to be of lower risk than transactions initiated through service providers without anti-money laundering and counter-terrorist financing (AML/CFT) obligations.

8. The risk of fraud and the sale of illegal goods are among the concerns of commercial websites and Internet payment systems. These concerns are among the motives for commercial websites and Internet payment systems to secure their communications, websites and payment systems. In some jurisdictions, online commercial websites are not as such required to detect or fight against ML/TF, but have a market incentive to detect fraud.

9. Some commercial websites and Internet payment service providers, aware of the risk of being used for illegal activity, have set up departments to screen and monitor the transactions of their customers, using a risk-based approach. In addition to monitoring for fraud, some Internet payment service providers have also set up AML/CFT mechanisms. Best practices in the sector, including customer due diligence, monitoring transactions, not accepting anonymous forms of payment (cash for instance) imposing transactions limits, maintaining transactions records, and reporting large or suspicious transactions to the competent authorities, could be helpful for other parties of the private sector.

10. The collaboration between commercial websites and Internet payment service providers to exchange information on commercial transactions underlying financial transactions is a factor which mitigates ML/TF risks, as well as risk of fraud. Legal dispositions encouraging such exchange of information could be very useful.

11. The report concludes that, as long as the sector and the relevant competent authorities understand the potential vulnerabilities associated with commercial websites and Internet payment systems and appropriate risk-based measures with regard to customer identification, record keeping and transaction reporting are taken, the mentioned issues may not necessarily constitute a higher risk for the online sector than for the offline sector.

12. The project team believes that even though awareness of ML/TF amongst major players in the online sector is increasing, due to efforts made by regulators and trade associations, efforts need to be made to increase this awareness, particularly regarding the mechanisms of ML/TF.

13. Looking ahead, the study identifies areas which could be the focus of future efforts in order to improve the capacity to cope with the identified ML/TF risks: *i)* building a better understanding amongst governmental bodies and the private sector of online ML and TF risks and related typologies and developing guidance for implementing mechanisms to detect suspicious transactions, *ii)* making traditional financial institutions aware that they still have an important role to play in the detection and

the monitoring of suspicious financial transactions, even when the payment is made via an Internet payment service provider, *iii)* given the international character of commercial websites and Internet payment systems, international cooperation is a key factor in the fight against ML and TF, *iv)* explore further ways Financial Intelligence Units (FIUs) can enhance the exchange of information and data pertaining to the criminal misuse of commercial websites and Internet payment systems. Finally, given the international character and presence of Internet, it is difficult to determine which jurisdiction has regulatory authority over an Internet payment service provider, and how enforcement action can be applied if there are violations. World based Internet payment service providers have locations and licences in different countries and regions. It is consequently important that governments impose similar regulations, requiring customer identification, due diligence, record keeping and transaction reporting, to avoid certain Internet payment service providers choosing the country with the poorest regulations or one that is not at all regulated.

INTRODUCTION

14. Criminals use a wide variety of mechanisms to launder the proceeds of their criminal activities and to finance terrorism, including using the formal financial system, the physical movement of cash by couriers and the movement of value through trade.

15. Over the years, the Financial Action Task Force (FATF) has focused considerable attention on these mechanisms and their related typologies. Hopefully, this effort is increasing the vigilance and experience of both the private and public sectors, making it harder for criminals to launder the proceeds of their criminal activities and to finance terrorism, using identified methods.

16. However, criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. In this context, commercial websites and Internet payment systems appear to be subject to a wide range of vulnerabilities that can be exploited by criminal organizations and terrorist financiers.

17. Faced with the risk that this sector can be used to launder money or finance terrorism, government officials have been called on to start regulating electronic commerce and in particular Internet payment systems.

18. For the purpose of this study, commercial websites and Internet payment systems constitute the areas of study, with a focus on mediated customer-to-customer commercial websites. The overriding objective of this study is to increase public and private sector understanding of ML/TF risks associated with commercial websites and Internet payment systems and to raise global awareness of the methods used to launder the proceeds of crime or finance terrorism using these conduits. Largely based on case studies, an analysis of ML/TF risks associated with commercial websites and Internet payment systems constitutes a large part of the research.

19. The study does not want to replace or duplicate the FATF study on the New Payment Methods, but could be used within the framework of supplementing that report.

20. Ten countries have joined the project team and have contributed to the study: Australia, Belgium (as project leader), China, Hong Kong China, Finland, France, Luxembourg, the Netherlands, the United States and the United Kingdom. Several countries made presentations during the workshop held in Bangkok, Thailand from 28 November 2007 until 30 November 2007 in the framework of the typology exercise of the FATF. A questionnaire has been circulated to the members of the project team. The following other countries participated in the workshop and also contributed to the study: Bangladesh, Chinese Taipei, the Fiji Islands, Germany, India, Japan, New Zealand, the Philippines, South Africa, Russia, Spain, Sweden, Switzerland and Thailand. Various elements of the presentations and replies to the questionnaire have been incorporated into the report.

21. The study has also relied on the experience and cooperation of the private sector. Representatives of eBay and PayPal attended the workshop and participated to the study. The UK based company PrePay Technologies as well as the Electronic Money Association (EMA), a European trade association based in London representing a group of 33 e-money issuers and payment service providers, also participated to the project and contributed to the study.

22. The private sector has also been consulted on the report and the conclusions of the study. A meeting was organised by the project leaders with some members of the project team and the above mentioned members of the private sector, on 4 April 2008 in Brussels. The private sector which contributed to the study received a copy of the report and has been given the opportunity to comment. The comments of the private sector have been taken into account when considered relevant.

23. Finally, the risks and vulnerabilities identified by the study will be useful to the FATF study on Money Laundering Threat Analysis Strategies.

NATURE OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS

Definitions

24. This section provides a functional definition of the different classes/types of commercial websites. Commercial websites can be divided into five categories[2]:

- Mediated customer-to-customer, sites that allow private individuals to sell to one another via an online marketplace.
- Mediated business-to-customer, sites that allow multiple merchants to sell to consumers via an online marketplace.
- Non-mediated customer-to-customer (*i.e.* Bulletin board services and online classifieds), sites that only allow customers to advertise goods they want to sell.
- Direct business-to-customer, merchants that sell goods to consumers via their own websites.
- Direct business-to-business websites, merchants selling to merchants.

25. The present study focuses on the first category of commercial websites. Mediated customer-to-customer sites are popular, easy to access, open to the public, and facilitate a high volume of cross border trade transactions. As such these sites are easily susceptible to criminal misuse. This type of commercial website facilitates transactions between private parties as opposed to simply providing seller contact information with any transactions occurring off-line.

26. Online classified-advertising sites, bulletin boards and social networking sites often allow sellers to post items for sale with the transaction taking place offline. While these businesses facilitate the introduction and communication of buyers and sellers, they do not play a significant role in the final sale nor financial settlement. This type of "non-mediated" person-to-person website is therefore not often in a position to see any aspect of the transaction process after the introduction of buyer and seller.

27. "Mediated" websites, on the other hand, play an active role in the completion of underlying transactions, such as by setting the selling price through an online auction, providing some form of verification process for buyers and sellers (including aggregating feedback from other customers), or facilitating financial settlement of transactions (such as providing escrow, or similar intermediary, services). While non-mediated websites may be abused for illegal purposes such as fraud, this paper focuses on mediated businesses that play an active role in facilitating transactions that could be abused specifically for ML or TF.

28. Mediated business-to-customer websites are also subject to AML/CFT risks. A website can sell clothing much of the day, and appears legitimate to its Internet payment service provider, but the website address (URL) may in fact be used to sell child pornography material for several hours each night. In some cases, businesses may allow 3rd party merchants to sell their own goods and services through the business's online portal.

[2] It is worth mentioning that certain commercial websites belong to more than one category.

29. Commercial websites and Internet payment service providers can be used for illegal transactions, including the sale of illegal drugs, weapons, firearms, counterfeit products and child pornography, or to facilitate fraud. Internet payment service providers can be used afterwards to launder the proceeds of these illegal activities.

30. For purposes of this report, the term Internet payment system is used to broadly describe an Internet-based company that provides financial transaction services to consumers. Furthermore, in most instances, Internet payment systems consist of non-bank financial institutions that may or may not be subject to regulatory oversight depending upon the legal jurisdictions of where such systems provide services to consumers. Consumers are attracted to Internet payment systems because such systems often are convenient, and serve as an alternative to making payments via a bank account or credit card which may not be available to everyone.

31. Considering the risks affecting commercial websites and Internet payment service providers, the project team considers that a clear distinction must be made between the business activities of commercial websites and the payment associated with these commercial activities (Internet payment services), even if some commercial websites are apparently providing both commercial activities and the associated financial service.

Main characteristics

32. This section lists the main characteristics of the type of commercial websites studied and the Internet payment systems linked to these websites.

Commercial websites

33. Commercial websites usually have some if not all of the following characteristics[3]:

- A simple Internet connection is sufficient to open an Internet account with a commercial website and to buy and sell items on the Internet.
- Websites can potentially be accessed from any location in the world.
- A customer can gain access from his own Internet connection or from the Internet connection of a third party (*e.g.* cyber cafes or phone shops that provide Internet access) or another access point that is not registered to the customer.
- A customer can register in one country and connect from another country.
- Registration is very easy and very rapid (only a few minutes are necessary to register).
- Registration is non face-to-face.
- A limited amount of information is required to register.
- No procedure to verify customer identification in certain cases.
- Anonymous e-mail addresses may be used as customer contact information.
- Commercial transactions are performed very rapidly. E-mail messages are used to inform the seller that the item he put on sale has been sold.
- Customers have access to a wide range of items (from small value items to high value items) on sale on a wide range of commercial websites located all over the world.
- Goods can be sold for either a fixed or variable price. For example, on auction sites, the price may be set by the seller or by different buyers, creating uncertainty over the true market value of the goods being sold.

[3] Some of these characteristics are characteristics of the Internet and also apply to Internet payment service providers

- Commercial websites may facilitate sale and financial settlement but leave delivery arrangement to buyers and sellers. Often, the only indication of non-delivery of goods will be if the buyer complains.

34. Some commercial websites and Internet payment service providers apply a risk-based approach when identifying customers. If the risk profile of the customer and transaction are high, additional verification methods are applied (simplified Customer Due Diligence (CDD) vs. enhanced Customer Due Diligence (CDD). The mechanisms of verification can be adapted to the country of registration and changed as necessary to adapt to criminal techniques to bypass identification and verification processes. The private sector representatives who participated in the study indicated that criminals do attempt to circumvent these processes and although none of the methods had a zero-failure rate, they were effective on a risk-weighted basis. In certain countries, online customer identification mechanisms using an electronic identity card are used and reduce the risk of identity theft.

Internet payment systems

35. As with any type of online business, the structure and operations of a given Internet payment system may vary drastically. However, in most cases such systems usually require a consumer, or user, to register with the Internet payment system before any transactions can be effected by the system. This registration process typically involves the collection and verification of some identification and/or contact information. For example, an Internet payment system may require a user to input his or her email address, telephone number, street address, and information needed to create a password and user identification (User ID) that will be required for the user to log into the Internet payment system.[4] Other information may be required based upon the business practices of the Internet payment system largely depending upon the type of services provided and the risk management processes required by jurisdictional authorities. The information collected is then verified using a variety of methods, ranging from the examination of paper copies of identity documentation to the use of online identity verification solutions provided by third parties.

36. Before a user of an Internet payment system can effect a transfer of funds through the system he generally must first fund the transfer. Funding a transfer through an Internet payment system may involve funding an "account" from which funds will be drawn for subsequent transactions or transfers, or providing the Internet payment system with the equivalent amount of funds the user wishes to transfer. Depending upon the operations of a given Internet payment system, the user may have several options for funding a transaction, and may not be limited to the use of the user's credit card or personal bank account. To avoid fraud or any form of criminal misuse, the Internet payment service provider may attempt to verify that the customer has control over and is authorised to use certain funding methods, such as a credit card or bank account. Once the user has successfully been verified, the user is free to conduct transactions through the Internet payment system.

37. It is important to note that in order for an Internet payment system to provide transaction services for their users, they oftentimes must intersect with traditional banking and settlement systems. For example, an Internet payment system that accepts major credit cards as a funding source from its users usually is required to maintain a merchant account at a financial institution. Through this merchant account the Internet payment system can receive funds from its users, via major credit card networks. Such funds can then be applied to a transaction instruction that has been initiated by a user within the Internet payment system. A similar type of relationship typically exists with an Internet payment system that accepts funds from its users via the user's personal bank account. Once again, the Internet payment system is typically required to maintain an operating account at a bank where the

[4] Note that at the time of registration an Internet payment system may not require a user to input their personal identification number (*e.g.* social security number, passport number, etc.) or date of birth. Based upon the best practices of a given Internet payment system such information may not ever be collected from a user.

transfer of funds from a user's personal banking account can be received. Typically these types of transfers are effected through clearing systems.

38. Internet payment systems may support various types of payment methods for consumers purchasing goods and/or services online from a business website (commonly referred to as Consumer-to-Business transaction or C2B transaction) and businesses purchasing goods and/or services online from another business (a Business-to-Business or B2B transaction)[5]. However, the type of transaction that is of concern for potential ML and TF vulnerability is a person-to-person (P2P) transaction, involving a transaction between two consumers, as when buyers and sellers interact via a mediated website.

39. Other types of funding could be provided directly by certain commercial websites (transactions not powered by an Internet payment provider) or requested by consumers selling items on P2P commercial websites:

- Credit cards.
- Prepaid scheme-branded cards[6] (anonymous in certain countries).
- Wire transfers (in favour of the bank account of the commercial website for further transfer to the seller).
- Wire transfers to the seller bank account (with a message accompanying the transfer and referring to a sale on the Internet).
- Gift cards or gift cheques (anonymous and transferable).
- Cheques (sent to the commercial website in certain countries, to the customers in other countries).
- Bank cheques.
- Postal orders/money orders in favour of the seller[7].
- Money transfers in favour of the seller.
- Cash is accepted on certain commercial websites.

Payment in cash can be made directly between buyer and seller, but this mechanism is not believed to be regularly used.

40. With Internet payment systems, the transaction takes place electronically very rapidly.

41. For global stakeholders (commercial websites and Internet payment systems available in different countries), the policies, practices, facilities (commercial and payments) made available to customers, may be different depending on the location of the parent company, local branch, or local website.

---

5 Some commercial websites and Internet payment service providers offer their customers the opportunity to use a more secured method of payment called the "third party of confidence". Using this facility (against the payment of a commission), the buyer knows that the funds for his purchases on Internet will be made available to the seller only if the goods purchased have been delivered and if he is satisfied that the goods correspond to the description on the commercial website.

6 Banks in certain countries offer prepaid scheme-branded cards (preloaded cards) to customers for whom banks do not want to open a credit limit (unemployed or persons without a regular income).

7 Certain commercial websites advise their users to be cautious when accepting money orders as payment facilities when purchasing items on the Internet, as experience has shown that money orders are often used by criminals who commit fraud (selling items they do not deliver for instance).

MONEY LAUNDERING AND TERRORIST FINANCING CASE STUDIES

42. The following section gives an overview of case studies involving the use of commercial websites and Internet payment systems. This section is divided into two subsections *i)* actual case studies and *ii)* potential vulnerabilities. Potential vulnerabilities are given to provide guidance to law enforcement agencies, financial intelligence units and the private sector.

Actual case studies

43. This subsection provides a number of case studies that illustrate various ways that commercial websites and Internet payment systems have been exploited for ML/TF purposes.

44. Commercial websites and Internet payment systems can be used to sell/purchase illegal products, like drugs or counterfeit goods. Sometimes, the sold/purchased dual-use or precursor products are not *per se* illegal but correspond to dual use goods such as products used to make explosive, weapons or other controlled goods. Postal and express freight are frequently used to distribute these goods.

45. Commercial websites and Internet payment systems can be used for committing illegal transactions, fraudulent transactions or illegal activities, activities outside of the FATF's remit. Nevertheless, various case studies indicate that commercial websites and Internet payment systems are also used to collect the proceeds of these illegal activities, and further to facilitate ML and TF transactions (by making the funds disappear: transferring the funds on a bank account in the country of the criminals or abroad, using them for other purchases on commercial websites,…).

Case study: The use of commercial websites and Internet payment systems to sell drugs

In one file, the bank account in Belgium of an individual was credited by wire transfers from an Internet payment service provider (small amounts for a total of EUR 4 700). The subject was under investigation in another European country for the sale of drug starters. Information from law enforcement confirmed that the subject was selling drug starters via a commercial website.

Source: Belgium.

46. In the above-mentioned case, the Internet payment service provider was used to collect the proceeds of the illegal activities and may afterwards be used to perpetrate the illegal activities and operations. The criminal could use the proceeds of his illegal activities to buy new drug starters and continue to carry out his illegal activities via the commercial website.

Case study: The use of commercial websites and Internet payment systems to sell counterfeit goods

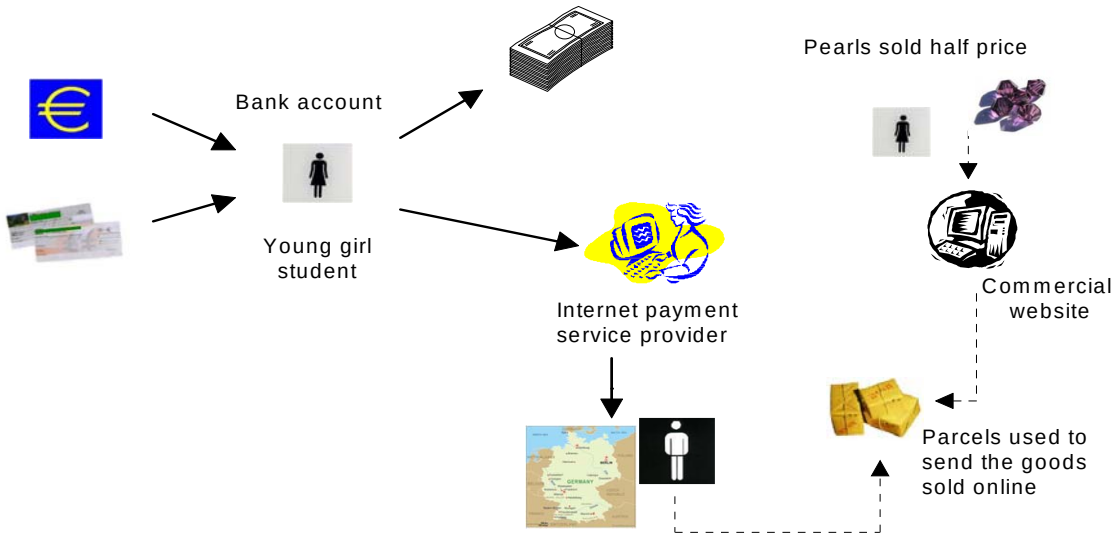
A bank reports the suspicious transactions of a young girl. From January 2005 to August 2005 (eight months), the bank account of the young girl, student, was credited by wire transfers and cheques written out by individuals located all over France. The amount of each cheque was rather small (EUR 20 to 40). Regarding the debiting operations, the girl made cash withdrawals and wire transfers bearing the mention “Internet payment provider bills”. The purchases amounted to a total of EUR 6 340 split into 43 operations.

In September 2005, she began to use a credit card so that it became more difficult for the bank to understand and analyse her transactions. Only a global amount of payments is registered monthly on her bank account.

Investigations showed that, from September 2005 to March 2006 (eight months), she made 63 purchases online for a total amount of EUR 39 282.24.

The young lady was selling counterfeit pearls of a famous brand at half price. She was using a provider in another European country which sold her parcels used to send the goods she had sold online.

Over 16 months, she earned more than EUR 43 000, roughly more than EUR 2 800 a month.



Source: France

Case study: The use of commercial websites and Internet payment systems to sell explosive precursor products

A foreign FIU communicated/disclosed to the Belgian FIU that they received a STR from an Internet payment service provider concerning a national from a European country selling the following items on an associated commercial website: potassium, chlorate, barium nitrate, strontium nitrate, ammonium nitrate. These items are considered as dual-use goods, because, put together, they can be used to make explosives. The goods were sold to customers in Eastern Europe.

The criminals planned to collect the proceeds of their “illegal” sales on the Internet through the Internet payment service provider and consequently to launder these proceeds, also using the Internet payment service provider.

Source: Belgium.

Case study: The use of commercial websites and Internet payment systems related to weapons trafficking

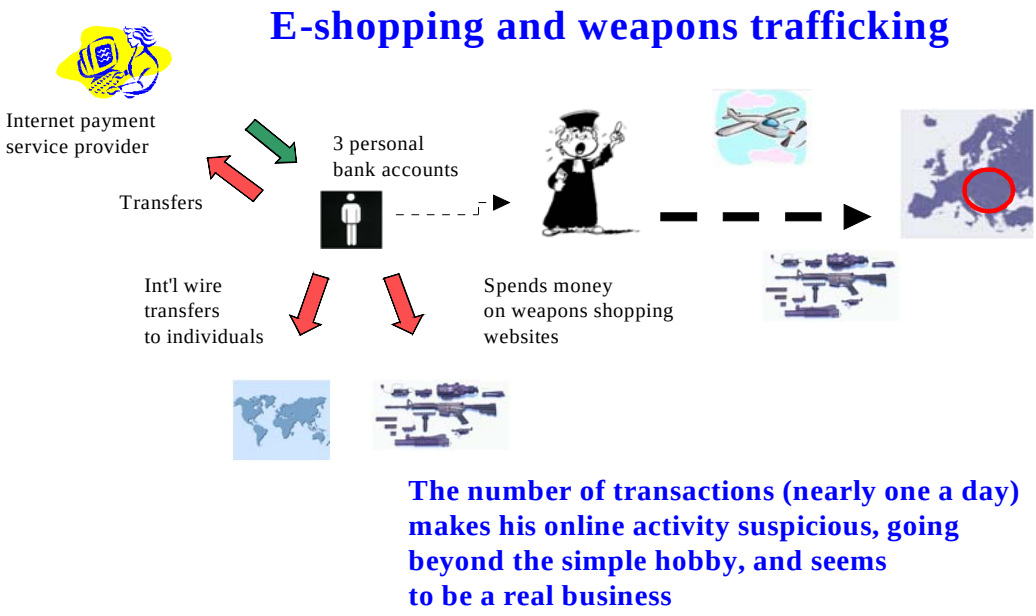
A case reported by a bank involves a lawyer receiving and initiating a lot of Internet payments on and from his three personal bank accounts, ordering international wire transfers to individuals, receiving cheques and making cash deposits with no apparent economic rationale.

From the message on his bank account accompanying the financial transactions with the Internet payment service provider (payment "gun X", payment "pistol Y") and the analysis of the wire transfers, it was possible to identify his online activity as related to weapons and elements of weapons sales transactions.

FIU's investigations revealed further that:

- over 4 years he made more than 1 600 selling operations, the frequency of this online activity revealing a potential illegal business activity related to the use of weapons commercial websites;
- he regularly travelled to countries from Central and Eastern Europe which are vulnerable to weapons trafficking and often stayed more than one week there, so that he might have smuggled weapons.

The case was transmitted to the judicial authorities for weapons trafficking.



Source: France.

47. Commercial websites and Internet payment systems can also be used for commercial activities performed without VAT registration and without paying taxes.

Case study: The use of commercial websites and Internet payment systems to sell goods illegally (avoiding tax obligations)

The persons on investigation were directors of a company involved in purchasing large quantities of duty free cigarettes and alcohol to sell on the domestic market contrary to their export-duty free status, thus avoiding tax obligations. Due to not paying any tax on the goods the company was able to markedly increase profits. The syndicate also generated false receipts that purported to come from an export company detailing their alleged cigarette exports. Investigations with the purported company confirmed that no such exports had ever been made. On arrival of the cigarettes, payment was made to the delivery driver on a cash-on-delivery basis.

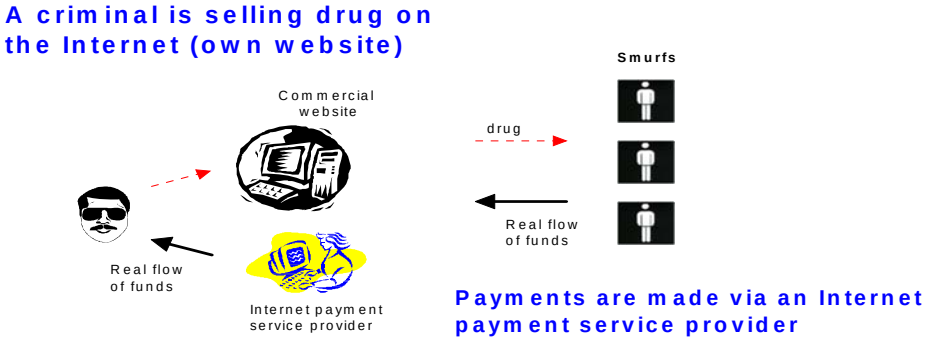
A large number of the company's sales occurred over the Internet from customers paying via credit card. A majority of the sales on the Internet were illegitimate and came from three different email addresses. Payments for these orders were made from one of two credit cards linked to Belize bank accounts. One of these cards was held in the company's name. The money in the Belize bank account was sent there by one of the directors using several false names from not only Australia but Belize, Hong Kong, and Vietnam. The director conducted structured wire transfers under false names and front company accounts. The funds were purchased at well known banks with multiple transactions occurring on the same day at different bank locations and all of the cash transfers conducted in amounts of just under AUD 10,000 to avoid the reporting threshold.

Source: Australia.

48. Criminals can develop their own commercial website to sell illegal products or perform illegal activities and use Internet payment service providers to collect the proceeds of these activities.

Case study: Criminals using their own commercial website to sell drugs and the use of an Internet payment service provider to collect the proceeds of their activities

An Internet payment system user owns a commercial website where he is selling cannabis, cannabis seeds and narcotics utensils. As he wishes to be paid via an Internet payment system, the buyers are using this payment system.



Source: Luxembourg.

Case study: The use of an Internet payment service provider account to collect proceeds of procurement on the Internet

The user of an Internet payment service provider receives payments from a website offering escort services or prostitution. This user is the registrant of the website and he gets the funds on an account from buyers. On the website, the use of the Internet payment system is indicated. The website is explicit, contains several prostitutes to be chosen by the client and is professionally set up. The commercial website and the IP logins are detected by the Internet payment service provider and the file transmitted to the FIU.

Source: Luxembourg.

49. As already mentioned in the FATF report on New Payment Methods, digital precious metals are a new online payment system that involves the exchange of options or the right to purchase an amount of precious metals at a specific price. These derivatives can be exchanged, like traditional commodity or securities derivatives, between account holders in a digital precious metal service. Consumers purchase a quantity of virtual precious metal holdings based on the current price of the metal on the world commodity exchanges. Once a purchaser has acquired a quantity of the virtual

precious metal, those holdings or a portion of them can be transferred either to another individual or a merchant in exchange for goods and services, also online. As a result, digital precious metal exchanges allow for the transfer of fixed "value" between unrelated 3rd parties, functioning as a money and value transmission business.

Case study: the use of e-gold as payment method

On 27 April 2007, a federal grand jury in Washington, D.C., indicted two companies operating a digital currency business and their owners. The indictment charges E-Gold Ltd., Gold and Silver Reserve, Inc., and their owners with one count each of conspiracy to launder monetary instruments, conspiracy to operate an unlicensed money transmitting business, operating an unlicensed money transmitting business under federal law, and one count of money transmission without a license under D.C. law. According to the indictment, persons seeking to use the alternative payment system E-Gold were only required to provide a valid e-mail address to open an E-Gold account – no other contact information was verified. The indictment is the result of a 2½-year investigation by the U.S. Secret Service with cooperation among investigators, including the Internal Revenue Service (IRS), the Federal Bureau of Investigation (FBI), and other state and local law enforcement agencies. According to Jeffrey A. Taylor, U.S. Attorney for the District of Columbia, "The defendants operated a sophisticated and widespread international money remitting business, unsupervised and unregulated by any entity in the world, which allowed for anonymous transfers of value at a click of a mouse. Not surprisingly, criminals of every stripe gravitated to E-Gold as a place to move their money with impunity."

Source: U.S. Department of Justice.

50. During the workshop, case studies were also presented where commercial websites and Internet payment services providers are used to facilitate the commitment of the underlying criminality (fraud in most of the cases) but not for the money laundering. These cases, even if they are not directly relevant in the framework of the present study, are given as they could be useful to traditional financial institutions for fighting against money laundering.

51. Commercial websites and Internet payment systems can be used by criminals to commit fraud. One of the mechanisms used is the sale of fictitious items which the seller will not deliver to the buyer after receiving the payment. If commercial websites are used to attract buyers (in this case the victims of the fraud), Internet payment systems are not necessarily used to collect the funds (the proceeds of these activities). Criminals frequently use bank accounts in traditional financial institutions or money transfers and postal orders to be paid for the goods they do not deliver. The same channels are thereafter used to launder the proceeds of these illegal activities by making the funds disappear.

Case studies: Transfers related to fraudulent sales on commercial websites (items never delivered)

The Belgian FIU received several STRs from banks in Belgium concerning bank accounts credited by wire transfers, apparently related to/justified by sales on commercial websites, and followed by cash withdrawals.

The majority of the wire transfers are of small amounts (maximum EUR 800), originate from various senders and, following the message accompanying the payment, should be related to sales on a commercial website, sometimes the sales of luxury goods. Payments are not made through an Internet payment service provider but originate from the bank account of the buyer and are credited on the bank account of the seller. The wire transfers are followed by instant withdrawals in cash.

The goods are never delivered to the buyer (victim of a non-delivery fraud).

In some reports the wire transfers are not followed by cash withdrawals but by transfers in a country known for producing counterfeit products (in cases related to the sale of counterfeit goods).

The fraudulent bank account is used only during a short period (because of buyer's complaints).

Investigation showed that false names are used on the commercial website (the name used by the seller on the commercial website (certainly a fictitious name) and the name of the bank account holder where the payment is made are different). In one file, information received from law enforcement indicated that the subject was known for using different names on the commercial website. In another file, the subject was using two different passports and different names.

Source: Belgium.

Case study: Sale of fictitious goods on commercial websites and the use of Western Union to collect the proceeds of these fictitious sales

The National Bureau of Investigation Money Laundering Clearing House investigates an aggravated fraud and money laundering case. The two main suspects in Finland were acting as Western Union agents in Finland. The offices of the agents were closed on 27 March 2007, and the suspects were taken into custody.

People from other countries than Finland were fooled into buying fictitious goods (in this case; cars or other vehicles) on commercial websites[8] and sending the payment to fictitious persons in Finland via Western Union.

The two Western Union agents in Finland picked up the money with the identities of the fictitious persons. Furthermore, the agents forwarded, again with fictitious identities, the money as Western Union transactions outside of Finland.

The two suspects in Finland received text messages from two persons (money flow managers) using mobile phone numbers including:

- information about the victims abroad (their name, the expected receiver of the money, the amount sent and the MTCN) as well as
- instructions for forwarding the money abroad (the name of the receiver, the amount and the country to which send the money).

The money flow managers are living in European countries.

The total number of victims is over 300 and the total loss for the victims is about EUR 1.07 million. The main source countries for the assets were the USA and the UK, but there were also a number of other source countries (about 25 countries).

The two Western Union agents in Finland say that they received 10 per cent of the money picked up by them. They also say that both the money flow managers visited Finland during the activity and took with them a significant amount in cash.

Based on the investigations, at least one of the money flow managers seems to have similar arrangements with local Western Union agents in a number of other European countries.

Searches at the Western Union offices and the homes of the agents and arrests were made on 27 March 2007.

The investigation of the phones, SIM cards and PCs gave good evidence. Hundreds of text messages as well as a few e-mail messages were found in which instructions were given to the Western Union agents concerning the fraud cases and the money transactions.

To support the investigation and the case in court, information is needed about as many predicate offences abroad as possible. Therefore, requests (FIU, Interpol or MLA) have been sent to 24 countries.
At the moment information was received about 181 fraud cases from 19 different countries.

[8] It is worth mentioning that on certain commercial websites, a seller cannot request potential buyers to pay by money orders. To avoid problem with fraud, these commercial websites do not allow their users to propose payments by money orders (this option is not available and a seller cannot request a payment by money orders when exchanging mails via the mail system of the commercial website).

Source: Finland.

52. It is worth mentioning that certain commercial websites propose mechanisms to their customers to avoid their site being used to commit such type of fraudulent activities: organizing rating systems to evaluate users' (buyers and sellers) reliability based on their previous transactions with the commercial website, advising their customers not to use money orders, encouraging the use of an Internet payment service provider associated with the commercial website because this is more secure, tracking and banning fraudsters.

Potential vulnerabilities

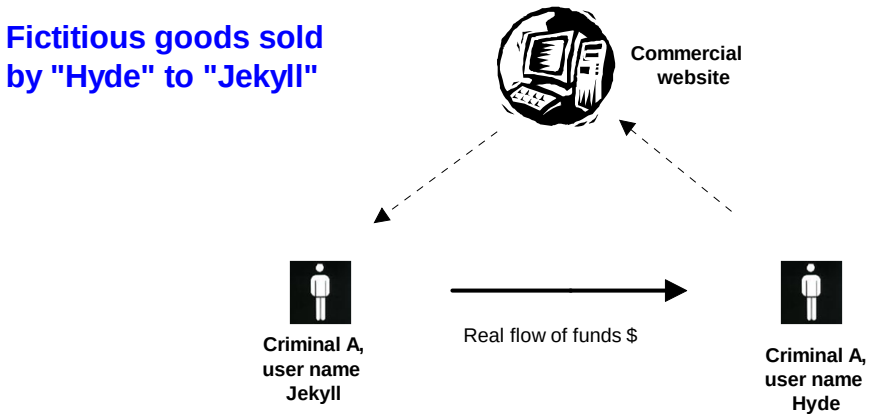
53. Potential vulnerabilities presented in this section are given to help the private sector stakeholders, not yet aware of possible ML or TF mechanisms, to detect possibly suspicious transactions. Some potential case studies present similarities with case studies analysed by FIUs and presented in the first subsection.

54. These potential vulnerabilities are considered feasible in reality by the private sector consulted during the study. However certain commercial websites and Internet payment services providers have developed monitoring and detection systems and mechanisms (cf. section "Risk management measures taken by the sector") in such a way that these transactions may be better detected and provide additional deterrence to criminals attempting to use these systems.

55. Criminals may use fictitious commercial transactions on commercial websites to justify movements of funds using traditional financial institutions or Internet payment systems. This typology shares many similarities with trade-based money laundering, where the transfer of funds for a transaction is disproportionate to the value of the goods delivered.

Potential case study: Fictitious sales on commercial websites followed by real payments

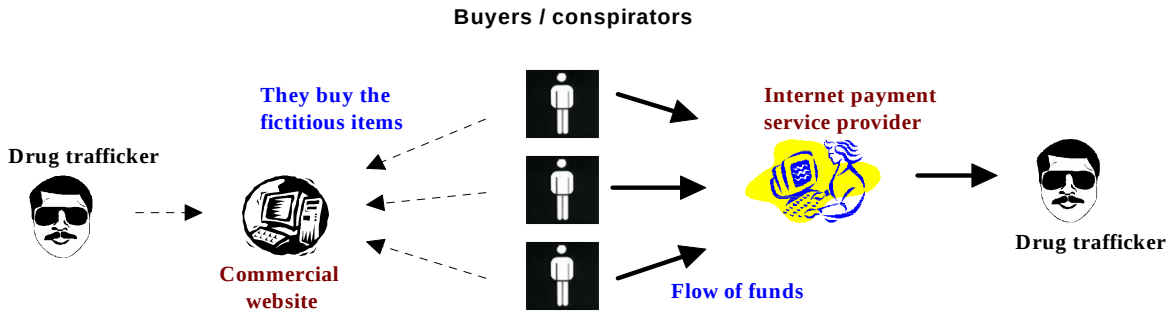
Buyer and seller know each other and may live in different countries or continents. No goods are delivered. Certain commercial websites between private individuals only put buyers and sellers in touch. They are not liable for the delivery, for checking the quality and/or the reality/existence of the goods offered for sale. The buyer will never complain for the non-delivery because seller and buyer are in league with each other. The buyer will pay the seller who will receive the funds on his bank account abroad. The beneficiary will have no difficulties justifying the origin of the funds received because the funds apparently come from sales on the Internet[9]. The buyer can also easily explain that he uses his credit card to buy something on the Internet. Commercial websites between private individuals allow the sale of goods of relatively high value, which will allow criminals to launder considerable amounts.



Source: Belgium.

Potential case study: The use of a commercial website to launder the proceeds of drug trafficking

A drug trafficker can use commercial websites to receive the payment of his illicit sales. Instead of raising his bank's suspicion with unjustified cash deposits, he publishes an announcement for whatever fictitious products. His drug clients then proceeds with an online immediate purchase. Once the drug trafficker receives the payment, he can deliver the drugs as well as justifying the credit operations on his bank account with "online sales operations". This implies that there is coordination between "seller" and "buyer".



Source: France.

[9] As also mentioned in the section "Considerations on second level of controls versus third level of controls", a statement or a printout of a screen of the commercial website showing an item on sale for instance must not immediately and unconditionally considered as an invoice or justifying a financial transaction on the bank account of the customer. Conversely, the presentation of such justification document could be used as a red flag or indicator for the financial institution.

56. If the item sold by criminals exists, it can happen that the price of the item sold is overrated by buyers and sellers who know each other and can consequently justify relatively bigger movements of funds. This is essentially the same typology used in trade-based money laundering.

Potential case study: The sale of goods at an overrated price

The mechanism is the same as in the above-mentioned example, except that the goods sold do exist and are sold at an overrated price through several fictive buyers. The net difference between the nominal sale price and the actual value of the goods delivered equals the value of money laundered. This type of transaction provides additional security for the launderers by creating a record trail of actual delivered goods, requiring law enforcement to prove that the value of the sale is grossly out of proportion with the actual market value of the goods.

Alternatively, value can be laundered in the reverse direction by having the buyer buy significantly less than the market value of the goods and then reselling the goods for a profit. The buyer would then be able to claim the difference in value was a profitable arbitrage deal while the seller would be to write off the difference as a market loss.

Many online businesses, particularly auction sites, sell goods that do not have a readily available market price. Also, overbidding is not unusual and could reflect legitimate transactions. In addition, since the items being sold remain in the possession of the seller throughout the auction process, the online auction company has little ability to ascertain the true market value of the item.

Source: Belgium.

57. As already mentioned above counterfeit products or stolen products could be sold on commercial websites, aka a "virtual fence". Internet Payment systems could be used to move and launder the proceeds of these sales.

Potential case study: The sale of counterfeit or stolen products using multiple identities and user names

A criminal sells via a Customer to Customer website stolen and counterfeit goods. By multiplying identities and user names, he reduces the risk of being identified by the monitoring unit of the shopping website. He can either use the proceeds generated by his illegal sales to buy other goods or services online or transfer it to his personal bank account, the crediting operations being justified by "online sales operations".

Source: France.

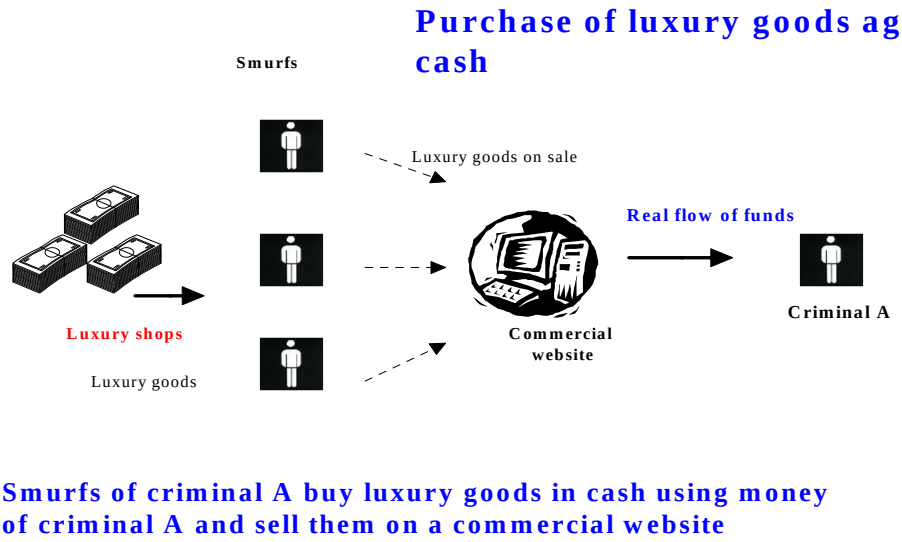
58. Not only counterfeit luxury goods could be sold on commercial websites, but also real luxury goods purchased with cash by smurfs recruited by criminals to launder the proceeds of their illegal activities.

Potential case study: The use of commercial websites to sell at a reduced price, of goods (not counterfeit) purchased by smurfs in luxury goods shops with cash

Criminals send smurfs to luxury goods shops to buy articles of relatively high value (handbags…) that they pay in cash. This first stage of the money laundering process allows criminals to inject cash, possibly in small denominations into the financial system. This stage takes place in luxury good shops, which are less aware of money laundering[10].

[10] The 3rd EU AML/CFT directive applies to natural or legal persons trading in goods, to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked. Merchants of high value goods accepting cash above EUR 15 000 are submitted the AML/CFT obligations (KYC, record keeping, cooperation with the FIU, adequate internal organisation). In certain countries, merchants in high value goods are not authorized to accept payments in cash if the value of the purchased goods exceeds a certain threshold (in Belgium: EUR 15 000).

The luxury goods are subsequently sold on commercial websites, at a lower price. Criminals accept to lose a lot of money to launder the proceeds of their illegal activities. The proceeds of the sale arrive on the bank account of the seller abroad.



Source: Belgium.

59. ML transactions not only take place in the first stage of the money laundering process (placement), but happen also during the two other ML stages (layering and integration). Criminals usually try to make the financial transactions more sophisticated for law enforcement authorities and investigators, using a combination of the different ML stages. Commercial websites and Internet payment services providers could be used at various stages of the ML process. Traditional financial institutions could be used during the placement stage and commercial websites and Internet payment services providers at later stages such as during the layering stage (the above mentioned potential case study) and the integration (the purchase of goods or items with illegal funds already injected in the financial systems). The two following case studies explained below provide examples of the use of the ML process at the integration stage.

Potential case study: The use of an electronic purse in conjunction with other ML methods

- An individual residing at the country border regularly imports tobacco and alcohol products exceeding the duty-free quantities from the neighbouring country.
- He sells them to individuals. The cash collected is used to credit a savings account opened in the name of one of his underage children. The justification given can be cash donations from the family to the child.
- The funds crediting the savings account of the child are regularly transferred to the bank account of the individual held in another bank. The origin of the funds appears to be legal – it comes from the savings account of one of his children; the justification for the transfers can be temporary financial difficulties, expenses made for the child like buying a scooter or paying driving lessons, etc.
- The funds transferred on the bank account of the individual can then credit an electronic purse to buy goods and services online.

Source: France.

60. Commercial websites and Internet payment systems can potentially be used to finance terrorism, taking into consideration the fact that terrorism financing may involve small amounts of money.

61. As already mentioned, commercial websites and Internet payment service providers depend on information they obtain from law enforcement and other authorities to facilitate the detection of suspicious transactions related to terrorist financing and it is not always necessary for Internet payment service providers to identify TF in their STRs in order to help counter terrorist financing.

Potential case study: The use of a commercial website and Internet payment service provider to finance terrorist activities also in conjunction with other ML methods

- Y, a well-known terrorist, under close watch of the intelligence services, residing in Germany, wants to send funds to Z, residing in France so that Z can buy cell phones or other items necessary to make explosive devices.

- Afraid of being detected if he uses funds transfer systems like Western Union or MoneyGram, he decides to use an alternative way to make his funds available.

- He asks a student to register on a C to C website and to open an Internet payment provider account. Y gives the student a prepaid card of EUR 799 to credit his Internet account.

- The student can then order a transfer from his Internet account to the Internet account of another student located in France.

- The student located in France can then credit his bank account with the funds received on his Internet account and buy prepaid cards to be handed over to Z.

- Z can use the prepaid cards directly or credit his bank account with them.

Source: France.

62. Front individuals or intermediaries such as the "students" in the example above are even recruited on the Internet, lured by the payment of a commission amounting from 5% to 10% of the funds to be transferred. Massive spams are sent, proposing to become the associate of a "financial company", the job consisting of receiving and transferring funds. These mules are used for ML/TF.

63. Other potential case studies :

Other potential case studies

- A criminal or a third party used by the criminal purchases goods on the Internet, using prepaid cards (anonymous).

- The purchase of prepaid cards against cash (from points of sales or third parties).

- The purchase from a third party (against cash) of assets/value held by the third party on an account opened on the Internet (Internet payment service provider).

- A money launder justifies movement of funds by a fictitious turnover from e-commerce activities.

- A criminal or money launderer detains assets on accounts opened on the Internet (Internet payment service provider).

Source: The Netherlands

64. If the above mentioned case study is feasible in reality, high standards of due diligence and computer software to detect suspicious transactions should detect such patterns as they are carried out on a multiple basis (multiple transactions is a prerequisite for criminals if they want their ML/TF transactions to be economically viable)[11]. On commercial websites and Internet payment service providers applying such due diligence mechanisms, a user multiplying transactions will be the subject of a "client verifying process", implying that the commercial websites will obtain more information on the seller (Memorandum of Association, VAT registration…). Commercial websites also work with companies selling luxury goods to identify individuals selling counterfeit luxury items.

Red flags – Indicators

65. This section, which resulted from the typological analysis, provides an overview of potential indicators of ML/TF. These red flags – indicators must call the attention of the Internet payment services providers when analysing suspicious transactions. An indicator is itself not sufficient to

[11] The commercial websites and Internet payment service providers consulted during the study apply these types of due diligence mechanisms and use monitoring software.

conclude that a transaction is suspicious and must be reported to the FIU. The Internet payment service provider has to collect additional information to analyse the suspicious transactions.

66. Certain Internet payment service providers already use these red flags – indicators to detect suspicious transactions/activities using risk models and computer software (cf. section "Risk management measures taken by the sector"). However, they are provided for Internet payment service providers which are not yet aware of the ML/TF risks and not yet familiar with such indicators.

67. This section is also provided for the private sector stakeholders to be added to their own developed indicators.

68. As mentioned below in the section "mechanisms used to mitigate ML/TF risks", Internet payment service providers have access to a range of information, inclusive information on the underlying commercial transactions, to analyse suspicious financial transactions.

69. Following red flags-indicators have been identified:

- The customer opens his individual Internet account with the payment service provider in one country but logs in regularly on the website from a single or multiple third countries.
- The account opened by the customer is loaded with funds transferred from a third country, which could indicate that the customer does not live in the country from which he registered but in another country where he cannot register (not accepted by the website for security reasons) or that he registered in one country but commits illegal activities in a third country, or that he concealed the results of his illegal activities in a third country.
- The customer starts to purchase items on the Internet for amounts not in line with his previous transactions profile.
- The customer loads his Internet account with cash[12], if the Internet payment services provider allows loading with cash[13].
- The customer account with payment service provider is loaded with funds transferred by a third party apparently not related to the customer.
- The transactions of the customer suddenly deviate from its previous transactions profile after his customer account had been loaded with money from a third party.
- The customer purchases items of high value[14] or purchases middle high value items on a regular basis with a prepaid debit card, an anonymous prepaid credit card[15] or a gift card where the origin of the funds is difficult to retrace[16].

---

12 It is worth mentioning that the loading of an account or a card with cash is not sufficient in itself to give rise to a suspicion of ML/TF. Cash could have a legal origin. Confronted with cash, the Internet payment service provider needs to apply higher standards of control or due diligence (monitoring of transactions, limits and restrictions…).

13 It is worth mentioning that systems which do not accept cash may be less risky.

14 According to the private sector consulted during the study, on commercial websites and Internet payment services provider, the average value of a commercial transaction and the subsequent payment are very low. Consequently money launderers wanting to use commercial websites and Internet payment service providers for their criminal activities and the ML may need to carry out several consecutive small transactions if they want to avoid being detected. In case they carry out a large transaction they will be detected by commercial websites and Internet payment service providers using sophisticated computer software.

15 It is sometimes difficult for Internet payment service providers to distinguish between a normal credit card and a prepaid credit card as credit card companies use similar credit card numbers for both credit cards.

16 It is worth mentioning that Gift cards have generally low face values. Criminals need to purchase several gift cards to make their ML transactions economically viable. Issuers of gift cards have also internal control

- The customer apparently resells goods purchased beforehand, without any economic reasons, or with a significant discount or increase on the price (monitoring feasible if the Internet payment service provider cooperates with the commercial website involved when analysing suspicious financial transactions);
- The buyer requests that the goods be delivered to a post office box or to a different address from the one registered to the account (facilities depending on the country of destination).
- A customer uses an account with an Internet payment service provider not to purchase items on Internet but to hide a sum of money obtained illegally. A customer opens an account with an Internet payment service provider, loads the account with important amounts of money, leaves the funds on the account during a certain period of time and requests the redemption of the funds later on[17].
- A customer requesting the balance from his Internet account to be transferred to a third party without apparent relation with him.
- The use of credit cards, particularly prepaid, issued in a foreign country.
- A customer sells illegal items or the goods appear on a list of forbidden items.
- Abnormality with the proposed price on an auction site or during an auction sale indicating a possible complicity between buyer and seller (a customer offers to purchase an item at a price largely higher than the requested price). Additional factors could include multiple transactions between the same buyers and sellers.
- The purchased goods are regularly shipped to a foreign country.
- The customer uses a credit card issued by a bank in an offshore centre or in a FAFT non-cooperative country[18].
- The funds originate from a non-cooperative country.
- The country of origin of the customer is known by the FATF as a non-cooperative country in the fight against money laundering or terrorism financing.
- An unexpected turnover for a recently established commercial website or an unexpected increase in the value of the commercial website after a few sales.

Suspicious behaviour or transaction may result from one indicator or a set of indicators.

70. The private sector participating in the study confirmed, based on their experience, the accuracy and pertinence of this list of red flag – indicators.

---

mechanisms to follow the issuance of gift card at local shops or supermarket, which reduce but do not eliminate anonymity.

17 Some e-money devices are limited in time.

18 All the non-cooperative countries identified by FATF have been delisted. Certain countries are still under monitoring.

MONEY LAUNDERING AND TERRORIST FINANCING RISKS

71. The AML/CFT risks of trade-based money laundering and non face-to-face transactions apply also to commercial websites and Internet payment systems. The AML/CFT regulations of commercial websites could be comparable to the ones existing for traditional commerce (those regulations only apply to merchants accepting cash over a predefined threshold) and the ones of Internet payment systems to the common payments systems, even if the relationship is non face-to-face, because risk-based CDD and monitoring measures are taken to reduce and mitigate the ML/TF risks.

72. These risks can be classified according to the ML phases:

Placement:

- **Anonymity[19] of customers on certain commercial websites and Internet payment services providers.** Both the registration and transactions could in certain circumstances be performed anonymously (on certain websites an anonymous e-mail address is enough for registration).
- **The relationship with customers is a non face-to-face relationship**. Transactions are non face-to-face transactions, which makes it more difficult for the commercial websites and Internet payment services providers to be sure that they are working with the customer who has been identified at registration.
- **The possibility to use multiple registrations.** The use of multiple (anonymous) registrations to purchase and sell items could create problems when screening, monitoring and reconstructing transactions and flow of funds.
- **Remote access to commercial websites and Internet payment systems.** Connection to commercial websites and Internet payment systems is available everywhere in world. A criminal can connect himself to the Internet from web terminals not affiliated or registered to his or her identity, which makes more difficult for law enforcement to locate and to pursue criminals and money launderers.
- **Relative "anonymity" associated with certain methods of payment.** With prepaid credit cards, gift cards/gift cheques[20] and when cash is used, the origin of the funds cannot be (easily) retraced[21].

Layering:

- **The speed of movement**. Transactions via commercial websites and Internet payment systems can be done very rapidly as transactions between sellers and buyers are performed electronically.

---

19 A good identification is a prerequisite for detecting a suspicion related to an individual/company but also for a serious and effective investigation of a suspicious operation.

20 Even if anonymous gift cards are generally issued for relatively small amounts.

21 Even if measures of internal control exist to monitor and to supervise the issuance of gift cards at local shops or supermarkets and the purchase of prepaid cards and avoid or survey sudden increases in the number of gift cards issued and amounts loaded (analysis of purchase details, pattern of purchases and spending locations, IP addresses, physical monitoring of premises), anonymity can be reduced but cannot be totally avoided.

- **The international character and the jurisdictional issue of where the transaction takes place.** Transactions on commercial websites and Internet payment systems can be performed across international borders and the jurisdiction where the Internet payment service provider is located may not be competent to investigate and prosecute ML or TF. Likewise, no single jurisdiction has clear responsibility for regulating and monitoring activity.

The speed of movement, the international character of the transaction and the jurisdictional issue related to the use of the commercial websites and Internet payment systems may impact on FIUs and law enforcement who investigate cases of money laundering or terrorism financing.

- **Volume - high number of transactions and amounts per transaction**[22]. The high number of transactions and consequently amounts per transactions make it more difficult for Internet Payment services providers to define criteria to monitor and screen transactions (which types of transactions should be regarded as suspicious?)[23];
- **The limited human intervention**. As less human intervention is associated with transactions via commercial websites and Internet payment systems, traditional first level detection mechanisms which rely heavily on the face-to-face relationship with the customer, are no longer available and must be replaced by sophisticated second level detection mechanisms[24].
- **The lack or inadequacy of audit trails, record keeping or suspicious transactions reporting by certain Internet payment services providers.**

Integration:

- **The possibility to buy high value items.** Buying (high value) goods, precious metals, real estate or securities on commercial websites using an Internet payment system.

[22] By limiting the use of an account, the Internet payment service provider should be able to limit the potential risk.

[23] It is worth mentioning that it is also difficult for traditional financial institutions to define criteria to monitor the transactions of their customers using computer software.

[24] If Internet payment service providers adequately monitor the financial transactions of their customers by detecting deviations from their customer's known profile of transactions, the face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem.

OVERVIEW OF REGULATIONS IMPOSED ON THE SECTOR

73. For the above-mentioned reasons, Government officials have been called on to start regulating the commercial websites and Internet payment systems fearing that criminals and terrorists could use them to launder money or finance terrorism.

General introduction

74. In general regulations are imposed to commercial websites mainly in the field of the protection of the consumer (better inform their users on their rights and duties, general terms of use and the use of electronic contracts, identification of the commercial website, advertising…), the prohibition to sell certain goods and the possibility to cancel a purchase made online.

75. For instance Electronic Commerce is regulated by means of several European Directives. The goal of the regulation is mainly to create transparency for consumers and thus give them the necessary protection. The main regulations stem from the E-Commerce Directive (2000/31/EC) and the Distance Selling Directive (1997/7/EC). The first Directive imposes several rules for transparency of the E-commerce company by obliging transparency about the nature and general information on the E-commerce company as well as transparency about the process of buying a product. The second directive states rules on revoking purchases (within certain time limits). Finally the European Regulation (2006/2004/EC) for coordination of cross-border requests for mutual assistance concerning consumer protection.

76. In the US, the Bureau of Consumer Protection of the U.S. Federal Trade Commission (FTC) works to protect consumers against unfair, deceptive, or fraudulent practices in the marketplace. The Bureau conducts investigations, sues companies and people who violate the law, develops rules to protect consumers, and educates consumers and businesses about their rights and responsibilities. The Bureau also collects complaints about consumer fraud and identity theft and makes them available to law enforcement agencies across the country.[25] The FTC's Division of Enforcement litigates civil contempt and civil penalty actions to enforce federal court injunctions and administrative orders in FTC consumer protection cases; coordinates FTC actions with criminal law enforcement agencies through its Criminal Liaison Unit; develops, reviews, and enforces a variety of consumer protection rules; coordinates multi-pronged initiatives to address current consumer protection issues; and administers the Bureau of Consumer Protection's bankruptcy programme.[26]

77. In most cases, there is no identification or STR-obligations in place for commercial websites. In The Netherlands, in case a commercial website provides payment services as well these obligations will be applicable.

78. This is consistent with the international AML/CFT standards which apply in the same manner to traditional commerce and do not require merchants to apply AML/CFT measures (CDD, cooperation with the FIU, adequate internal organization) if they do not accept cash over a preset threshold.

79. The AML/CFT obligation (among others the obligation to monitor and detect suspicious transactions) is an obligation imposed on financial institutions and e-money providers.

---

25 Federal Trade Commission (2007a).

26 Federal Trade Commission (2007b).

80. In the European Union, e-money issuers are required to be licensed, they are regulated in the country in which e-money is issued. With the European passport mechanism, an e-money issuer licensed in one European country is allowed to operate across the EU. E-money issued in one European country can be spent on a commercial website in another European country. E-money issuers are mainly located in the UK, Luxembourg, and Germany. In the US, Internet payment service providers are licensed as a money services business (MSB). Licences are also granted to Internet payment services providers in other countries such as Australia. There are apparently no regulations imposed to Internet payment services providers in China. The issuer can only issue the e-money and target customers of the country of issuance (the country where he gets the licence).

81. In the European Union, the prudential supervision of the business of e-money institutions is regulated by the EU Directive 2000/46/EC ("E-money Directive"). The directive introduces a legal framework that harmonises the prudential supervision of electronic money institutions for ensuring their sound and prudent operation and their financial integrity. The legal framework includes among others measures like the obligation to have an initial capital and requirements to own funds sufficient to cover their financial liabilities related to outstanding electronic money, limitations of investments, sound and prudent management, administrative and accounting procedures and adequate internal control mechanisms. For the purpose of the prudential supervision of electronic money institutions, the issuance of electronic money is not considered as a deposit-taking activity and subject to the supervisory regime applying to credit institutions if the received funds are immediately exchange for electronic money.

82. The EU AML/CFT Directives apply to electronic money institutions. Directive 2005/60/EC foresees simplified customer due diligence (CDD) where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where, if the device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer as referred to in Article 3 of Directive 2000/46/EC.

83. In regulated sectors like the sector of the Internet payment service providers, efforts have been made by regulators and by trade associations to develop guidance to the sector for the application of AML/CFT regulations and with fraud and ML/TF typologies exercises.

Overview by country

United Kingdom

84. The UK does not have a specific regulatory regime for electronic commerce, although the Financial Services Authority does regulate electronic money in the UK, as well as the sale of financial services by electronic means by firms in the UK.

85. E-money is defined in UK law as monetary value as represented by a claim on the issuer which is stored on an electronic device, issued on receipt of funds and accepted as a means of payment by persons other than the issuer. E-money is considered as an electronic surrogate for coins and banknotes, intended to effect payments of limited amounts.

86. The FSA's approach to regulating e-money is based on requirements of the EU's E-money Directive. E-money issuers also have obligations under the Money Laundering Regulations 2007 to, for example, apply customer due diligence measures and to undertake ongoing monitoring of their business relationships. In the event that potentially suspicious activity is detected, the firm has a legal obligation to report this to the authorities. The FSA would expect e-money issuers to be able to demonstrate that they deploy an adequate range of controls for the type of risks that they encounter. Discussion of steps that can be taken by e-money issuers to meet their legal obligations is provided by Guidance issued by the Joint Money Laundering Steering Group (JMLSG).

Luxembourg

87. The relevant Luxembourg legislation transposes the E-Money Directive and the EU AML/CFT Directives. Since July 2007 one Internet payment provider has established its EU Headquarters in Luxembourg. This entity is licensed as a bank by the Luxembourg financial sector supervisory authority, the *Commission de Surveillance du Secteur Financier* (hereafter the "CSSF"). Thus this Internet payment provider is submitted to the same AML/TF legislation and guidelines of the CSSF as any bank operating in Luxembourg. In particular it has the following obligations: costumer identification (CDD (simplified/enhanced) -on a risk based approach-), records keeping, adequate internal AML/CFT procedures, cooperation with the Luxembourg authorities (in particular with the FIU). The regime of administrative sanctions in case of breach of those AML/CFT obligations and the criminal offence in case of intentional breach of those obligations also apply.

The Netherlands

88. In the Netherlands the E-Money Directive (2000/46/EC) and Third Anti Money-Laundering Directive (2005/60/EC) apply. Payment methods on the Internet need an E-money license and a special regime will be applicable in that case. The regulatory response consists of: registration/licensing, (prudential) supervision, record keeping, suspicious transaction reporting, other specific AML policies & procedures (CDD-regulation). The providers who have a waiver have a less burdensome regime. The regulatory response consists of: record keeping, no suspicious transaction reporting, no other specific AML policies & procedures. Explicit waivers have been given for prudential purpose to five E-money institutions. Furthermore payment providers often have developed a self regulatory approach to a certain extent. The main goals for this approach are to protect the good name of the company, judicial liability issues and credit risks.

United States

89. Banking organizations that provide payment methods used for electronic commerce in the United States are subject to a full range of AML/CFT requirements, including among other things, requirements to: detect and report suspicious transactions; maintain records of funds transfers, and to implement AML compliance and customer identification programs. The cornerstone to this strong AML compliance program is the adoption and implementation of comprehensive customer due diligence policies, procedures, and processes for all customers. These processes assist U.S. banking organizations in determining when transactions are potentially suspicious.

90. When a banking organization within the United States determines a transaction is suspicious, it is required to file a Suspicious Activity Report (SAR) with the U.S. financial intelligence unit, known as the Financial Crimes Enforcement Network (FinCEN). Banking organizations within the United States are required to report transactions involving or aggregating to at least USD 5 000 that are attempted or conducted by, at, or through the institution in which the organization "knows, suspects, or has reason to suspect" the transaction: *i)* involves funds derived from illegal activities or is conducted to disguise funds derived from illegal activities, *ii)* is designed to evade the reporting or record keeping requirements of the Bank Secrecy Act (BSA) (*e.g.* structuring transactions to avoid currency transaction reporting), or *iii)* "has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the banking organization knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction."

91. The Federal banking agencies and the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) are the primary government agencies responsible for enforcing compliance with the relevant AML/CFT regulations.

92. The U.S. Federal banking agencies have been charged (under U.S. Federal banking laws 12 USC 1818(s) and 12 USC 1786(q) for banks and saving banks) with ensuring that banking organizations, subject to their respective jurisdictions, maintain effective Bank Secrecy Act/Anti Money Laundering compliance programs.

93. Several other regulations apply to electronic funds transfer activities. They concern the rights, liabilities, and responsibilities of parties in electronic fund transfers (EFT) and protect consumers using EFT systems, such as ATMs and debit cards.

Singapore

94. E-money is broadly referred as Stored Value Facility (SVF) in Singapore. Under Singapore law, a SVF is a form of prepaid electronic cash or card that can be used within the system of the SVF issuer. The SVF issuer is also known as the holder of the SVF.

95. The issuance and management of SVFs are governed by the Payment Systems (Oversight) Act 2006 (PS(O)A) and its related regulations[27]. Any entity can issue a SVF and hold the stored value. However, SVF with total outstanding stored value exceeding SGS 30 million will require approval from the Monetary Authority of Singapore (MAS) and a bank licensed by the MAS to be fully liable for the stored value. SVFs whose aggregated stored value falls below the prescribed SGD 30 million do not require MAS' approval to operate but are required to provide disclosure to advise potential users that such SVFs are not subject to MAS' approval.

96. In addition to the PS(O)A regulatory requirements, any holder SVF which issues a SVF that has a load limit of more than SGD 1 000 has to adhere to and apply the MAS AML/CFT Notice to holders of SVF on the prevention of money laundering and countering the financing of terrorism[28].

97. The Notice imposes preventive measures to holders to limit the risk of SVFs being used for illegitimate purposes. The Notice sets out obligations which require holders to take measures to mitigate money laundering and financing of terrorism risk in the following fields; *i.e.* due diligence measures (simplified, enhanced), identification of users (customers), verification of identification of users, identification and verification of identities of Beneficial Owners, non face-to-face verification, review of relevant transactions, record keeping, suspicious transactions reporting, internal policies, audit and training.

98. Any holder of SVF which fails or refuses to comply with the requirements under the Notice shall be liable on conviction to a fine not exceeding SGD 1 000 000 and, in case of a continuing offence, to a further fine of SGD 100 000 for every day during which the offence continues after conviction (under section 27B of the MAS Act[29]).

99. The MAS has also issued SVF Guidelines[30] which recommend sound principles and risk mitigating factors for all holders of SVFs. These principle-based recommendations address issues such as transparency, disclosure, public confidence, stored value protection, prevention of money laundering and countering the financing of terrorism.

---

27 *Payment Systems (Oversight) Act 2006 (PS(O)A).*

28 Monetary Authority of Singapore, (2007).

29 *Monetary Authority of Singapore Act (Chapter 186).*

30 Monetary Authority of Singapore, (2006).

China

100. There are no regulations in place addressing Electronic Commerce or Internet payment systems in China. Nevertheless, on 13.12.2007, the Chinese Ministry of Commerce issued an opinion on Enhancing the regularised Development of Electronic Commerce. The objectives of the guidance are to help the third-party electronic payment service providers to improve the reputation of the industry, operate in a prudent and stable manner, prevent blind business expansion and out-of-order competition, and ensure the safety of users' funds. The guidance encourages measures like standardised operation and management, overseeing business flow, secure electronic payment, keeping transaction data, and prevents online illegal financial transactions …

Hong Kong, China

101. Hong Kong, China does not have licensing systems for e-money and Internet payment service providers. In Hong Kong, China, 'e-money' is very much represented by Multi-purpose stored value cards. Institutions in Hong Kong China issuing or facilitating the issuance of Multi-purpose stored value cards must be authorised by the Hong Kong Monetary Authority (HKMA) under the Banking Ordinance, Cap. 155 (BO)[31]. These institutions are called authorised institutions (AIs) and are subject to supervision of the HKMA.

102. Internet payment service providers, in Hong Kong, China, only provide a platform for the users to settle various types of payment through transferring money from their designated bank accounts to that of the vendor of goods or services. Nevertheless, when such service providers carry on a business of taking deposits and cash, they have to get a licence from HKMA to conduct business as an AI.

103. The HKMA has set out various supervisory policies and requirements to be observed by AIs in the form of supervisory guidelines. The supervisory guidelines issued by the HKMA with respect to AML/CFT are the "Guideline on Prevention of Money Laundering" and the "Supplement to the Guideline on Prevention of Money Laundering". These guidelines are issued in the form of a statutory guideline pursuant to section 7(3) of the BO. These guidelines impose obligations on AIs to put in place effective systems and procedures for combating money laundering and terrorist financing and are developed based on the latest international standards including the current 40 Recommendations on anti-money laundering and 9 Special Recommendations on countering the financing of terrorism of the FATF. The requirements in these guidelines apply to AIs which issue Multi-purpose stored value cards.

104. Under the AML/CFT guidelines, AIs are required to *i)* conduct the customer due diligence process to identify and verify the identity of their customers and the beneficial owners of their customers using reliable, independent source information, *ii)* obtain information on the purpose and intended nature of the business relationship, and *iii)* conduct on-going due diligence and scrutiny of transactions throughout the business relationship. AIs are required to adopt a risk-based approach in their CDD process. AIs should develop customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher money laundering/terrorist financing risk. For those customers identified with higher ML/TF risk, AIs should adopt a more extensive customer due diligence process and subject them to close monitoring. In undertaking the CDD

[31] A Multi-purpose stored value card is defined in the BO as a card on which data may be stored in electronic, magnetic or optical form and for or in relation to which a person pays a sum of money to the issuer of the card (directly or indirectly) in exchange for *i)* the storage of the value of that money, in whole or in part on the card; and *ii)* an undertaking by the issuer (express or implied) that the issuer or a third party will, on production of the card, supply goods and services (which may include money). There is currently only one issuer of Multipurpose stored value cards (*i.e.* Octopus Cards Limited) in Hong Kong, China. The Octopus Cards Limited is authorised as a deposit-taking company under the BO. Octopus cards are designated for small amount retail payments and there is a maximum storage limit of HKD1 000 per card.

process, AIs should, whenever possible, conduct a face-to-face interview with a new customer to ascertain the customer's identity and background. In cases where a face-to-face interview is not conducted, they should apply equally effective customer identification procedures and on-going monitoring standards to mitigate the risk. The AML/CFT guidelines also require AIs to keep proper account and transaction records.

105. Section 25A of the Organised and Serious Crimes Ordinance, CAP 455, (and similar provisions under Hong Kong's anti-terrorist financing legislation) provides requirements for reporting of suspicious transactions by all persons in Hong Kong to Hong Kong's Joint Financial Intelligence Unit, (JFIU). Failure to report a suspicious transaction is a criminal offence. All parties engaged in financial transactions of any kind must have systems in place to detect suspicious transactions to comply with this law, but the exact methods used are the responsibility of each company. Moreover, under the HKMA's AML/CFT guidelines, AIs should put in place effective management information systems to enable them to identify and report suspicious transactions. The Organised and Serious Crime Ordinance and Drug Trafficking (Recovery of Proceeds) Ordinance, (and similar provisions under Hong Kong's anti-terrorist financing legislation) makes provision for reporting of STRs to the JFIU. The reporting obligations apply to any person who knows or suspects that any property represents any person's proceeds of an indictable offence, or the property was used in connection with or is intended to be used in connection with an indictable offence, he shall disclose that knowledge or suspicion to an authorised officer (*i.e.* JFIU officer) as soon as practicable.

106. The HKMA ensures compliance of AIs with its AML/CFT guidelines through its on-going supervisory process. If an AI fails to comply with a requirement under the AML/CFT guidelines, the HKMA will require the AI to take appropriate remedial actions to rectify the situation. The HKMA will follow up with the AI to ensure that the deficiency has been satisfactorily addressed. Where the non-compliance is considered to be serious, the HKMA will impose supervisory measures against the AI[32].

Australia

107. Payment methods are regulated largely by a combination of the Payments System (Regulation) Act 1998, the Payment Systems and Netting Act 1998, and the Electronic Funds Transfer (EFT) Code. The Reserve Bank of Australia (RBA) administers the Payments System (Regulation) Act 1998, and the *Payment Systems and Netting Act 1998* with the goal of achieving efficiency, competition and stability. The Australian Securities and Investments Commission administers the EFT Code with the goal of providing consumer protection.

108. Australia's primary anti-money laundering and counter-terrorism financing (AML/CTF) legislative package includes the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) and Anti-Money Laundering and Counter Terrorism Financing Rules. The AML/CTF Act sets out general AML/CTF principles and obligations. With the details of how these obligations are to be carried out being set out in subordinate legislative instruments known as the AML/CTF Rules.

109. The AML/CTF Act covers the financial sector, gambling sector and bullion dealing and any other professionals or businesses that provide particular designated services. Being activities-based,

[32] There is a broad range of supervisory measures available to the HKMA. They include for example issuing a statement of warning to the senior management of the AI, imposing restriction on the AI's business, downgrading the supervisory ratings of the AI and commissioning an external auditor to review the AML/CFT system of the AI. In the event that the AI fails to take appropriate remedial actions, the HKMA will consider exercising its formal powers under the BO, which include withdrawing the consent given to the responsible directors and chief executives, attaching conditions to the AI's authorisation, requiring the AI to seek advice from an Advisor appointed by the HKMA and suspending or revoking the authorisation of the AI. The supervisory measures to be taken in each case will depend on the seriousness of the deficiencies identified in the AI and are considered to be effective, proportionate and dissuasive.

under the AML/CTF, it does not matter how designated services are provided (*i.e.* electronic, paper or face to face).

110. The AML/CTF Act imposes a number of obligations on businesses (called reporting entities) when they provide these designated services. These obligations include: customer due diligence (identification, verification of identity and ongoing monitoring of transactions); reporting (suspicious matters, threshold transactions and international funds transfer instructions); record keeping, and establishing and maintaining AML/CTF program.

111. The AML/CTF Act implements a risk-based approach to regulation. Businesses are able to determine the way in which they meet their obligations based on their assessment of the risk of whether providing a designated service to a customer may facilitate money laundering or terrorism financing. The AML/CTF Rules specify how the obligations may be complied with by a reporting entity putting in place appropriate risk-based systems and controls. When determining and putting in place appropriate risk-based systems and controls, the reporting entity must have regard to the nature, size and complexity of its business and the type of ML/TF risk that it might reasonably face. In identifying its ML/TF risk a reporting entity must also consider the risk posed by the following factors: its customer types, including any politically exposed persons, the types of designated services it provides, the methods by which it delivers designated services; and the foreign jurisdictions with which it deals.[33]

112. The Australian Prudential Regulation Authority (APRA) authorises certain e-commerce payment mechanisms to be a Purchased Payment Facility (PPF). PPFs, such as smart cards and electronic cash, are facilities which consumers pay for in advance and use to make various types of payments. Consumers rely on the holder of the stored value redeeming that value on demand.

113. APRA's prudential standard regarding PPF's seeks to ensure that those who provide PPF facilities are subject to prudential requirements commensurate with their risk profile. A PPF provider is not authorised to conduct general banking business. Under the prudential standard, a PPF provider is required to comply with AML/CTF requirements as administered by AUSTRAC (under the Anti-Money Laundering and Counter-Terrorist Financing Act 2006).

114. APRA also authorises those who carry on a credit card issuing and/or acquiring business in Australia as a "specialist credit card institution" (SCCI). SCCIs are a special class of authorised deposit-taking institutions (ADIs) that are authorised to perform a limited range of banking activities. SCCIs may only perform credit card issuing and/or acquiring business and any other services related to credit card issuing and/or acquiring. SCCIs are not permitted to accept deposits (other than incidental credit balances on credit card accounts).

[33] [Australian] Attorney-General's Department (2007).

RISK MANAGEMENT MEASURES TAKEN BY THE SECTOR

Introduction

115. As with any type of business, commercial websites and Internet payment systems are confronted with various types of risks ranging from the technical safeguards of their websites from computer hackers and viruses to the outright criminal misuse of their systems by criminals for purposes of facilitating fraud, and Internet payment systems for money laundering and other financial crimes. Risk management is therefore an ongoing process that may be developed by commercial websites and Internet payment systems to minimise their exposure to various risks. This may include the establishment of customer user agreements and policies by a company that set strict rules and policies for the use of their respective system by a user. In addition, commercial websites and Internet payment systems may also establish "best practices" designed to set internal standards for how a company may safely operate while at the same time providing effective services to their users. Risk management may also encompass Anti-Fraud and Anti-Money Laundering/Terrorist Financing (AML/TF) programs that may have been implemented by commercial websites and Internet payment systems. Finally, a risk-based approach may also integrate other initiatives that are undertaken by a commercial websites and Internet payment systems that are required under the regulatory regime of a specific country or jurisdiction where a commercial websites and Internet payment systems may provide services, *e.g.* reporting requirements (for Internet payment systems), etc. Other stakeholders (such as the tax authorities and authorities supervising payments) are or must be involved in the fight against ML or TF and the mitigation of ML or TF risks. If commercial websites have no reporting obligations they are controlled by these stakeholders.

AML/CFT mechanisms used to mitigate fraud, money laundering and terrorism financing risks

116. Internet Payment service providers, subject to regulations from a supervision authority, mitigate the above mentioned ML/TF risks by applying different mechanisms. During the study the project team obtained confirmation on the use of such mechanisms by consulting, as mentioned in the introduction, one of the most important mediated customer-to-customer commercial websites and Internet payment service provider as well as a smaller electronic money issuer and the Electronic Money Association representing a range of e-money issuers and payment service providers. The project team also obtained confirmation that AML/CFT regulations imposing similar mechanisms apply to Internet payment service providers in the most industrialised countries.

117. A non-exhaustive list of these mechanisms is provided in this section:

- Implementing important worldwide security teams patrolling sites to detect fraud and misuse.
- Applying risk-based Customer Due Diligence (simplified CDD vs. enhanced CDD).
- Scoring customer risk at opening of account.
- Risk-based verification of information entered by customers (e-mail address/IP address, identity of credit card holder, stolen credit cards …).
- Automated call, random charges to verify identities of customers.
- Sending a letter to verify customers address.
- Credit cards address verification.

- Consulting commercial databases to confirm information received from customers;
- Phone calls by staff to obtain additional information from customers.
- Activity limits, sending and withdrawals limits.
- Verification of funding source.
- Real time screening of customers, their activities and items sold.
- Monitor, using risk models built to detect bad activities, information:
  - obtained from customers (identity, address, e-mail and IP addresses used, About Me page, …)
  - collected from customers (phone call to sellers, …)
  - obtained internally (previous transactions, item country location, customer location, shipping methods used, behaviour of customers during auction processes, accepted payments, …)
  - obtained from external sources (countries at risk for certain forms of criminalities, check listings of presumed terrorists or terrorist groups, …)
- Risk models to detect abnormal (with regards to previous transactions) or high volume activity.
- Models/software to detect suspicious activities (based on various red flags and indicators).
- Manual review of abnormal transactions and of higher use accounts.
- Detect abnormal and suspicious activities in withdrawals.
- Refuse transactions on prohibited items (drugs, firearms, counterfeit products…).
- Remove offending items from the website.
- Cooperate with commercial company to detect counterfeit products and remove them from sales.
- Analyse the physical and electronic evidence left by criminals on the net.
- Delay a transaction.
- Display message to customers on regulation applying to certain countries and transactions.
- Encourages the reporting of suspicious items on sale, suspicious auctions or suspicious behaviour of customers (sellers or buyers) – scoring of customers (buyers and sellers by each other).
- Does not accept or distribute cash.
- Maintain full audit trails of commercial transactions and payments.

118. The most organised Internet payment service providers collect a range of data and information about movements of funds between buyers and sellers, located in different countries all over the world but customers of the same Internet payment service provider, commercial transactions between buyers and sellers, data and information accumulated over a long period of time and available centrally.

119. Consequently, they have a global view of the movements of funds and the commercial transactions between buyers and sellers internationally, information that the banks of buyers and sellers do not have. They can easily reconstruct commercial transactions and movements funds between different countries and persons in the world.

120. Certain Internet payment service providers have the opportunity to access data and information on the commercial transaction underlying a financial movement of funds because they provide payment facilities to commercial websites belonging to the same financial group. Nevertheless, certain Internet payment service providers providing payment facilities to commercial websites not belonging to the same financial group can also obtain but in a more limited way information on underlying commercial transactions.

121. An easy data sharing of information with commercial websites reduces the risks of misuse and the risks of ML/TF.

122. If Internet payment service providers adequately monitor the financial transactions of their customers by detecting deviations from their customer's known profile of transactions, the non face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem.

123. Nevertheless, it is worth mentioning that an Internet payment service provider will be able to build a better and much accurate customer's profile of transactions if the number of transactions performed by a customer is significant.

124. Exchange of information between commercial websites and Internet payment services providers possibly located in different countries is sometimes not easy because of the differences in the privacy legislation.

125. As already mentioned in the subsection regarding regulations, AML/CFT reporting obligations are applicable to Internet payment service providers in the country in which they are physically located. Certain commercial websites and Internet payment service providers work closely with law enforcement. They encourage regulators and law enforcement to play an active role in the fight against the use of commercial websites and Internet payment service providers for criminal activities.

CONSIDERATIONS ON "SECOND LEVEL OF CONTROLS VERSUS THIRD LEVEL CONTROLS"

126. Internet payment service providers, licensed as e-money providers or as a bank, have several obligations in the field of identification of customers, detection, monitoring and reporting of suspicious financial transactions. As explained in the section above, they have access to a wide range of information for monitoring the transactions of their customers and certain Internet payment service providers have implemented ongoing due diligence mechanisms which include: scrutiny of transactions undertaken throughout the course of the relationship to ensure the transactions conducted are consistent with their customer's known profile. In many cases, the profile of a customer can only be deducted from previous transactions with the payment service provider.

127. When services of Internet payment services providers are used, banks of buyers and sellers do not have a global view of the flow of funds between buyers and sellers, as this information is only known by the Internet services provider itself. A customer of a bank may order his bank to transfer funds from his bank account to his account with an Internet payment service provider. Afterwards the customer will request the Internet payment service provider to transfer funds for a purchase on a commercial website. The bank can be totally unaware of this purchase and the reasons for funding the account with the Internet payment service provider. In the United States, similar cases have been identified with payments requested by customers of banks in favour of Internet payment service providers and used thereafter by these customers on gambling websites, without the bank knowing the funds were used for this illegal activity in the United States.

128. But banks still have an important role to play in the monitoring and detection of suspicious transactions, even if the funds are transferred to or originate from an Internet payment service provider. For instance, a transaction with an Internet payment service provider can be abnormal or disproportionate to the bank with regards to the known profile (professional activities, professional revenues, customer bank transactions profile) of its customers.

129. It is also important that financial institutions, such as the banks, do not exonerate themselves from their AML/CFT responsibilities, in particular the detection of suspicious financial transactions, when the funds originate from an Internet payment service provider, and even if the transactions concern relatively small amounts. A statement or a printout of a screen of the commercial website showing an item on sale must not immediately and unconditionally considered as an invoice or justifying a financial transaction on the bank account of the customer. Conversely, the presentation of such justification document could be used as a red flag or indicator for the financial institution.

POLICY IMPLICATIONS

130. ML/TF risks associated with commercial websites and Internet payment systems have been analysed and the focus has been put on the type of electronic commerce identified for various reasons (increasing popularity, easy access, available to private individuals, high volume of cross border trade transactions …) as the most susceptible to be used by criminals for ML/TF: mediated customer-to-customer. The work of the project team has led to the following key findings with respect to ML/TF vulnerabilities of commercial websites and Internet payment systems.

Key findings

131. Criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. As the Internet becomes more and more a worldwide phenomenon, commercial websites and Internet payment systems appear to be subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist groups.

132. Various vulnerabilities of commercial websites and internet payment systems have been highlighted: the non face-to-face registration which may lead to identification problems; the speed of transactions, the limited human intervention and the high number of transactions, which may cause problems concerning audit trails, monitoring and detection of transactions; the international character, which is inherent to the Internet, which may create issues concerning jurisdictional competences; difficulties for traditional financial institutions to monitor and detect suspicious financial transactions with the consequence that their abilities in the detection of suspicious financial transactions, when an Internet payment service provider is used, could be affected.

133. Some of the ML/TF risks associated with trade-based money laundering and non face-to-face business and financial transactions apply also to commercial websites and Internet payment systems. The financial transactions that are initiated from a bank account or a credit card (which is the majority of online payments) already involve a customer identification process as well as transaction record keeping and reporting obligations. While low value transactions do not equate to low risk, these transactions are subject to the regulatory controls already applicable to the financial sector and may be consequently less risky. Regarding the risks associated with the non-face-to-face registration and the possible anonymity of the users the study highlights the need for online identity verification solutions (the electronic identity card used in certain countries for instance) to help commercial websites and Internet payment service providers mitigate the risks of criminal activity. The report also indicates that if Internet payment service providers adequately monitor the financial transactions of their customers, monitoring for and acting on deviations from the customer transaction profile, the lack of face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem. Online and offline retail merchants and payment services should have comparable AML/CFT obligations.

134. It is also important that efforts to fight against fraud and ML/TF by commercial websites and Internet payment service providers in different countries not be hampered by divergent privacy legislation, potentially interfering with the amount of customer information that service providers could exchange regarding suspected ML/TF.

135. Although the challenges to identifying TF apply equally to Internet payment systems (the suspicions being mostly based on name matching with the names provided by the competent authorities), it is not always necessary for Internet payment service providers to identify TF in their

STRs in order to help counter terrorist financing. Any suspicious activity is important to report regardless of the type of activity. Some Internet payment service providers have put in place systems to detect, monitor and analyse suspicious transactions - even for small amounts.

136. Concerning the risk-based approach to combat ML/TF we can refer to the June 2007 FATF Guidance which states that : "By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention." Applying this principle to online transactions, the private sector may be allowed to consider low value consumer payments initiated from financial institutions or credit card account (which require customer identification and verification procedures, as well as transaction record-keeping and reporting policies), to be of lower risk than transactions initiated through services providers without AML/CFT obligations.

137. The risk of fraud and the sale of illegal goods are among the concerns of commercial websites and Internet payment systems. These concerns are among the motives for commercial websites and Internet payment systems to secure their communications, websites and payment systems. In some jurisdictions online commercial websites are not as such required to detect or fight against ML/TF, but have a market incentive to detect fraud.

138. Some commercial websites and Internet payment service providers, aware of the risk of being used for illegal activity, have set up departments to screen and monitor the transactions of their customers, using a risk-based approach. In addition to monitoring for fraud, some commercial websites and Internet payment service providers have also set up AML/CFT mechanisms. Best practices in the sector, including customer due diligence, monitoring transactions, not accepting anonymous forms of payment (cash for instance) imposing transactions limits, maintaining transactions records, and reporting large or suspicious transactions to the competent authorities, could be helpful for other parties of the private sector.

139. The collaboration between commercial websites and Internet payment service providers to exchange information on commercial transactions underlying financial transactions is a factor which mitigates money laundering and terrorism financing risks, as well as risk of fraud. Legal dispositions encouraging such exchange of information could be very useful.

140. The report concludes that, as long as the sector, and the relevant competent authorities, understand the potential vulnerabilities associated with commercial websites and Internet payment systems and appropriate risk-based measures with regard to customer identification, record keeping and transaction reporting are taken, the mentioned issues may not necessarily constitute a higher risk for the online sector than for the offline sector.

141. The project team believes that even though awareness of ML/TF amongst major players in the online sector is increasing, due to efforts made by regulators and trade associations, efforts need to be made to increase this awareness, particularly regarding the mechanisms of ML/TF.

142. Given the international character of commercial websites, international cooperation is a key factor. Cooperation between, for example, FIUs, law enforcement and other parties involved is therefore important. Internet payment service providers report in the country where they are established (got a license) and not in the country of residence of the individuals involved in the suspicious financial transactions, which for FIUs and law enforcement may lead to identification and follow-up problems (it is difficult to confirm the true identity of the parties involved in the transactions in the country of the disclosure given that the individuals do not live in the country and the transactions are difficult to explain / justify as they does not take place in the country where the Internet service provider is located and reports.

Issues for consideration

143. Looking ahead, there appear to be a number of areas that could be considered to improve the capacity to cope with ML/TF risks associated to commercial websites and Internet payment systems.

144. **Building a better awareness:** Creating an understanding of the ML or TF risks amongst governmental bodies and the private sector is critical. Making the traditional financial institutions aware of their role in the detection and the monitoring of suspicious financial transactions. Therefore it is necessary to raise awareness by identifying red flags and typologies. Awareness could also be raised by training programs and outreach sessions to the private sector. The regulators and trade associations which have already contributed to the issuance of AML/CFT guidance to the sector and the development and issuance of ML/TF typologies could be of great help.

145. **Imposing similar regulations**: Given the international character and presence of Internet, it is difficult to determine which jurisdiction has regulatory authority over an Internet payment service provider, and how enforcement action can be applied if there are violations. World based Internet payment service providers have locations and licences in different countries and regions. It is consequently important that governments impose similar regulations, requiring customer identification, CDD, record keeping and transaction reporting, to Internet payment service providers all around the world, to avoid certain Internet payment service provider choosing the country with the poorest regulations or not at all regulated.

146. **Exploring industry best practices**: The high standard for customer due diligences and the sector best practices (monitoring of transactions, non-acceptance of certain forms of payment (cash for instance) considered as high risk for ML/TF, limits imposed to transactions, …) identified during the workshop and presented in the report could be helpful for other players in the private sector and could be an important part of the training programs and outreach sessions to the private sector.

147. **Bearing in mind that international cooperation is a key factor**: International cooperation is a key factor in the fight against ML and TF given the international character of the Internet and commercial websites activities. Countries need to work cooperatively to identify and combat the use of commercial websites and Internet payment systems for ML/TF purposes. International cooperation to ensure that entities operating in multiple jurisdictions are being properly regulated and monitored somewhere is also important.

148. Approaching the Egmont group in order to discuss the awareness raising amongst FIUs in view of combating ML/TF via commercial websites and Internet payment systems: There is a need to explore ways FIUs can enhance the exchange of information and data pertaining to the criminal misuse of commercial websites and Internet payment systems.

REFERENCES

[Australian] Attorney-General's Department (2007), *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*, accessed through: *www.comlaw.gov.au*.

FATF (2006a), *Report on New Payments Methods*, FATF, Paris, *www.fatf-gafi.org*.

FATF (2006b), *Trade-based Money Laundering*, FATF, Paris, *www.fatf-gafi.org*

FATF (2007), *Guidance on the Risk-Base Approach to Combating Money Laundering and Terrorist Financing, High Level Principles and Procedures*, FATF, Paris, *www.fatf-gafi.org*.

Federal Trade Commission (2007a), "*About the Bureau of Consumer Protection*", Federal Trade Commission web site, *www.ftc.gov/bcp/about.shtm.*

Federal Trade Commission (2007b), "*Division of Enforcement*", Federal Trade Commission web site, *www.ftc.gov/bcp/about.shtm.*

Monetary Authority of Singapore, (2006), "*Stored Value Facilities Guidelines"*, accessed at: *www.mas.gov.sg/resource/legislation_guidelines.*

Monetary Authority of Singapore (2007), *Prevention of Money Laundering and Countering of Terrorism – Holders of Stored Value Facilities*, Notice PSOA-No.2, Singapore, accessed at: *www.mas.gov.sg/resource/legislation_guidelines*.

Monetary Authority of Singapore Act (Chapter 186), http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-186&doctitle=MONETARY%20AUTHORITY%20OF%20SINGAPORE%20ACT%0a&date=latest&method=part.

Munro, Neil (2001), "*Internet-Based Financial Services: A New Laundry?*", *Journal of Financial Crime*, Henry Stewart Publications, Vol. 9, No. 2, pp. 134-152, Henry Stewart Publications.

Philippsohn, Steve (2001), "*The Dangers of New Technology – Laundering on the Internet*", *Journal of Money Laundering Control*, Henry Stewart Publications, Vol. 5, No. 1, pp. 87-95.

[Singapore] *Payment Systems (Oversight) Act 2006 (PS(O)A)* accessed at: *www.mas.gov.sg/legislation_guidelines/payment_system/payment_act2006/Payment_Systems_Oversight_Act_2006.html.*

***

Appendix PP:

FATF, *FATF Report: Money Laundering and Terrorist Financing Related to Counterfeiting of Currency* (Paris: FATF, 2013)

FATF

FATF REPORT

Money laundering and terrorist financing related to counterfeiting of currency

June 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

CASE STUDIES

CHARTS

ABBREVIATIONS

AML	Anti-Money Laundering
APG	Asia Pacific Group on Money Laundering
CCC	Currency Counterfeiting Convention
CCN	Counterfeit Currency Notes
CDD	Customer Due diligence
CFT	Combating financing of terrorism
DNFBP	Designated Non-Financial Business and Professions
EAG	Eurasian Group on Combating Money Laundering and Terrorist Financing
ECB	European Central Bank
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Bodies
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
LEA	Law enforcement authority
ML	Money Laundering
MVTS	Money and value transfer service
OC	Organised crime
OCG	Organised criminal group
OCTA	Organized Crime Threat Assessment
OECD	Organisation for Economic Co-operation and Development
TF	Terrorist Financing
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
USSS	United States Secret Service

DEFINITIONS

Currency:

The CCC 1929 defines currency in Article 2 as "paper money (including banknotes) and metallic money, the circulation of which is legally authorized".

Currency counterfeiting:

Article 3 of the CCC 1929 refers to "fraudulent making or altering of currency, whatever means are employed".

League of Nations' Currency Counterfeiting Convention (CCC) 1929:

League of Nations International Convention for the Suppression of Counterfeiting Currency of 1929.

Money laundering:

The definition is provided in the Article 6 of the *UN Palermo Convention 2000*:

> *The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action; The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; Subject to the basic concepts of its legal system: The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime; Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.*

Money laundering offence:

"[R]efers not only to the primary offence or offences, but also to ancillary offences" (FATF, 2013: 119).

Organised criminal group:

Article 2 of the *UN Palermo Convention 2000* defines *organised criminal group* as being "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit".

UN Palermo Convention 2000

The United Nations Convention against Transnational Organized Crime 2000

Terrorist:

"Any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of

terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act".[1]

Terrorist act:

The FATF standards define terrorist act according to the *International Convention for the Suppression of the Financing of Terrorism* (1999). A terrorist act therefore includes:

> (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties:
>
> *(i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970);*
>
> *(ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971);*
>
> *(iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973);*
>
> *(iv) International Convention against the Taking of Hostages (1979);*
>
> *(v) Convention on the Physical Protection of Nuclear Material (1980);*
>
> *(vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988);*
>
> *(vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005);*
>
> *(viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005);*
>
> *(ix) International Convention for the Suppression of Terrorist Bombings (1997); and*
>
> *(x) International Convention for the Suppression of the Financing of Terrorism (1999).*
>
> (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act[1].

Terrorist financing:

Refers to the financing of terrorist acts, and of terrorists and terrorist organisations (FATF glossary)[1].

Terrorist financing offence:

Refers not only to the primary offence or offences, but also to ancillary offences[1].

---

1 FATF (2012), *p.* 122.

Terrorist organisation:

"Any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act".[2]

[2] FATF (2012), *pp*. 122-123.

EXECUTIVE SUMMARY

The counterfeiting of currency emerged as a violation of law at the same time that "money" became a standardised unit of exchange. From Sumerian coin shell money to metallic coins and finally the introduction of paper money, it has always been a high profit-generating crime for individuals and criminal groups alike. With the increased demand and its acceptance beyond local markets, ample opportunities arose for counterfeiters. Over time it has evolved into more serious forms and has been, and continues to be, used as a means of economic warfare.

FATF Recommendation 3 designates counterfeiting currency as a predicate offence for money laundering (ML). However, specific aspects linked with the offence of currency counterfeiting such as the production of counterfeit currency, its smuggling and placement into the financial system, and laundering of proceeds, have not been considered directly in typologies research to better understand the differences and similarities between counterfeiting as predicate offence and the related methods of laundering these proceeds. This research project provides an overview of these different aspects of counterfeiting of currency and focuses on its relation with organised crime (OC), ML and terrorist financing (TF). It identifies and describes ML and TF aspects associated with counterfeit currency. The findings of the report are based on general research in Open Sources, on expert knowledge, and were supported by the input from 25 countries (see Annex 1) who responded to a survey developed by the research team.

The counterfeiting of currency is a widespread phenomenon. While it should be relatively easy to detect counterfeit banknotes with the “feel-look-tilt” features that many physical currency notes possess, it has become increasingly difficult for some counterfeits to be identified, especially those printed by offset printing method and with innovative techniques used to imitate some of the security features. The seizure of “high quality” counterfeit currency notes (CCN) in multiple jurisdictions throughout the world appears to indicate the involvement of criminal groups operating internationally. Organised Criminal Groups (OCGs) based in one country have been found to be smuggling counterfeit currency of other countries. These criminal groups use their already existing infrastructure in terms of a covert network of smugglers and ML businesses to introduce counterfeit currency into the financial system to multiply their profits.

Research on the involvement of OC networks in the production and distribution of counterfeit money is readily available. However, reliable and public available information on TF by means of counterfeit money is comparatively rather scarce. Six of the countries responding to the survey reported the linkage of counterfeit currency with OC and TF: India, Kyrgyzstan, Nepal, Russia, Tajikistan and the United States. They also refer to links between OCG and terrorism, including TF and the use of counterfeit money as a means of economic warfare.

Counterfeiting has become attractive to terrorists and their sympathisers, as it is very profitable, particularly when comparing the associated risks to those of other forms of criminal activity such as trafficking in drugs. While OCGs carry out currency counterfeiting throughout the world as one of many criminal activities, currency counterfeiting for the purpose of financing terrorism is seen only in certain regions. Academic research suggests that terrorist organisations active in Europe, Asia, and Latin America, rely on common criminal activities such as extortion, kidnapping, narcotics

trafficking, counterfeiting and fraud, to finance their operations and even forge relationships with OCGs. The survey responses indicate that the nature, intensity and character of the nexus between currency counterfeiting and TF have not been a subject of serious scrutiny.

Counterfeiting has evolved from a mere criminal activity generating proceeds that are then also used to fund terrorism, into an activity intended to replace real currency. In certain instances, particularly during wartime, the infiltration of high-quality counterfeit notes has been used to attack the economy of a country in an effort to erode the faith in its currency.

Since the counterfeiting of currency has an international dimension, it also becomes imperative to move the proceeds across international borders. Furthermore, the very activity of trafficking counterfeit notes results in their introduction into the regular financial stream. In this respect, the methods for introduction of counterfeit notes into a financial system are very similar to those used for "placement" of illicitly generated proceeds by other types of criminal activity. This means that a large scale currency counterfeiting operation can only be called effective when the laundering of the criminal proceeds is effective too.

The survey indicates that the most frequently used method to move the proceeds of crime is the use of cash couriers. For layering and integration of proceeds of crime related to counterfeit currency, the most frequently used techniques are intermingling in cash-intensive business, movement through multiple jurisdictions, movement through multiple accounts and false or misleading declaration of goods and services.

This study sets out a series of red flag indicators, which will help identify ML techniques related to currency counterfeiting crimes. It also highlights areas for improvement in the co-operation between Law Enforcement Agencies (LEAs) and Financial Intelligence Units (FIUs).

Governments around the world periodically review the security features of their currencies to protect against the threat of counterfeiting. Financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) by virtue of handling large volumes of physical currency have to be particularly alert in ensuring action against counterfeiting within the financial system. To do this, they need to develop and implement preventive measures for the detection and reporting of counterfeit currency notes (CCN), as well as carry out training and awareness-raising.

Legal provisions criminalising the act of counterfeiting currency as well as laundering its illegal proceeds have been established in most jurisdictions. However, the responses to the survey appear to indicate that national legislation generally focuses more on the ML and/or TF activities – with currency counterfeiting by default as one of the predicate offences – rather than foreseeing specific ML/TF activity in counterfeit currency related provisions.

The legal provisions criminalising the act of counterfeiting currency focus on this activity per se, although counterfeiting currency remains a predicate offence to ML in the legislations of many countries. The responses to the survey indicate that there is generally very low focus on the ML and/or TF activities associated with this crime.

Armed with legal provisions, police and customs authorities play a very important role, especially in the conduct of intelligence-led operations and the seizure of counterfeit currency. Data from past

operations are collated to study emerging trends. Trends and intelligence gathered are used in profiling offenders and routes and in identifying possible *modi operandi*[3].

The survey reveals that the national legislation in many countries permits special investigation techniques such as undercover/sting operations, intercepting communications, controlled delivery, tracing and recovery of assets, confidence buys to be used in counterfeiting investigations. However, the extent of the use of these techniques by LEAs is sometimes limited due to resources and restrictive laws, which consequently hinders effective cross-border co-operation.

Relevant international co-operation practices were also analysed as part of the study. In most countries, this international co-operation is dealt with by LEAs, very often in co-operation with central banks.

The first international legal instrument dealing with counterfeit currency is the *International Convention for the Suppression of Counterfeiting Currency* signed at Geneva on 20 April 1929 (CCC 1929). This convention is a specific, legal, international and binding instrument for fighting against currency counterfeiting. The *UN Convention against Transnational Organized Crime* which was adopted by General Assembly on 15 November 2000 is one of the main international legally binding instruments in the fight against cross-border OC.

INTERPOL provides technical and forensic support, and operational assistance to support member countries in addressing the problem of counterfeit currency. Of particular interest is the S-Print Project[4], an international monitoring system on the security printing industry and suppliers, including the verification of second-hand *intaglio* machines, security printing equipment and suspicious purchase orders.

With regard to international co-operation, various impediments have been identified such as late or no responses to requests, or complicated and time-consuming procedures. The survey indicates that there is room for enhanced international co-operation.

The European Union's legal framework on the protection of the euro against counterfeiting can be seen as a "best practice" example with regard to co-operation at the regional level. EUROPOL acts as the *European Central Office* for combating euro counterfeiting within the meaning of Article 12 of the CCC 1929. Even before the euro was physically introduced as physical currency in (initially) 12 European Union (EU) member states in 2002, provisions had been made to protect it gainst counterfeiting. Those provisions have since been further developed and are complemented by a number of institutions responsible for the exchange of strategic, technical and operational information to support efficient cross-border co-operation. The European Commission's funding programme Pericles[5], managed by its Anti-Fraud Office OLAF, has been established to take into account the international and multidisciplinary aspects of combating counterfeiting of the euro.

---

3 Reference is made to a study completed in 2013 commissioned by Europol and the Dutch National Bank that made for the first time an attempt to scientifically research the profile of a person that distributes counterfeit banknotes.

4 www.interpol.int/Crime-areas/Financial-crime/Counterfeit-currency-and-security-documents/Project-S-Print

5 http://ec.europa.eu/anti_fraud/euro-protection/training/index_en.htm

I. INTRODUCTION

The menace of counterfeit currency is a global phenomenon. Related criminal activity has the capability to generate high profits and is often linked to other types of criminal activities such as trafficking in drugs and racketeering. Currency counterfeiters continue to improvise and take advantage of new technologies to keep pace with regular periodical changes in currency design and security features.

The 2003 FATF Recommendations on ML and TF designated "counterfeiting currency" as one of the 20 predicate offences for ML. Although today counterfeiting currency is among the designated categories of offences as per FATF standards, the FATF has not yet considered it directly in a typology study in order to determine its nature, the scale of the problem, and the methods of laundering these proceeds. It is also unclear how, if at all, the techniques of placing counterfeit currency into the legal financial system differ from those used to launder non-counterfeit illicit cash proceeds. Furthermore, it is little understood how the counterfeiting of currency generates illicit (non-counterfeit) proceeds that must then be laundered.

1. SCOPE OF THE STUDY

Currency counterfeiting has various manifestations:

- Individuals producing counterfeit currency to be used for personal use.
- Criminal groups producing counterfeit currency as a profit-making activity in order to sell or resell it for illegal gain.
- The use of CCN for financing terrorist activities.
- States and/or terrorist groups using counterfeit currency as a means of economic warfare.

This project provides a short overview of these different manifestations but focuses on the second and third one, since it is these activities that are the determining factors related to ML and TF.

The study reflects the situation on counterfeit banknotes only.

2. AIMS OF THE STUDY

The goals of the FATF typologies research on counterfeiting of currency are:

- To identify and describe ML and TF methods associated with counterfeit currency;
- To compare the methods of placement of counterfeit currency with those of other criminal proceeds;
- To study the links of counterfeiting of currency to organised crime, TF and other criminal activity;

- To identify AML/CFT measures that are potentially useful in detection of counterfeiting of currency and associated to ML and/or TF;
- To identify red flag indicators for detection of suspicious transactions relating to counterfeit currency;
- To identify gaps in the legal framework and/or mismatches in the operational interaction of LEAs, customs and FIUs preventing successful investigation and prosecution of ML/TF arising from counterfeit currency.

3. METHODOLOGY

This study is based on two main types of sources of information. Primary information was gathered by means of: (1) survey questionnaires sent to FATF members and FATF-Style Regional Bodies (FSRBs); (2) several workshops run by the project team;, and (3) opinions, experience and knowledge of experts related to subject matters such as currency counterfeiting, ML and TF. This primary information assisted the research team in establishing the general parameters of its work and in focusing its requests for further information. The views of experts were particularly helpful to uncover shortcomings in a highly specific field of this activity.

Secondary information was systematically developed, mainly from academic articles, and used to complement the survey responses received.

Due to the limited number of survey responses received (25 in total), the report does not present a complete picture for all countries of the world. Nevertheless the information collection process and the literature review suggest that while OC and TF related to counterfeiting of currency have, to a certain degree, attracted the attention of scholars, the ML aspect of counterfeiting of currency has not been a serious subject of research up to now. Information related to currency counterfeiting has often been treated under the more general offence of fraud or incorporated into articles related to other forms of criminal activity.

4. SCALE OF THE PROBLEM

Currency counterfeiting crimes can have a high impact on the political and economic system of one country as they are able to challenge the foundation of sovereignty. The involvement of OC and terrorist groups can pose a serious threat to national economies and global security.

Estimates for the proceeds generated by currency counterfeiting are rare, and the survey does not provide comprehensive figures. According to statistical data provided by LEAs and regional institutions of the Bank of Russia, the number of counterfeit notes detected in recent years has decreased[6]. Haken suggests that the amount of counterfeit US dollars and euros is not large in the general context of all currency in circulation and cites a US Secret Service (USSS) 2005 estimate of one counterfeit USD for every USD 12 400 out of USD 760 billion in circulation[7]. European Central Bank (ECB) statistics from 2010 indicate that more than 97% of counterfeit banknotes withdrawn

6 Krylov, O.V. (2012).

7 Haken, J (2011), *p.* 18.

from circulation in the second half of that year were in countries of the "Euro area"[8]. Seizures of counterfeit euro notes in EU countries outside the Euro area amounted to 1.5% with a similar seizure amount for countries outside the EU[9]. These figures need to be seen from the perspective that countries outside the EU are not obliged to report euro counterfeiting seizures to the ECB. The statistics[10] also do not include counterfeit banknotes that were seized before they were put into circulation, *e.g.,* counterfeits seized in dismantled print-shops. On the other hand, in India there has been an increase in the recovery and seizures of counterfeit Indian currency by about 210% in 2011 as compared to 2009.

Another factor that makes estimates of proceeds of crime difficult is "dark figures". The 2006 final report to the US Congress by the Secretary of the Treasury refers to the unlikelihood of large amounts of counterfeit US dollars circulating for a very long time before being detected, due to the way that US currency is used and moved. Collected data, input from currency dealers, information on currency flows and analysis of economic data, appear to indicate that US banknotes "are exchanged sufficiently often that they regularly move through financial institutions and exchange houses"[11]. Counterfeit banknotes are thus more likely to be detected.

INTERPOL publishes yearly statistics for all counterfeit currency seizures that take place in 190 countries. Data from 100 Interpol members (see Annex 2) reveal that 3.27 million pieces of CCN representing115 different currencies were detected in 2011:

- 98 countries out of the 100 countries reported that they detected/seized counterfeit national currency.
- On average, each country reported detection/seizure of 4.35 different types of currencies other than the national currency.
- Switzerland, followed by the United Kingdom; Hong Kong, China; and the Netherlands, were the top four countries in terms of different types of counterfeit currencies detected/seized in their jurisdiction.
- The US dollar, euro, pound sterling and Yuan renminbi were the top four currencies reported as counterfeited by other countries (see Chart 1);

---

8 The "Euro area" includes those the EU members whose currency is the euro and in which a single monetary policy is conducted under the responsibility of the Governing Council of the ECB. In 2013, it comprised Belgium, Germany, Greece, Spain, Estonia, Ireland, France, Italy, Cyprus, Luxembourg, Malta, the Netherlands, Austria, Portugal, Slovenia, Slovakia and Finland.

Source: www.ecb.int/home/glossary/html/glosse.en.html, retrieved 7 May 2013.

9 Europol (2011a), *p.* 34.

10 ECB (2013).

11 US Treasury Department (2006), p.X.

Chart 1. **Top 10 currencies reported as counterfeit by different countries**

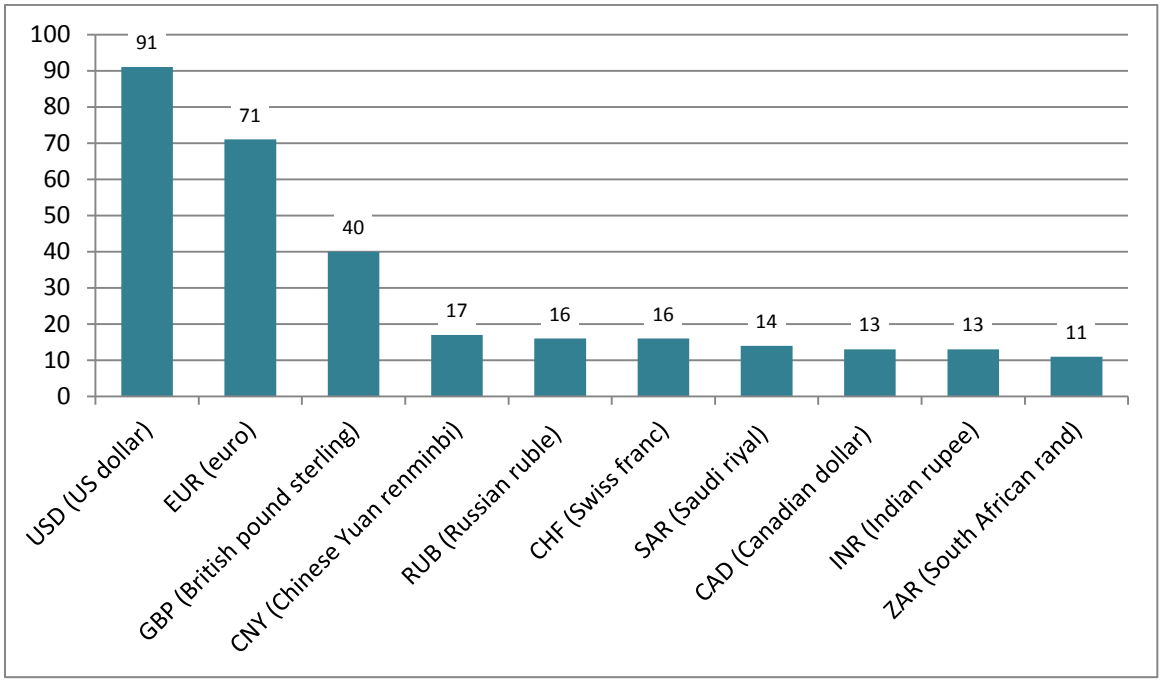
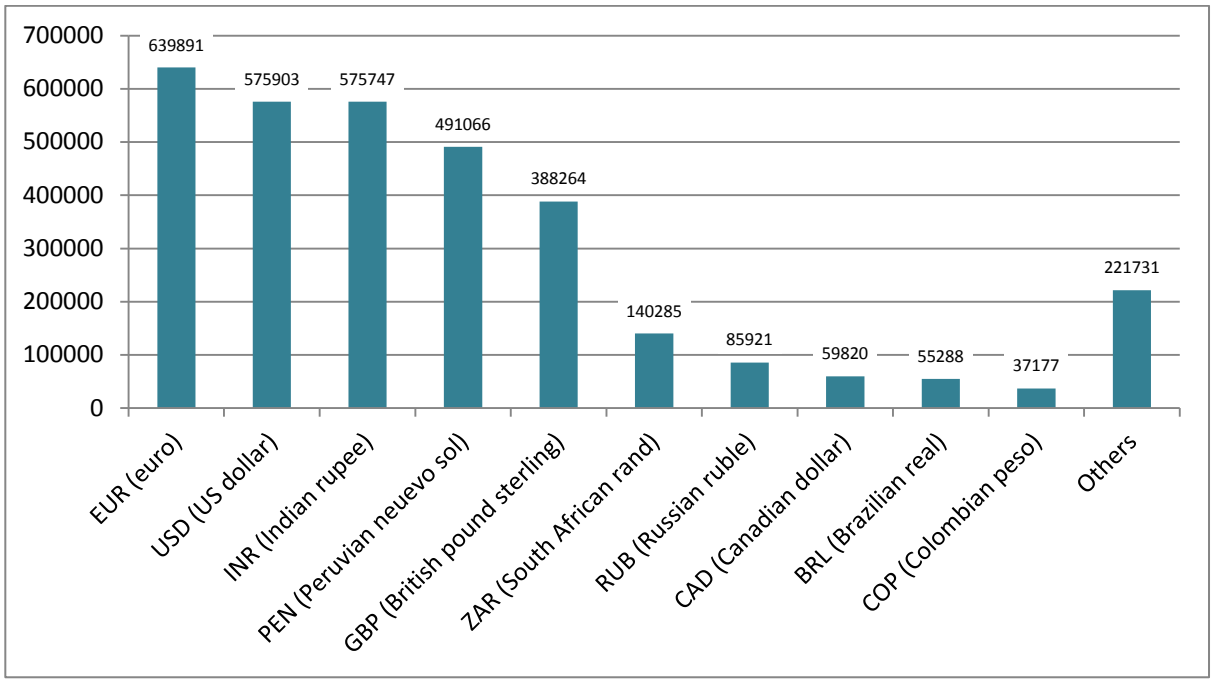
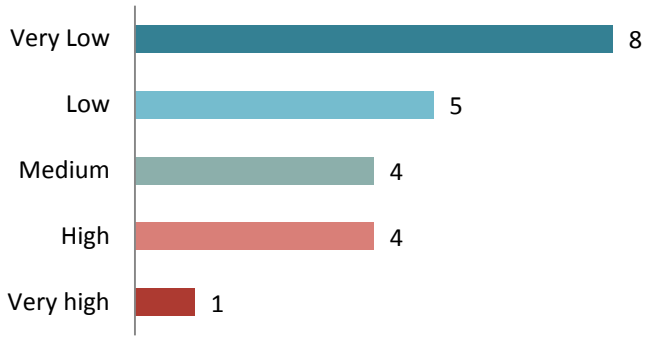


Chart 2. **Top 10 currencies in terms of number of notes reported as counterfeit by different countries**



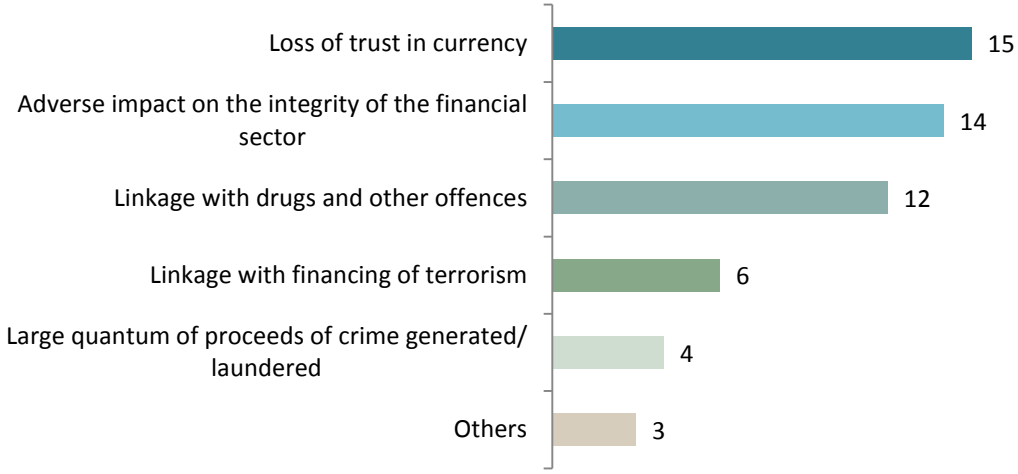
The threat from counterfeiting of currency was assessed by the responding countries on a range from “very high” to “very low”. Thirteen countries evaluated the threat from currency counterfeiting as "low" to "very low". Five countries responded the threat as "high" to "very high" while four countries claimed the threat is "medium".

Chart 3. **Threat rating for counterfeiting of currency**
Option selected by number of countries



When asked to identify the factors underlying the threat from currency counterfeiting, respondents referred to the "loss of trust in the currency system" followed by the "adverse impact on the integrity of the financial sector" rather than the "financial loss" one faces by "accepting" a counterfeit or the actual financial damage which is in fact compared to other forms of criminal activity quite small (for more information see Chart 4).

Chart 4. **Factors underlying the threat assessment of counterfeiting of currency**



The technology revolution in the cyberspace-age makes equipment necessary for the production of counterfeit money cheap, easy to purchase and to operate. "The advent of desktop publishing, colour printers, and photocopiers means that currency counterfeiting is no longer the exclusive domain of lithograph experts with expensive offset printers. As such, a greater number of amateurs can produce larger numbers of bogus bills"[12]. Essentially, everyone with basic computer skills, access to a PC, a scanner and a printer has the potential to become a counterfeiter. However, the success of introducing counterfeit notes into legal circulation very much depends on the quality of the product. Public awareness sessions by the private banking sector in co-operation with LEAs and

12 Schneider, S. (2002), *p.* 21.

central banks increased the public's attention and contributed to a reduction in counterfeit products.

Regarding the preferred currency for counterfeiting, the above mentioned report from the US Treasury Department concludes, "as much as 60 percent of genuine [US] currency is likely held abroad" [13]. Nevertheless, since the introduction of the physical euro as official means of payment in 2002, this new currency has rapidly become the second-most-traded currency in the world and in certain cases may even eventually displace the US dollar.[14] Furthermore, the Euro area is expected to continue to grow in the future. The 2011 Europol Organised Crime Threat Assessment (OCTA) suggests that OCGs both inside and outside Europe will continue to target the euro for its counterfeiting activities[15]. With the internationalisation and broad acceptance of the euro, citizens of the Euro area have come to realise that they can exchange the euro as easily as they did before with the US dollar and might even find it more convenient[16]. The Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) suggests that when the full convertibility to one of the major global currencies is guaranteed, this factor contributes to the motivation of OCGs to produce counterfeits in those currencies[17].

13 US Treasury Department (2006), *p.*42.

14 US Treasury Department (2006).

15 Europol (2011a), *p.* 34.

16 US Treasury Department (2006).

17 GIABA (2010), *p.* 69.

II. THE COUNTERFEITING OF CURRENCY AND ITS RELATION TO OC, ML, AND TF

1. TECHNIQUES USED IN THE PROCESS OF PRINTING AND CIRCULATION OF CCN

Counterfeiters can be classified into three categories: (1) amateurs; (2) semi-professionals; and (3) professionals. Amateur counterfeiters are people who have no or poor knowledge of graphic arts and who utilise commercially available means. Semi-professional counterfeiters have some knowledge in graphic arts and use commercially available means. Professional counterfeiters are individuals with expert knowledge in printing and who use professional printing equipment to make CCN. Counterfeiters can act alone or as part of a group.

The number of perpetrators who act alone seems to be high, but the damage they cause is marginal since the area of distribution is mostly local. One of the reasons lies in the motives for carrying out such activity. For example, the individual acting alone may be short of money due to unemployment. The counterfeiting activity serves to generate funds that can be used to replace loss of income and thus to purchase needed or luxurious goods. Such individuals are both producer and distributor. They do not have to share their knowledge with others and they do not run the risk of getting compromised by infiltrated informants or undercover agents. On the other hand, they normally do not have access to a large distribution network. Their profits are thus relatively small, although they may still run the risk to attract attention from law enforcement.

Intensive currency counterfeiting activity is mostly carried out by OCGs. These OCGs range from small, domestic groups to substantial, international groups of criminals involved in the printing and/or the circulation of CCN as a profit-making activity.

The two main techniques of production of CCN used by counterfeiters are (1) printing by offset and by (2) digital graphic chain. The traditional method of the offset production is similar to the one used for the printing of newspapers, tax labels or stamps. To use an offset press, specific know-how is needed and these machines are not easy to find on the (second-hand) market. On the other hand, the digital graphic chain production simply requires a basic hardware consisting of a computer, a scanner, a laser/inkjet printer or a colour copying machine, an image processing software and some commercial paper. The offset and the digital graphic chain techniques relate to the visual of the counterfeit banknotes. Others diversified techniques are complementary used to counterfeit the security features of the banknotes.

In the chain of CCN (from the printing to circulation), there are several different operators especially when it comes to the involvement of OCGs:

- the printer(s),
- the distributors,
- the retailers, and
- the "mules" who are the last ones in the distribution chain causing the actual financial damage.

Each of them has a specific role to play. It is difficult to estimate the proceeds of crime generated by each of them, because there is a shortage of comprehensive information available on the complete working of various layers of the OCG. Currency counterfeiting occurs more often at times when new currencies are issued, taking advantage of the usually poor knowledge amongst the public about the look and feel of new banknotes. The crime of counterfeiting of currency has become international in character. The perception that working in groups decreases the risk and increases global reach motivates these OCGs which are driven by profit, to work very efficiently. The diversity in background or ethnicity of the individual group members does not seem to affect the group's efficiency.

2. COUNTERFEIT CURRENCY AND OC

A. THE INTERNATIONAL/GLOBAL DIMENSION OF OC CURRENCY COUNTERFEITING

The connection between currency counterfeiting and transnational organised criminal groups is also reflected by the fact that the majority of high-quality counterfeit US dollars appear to be produced by counterfeiters with origins in Colombia, Peru, Israel, the Russian Caucasus region and the western Africa region: the regions known to have the presence of such organised criminal groups. Similarly, the euro is also counterfeited outside Europe.

The majority of survey responses indicate that there are no domestic OCGs involved in printing and/or circulation of counterfeit currency as a profit-making activity. The main problem is caused by international OCGs operating in their respective national/territorial jurisdiction. Members of an OCG that is running an illegal print-shop usually avoid distributing their “products” in the same country where the print-shop is located. OCGs that operate in countries with a currency as legal tender that is only accepted in that jurisdiction often turn to the production of foreign currencies with an international distribution dimension such as the US dollar or the euro to dissimulate that they are distributing CCN within the target country and for the purpose of widening the scope of distribution to other countries in order to gain more profits. In the survey eight countries replied that there is counterfeit foreign currency in circulation in their jurisdiction while five stated that counterfeit national currency is printed abroad. This is supported by INTERPOL statistics and case studies such as the one reported by Hong Kong, China, about a seizure in February 2012 of counterfeit Indian Rupees found concealed in a shipping consignment from Pakistan via Hong Kong, China, to Nepal[18].

Europol's OCTA states that within Europe, Italy and Bulgaria "are among the foremost countries for counterfeit currency production sites"[19]. With regard to the counterfeiting of USD "Bulgaria was a country of concern because of the growth of organised crime in south-eastern Europe"[20]. This picture began to change in 2002 when the euro was introduced. Since then "both production and trafficking of counterfeit U.S. banknotes have declined sharply"[21]. Indeed the introduction of the

18 Retrieved from the response of Hong Kong to the questionnaire.

19 Europol, 2011a, *p*. 34.

20 US Treasury Department, 2006, *p.* 60.

21 US Treasury Department, 2006, *p*. 60.

Euro was consecutively followed by numerous print-shops dismantled in Bulgaria. A 2012 report of the European Commission claims that "structures of organised crime were disrupted, with a positive impact curbing prostitution, human trafficking and counterfeiting"[22]. "Bulgarian producers cooperate mainly with Bulgarian, Lithuanian, Turkish, Romanian and Albanian criminal groups to circulate banknotes"[23].

Belgium reported in their responses to the questionnaire that Italian nationals and those of West African origin living in certain Belgian cities are exclusively distributing counterfeits coming from Italy[24].

The war in the area of former Yugoslavia with economic blockades, the presence of weak states in the post-war context, the sometimes legal vacuum, and the coexistence of several OCGs, provided a favourable environment for OC. These preconditions mixed with the geographical location (being the link between Asia and the Mediterranean Sea for the trafficking of illicit commodities to and from the EU), allowed the Western Balkans to become a hub for international OC inter alia involved in currency counterfeiting crimes. Illegal euro print-shops dismantled in Bosnia and Herzegovina and Serbia with existing networks to and in EU member states reflect their specialisation and sophistication in this activity.

Chechen militants have been identified as the primary distributors of counterfeit US dollars and Russian ruble in Russia. Russian OCGs are reported to have consolidated their presence among Albanian, Chinese and Nigerian OCGs in northern and central Italy. By means of laundering the criminal proceeds Russian OCGs have acquired property in tourism and leisure industries and spread their activities in other serious crimes such as , trafficking of arms or synthetic narcotics and trafficking in human beings. [25]

Counterfeit currency and the profit derived therefrom have been used to finance extremist and terrorist activities in North Caucasus[26]. Russian ruble, US dollar and euro are also imported by the OCGs into Russia from Georgia, Kazakhstan, Israel, Eastern Europe and some countries of the EU[27]. The Russian LEAs are reported to have actively suppressed the activity of OCGs associated with the production and distribution of counterfeit money.

Turkish/Kurdish OCGs, apart from being involved in currency counterfeiting, are also involved in drug and human trafficking, production of illegal documents, smuggling, blackmail and extortion; and also in ML by investing the proceeds of the crime in legal businesses[28].

Similarly, Chinese OCGs, commonly known as "Black Society Groups" are involved in migrant smuggling, drug trafficking, smuggling, including arms smuggling, apart from counterfeiting of

22 European Commission (2012b), *p*. 31.

23 Europol (2011a), *p*. 35.

24 Retrieved from one of the two Belgium responses to the questionnaire.

25 Berry, L. *et al.* (2003), *p.*73.

26 Krylov, O.V. (2012).

27 Krylov, O.V. (2012).

28 Shanty, F. (2008), *p.* 467.

currency[29]. Europol's OCTA also suggests that for the production of counterfeit euro Eastern Asia "plays an increasing role in the supply of raw material and equipment"[30].

In India, the problem of counterfeit currency has domestic as well as international dimensions. The high-quality counterfeit Indian currency notes, however, invariably have strong international linkages. The involvement of OCGs based in the neighbouring countries is clearly seen by the Indian LEAs. Evidence with Indian LEAs indicate that high-quality counterfeit Indian notes are printed in Pakistan and then smuggled into India through transit points at Dhaka, Bangladesh, Sri Lanka, UAE and Bangkok. The other route to smuggle and pump the counterfeit Indian rupees is by smuggling through the India-Pakistan border and India-Nepal borders.

OC and OC networks of transnational character have also seriously affected Western-African countries by criminal activities such as drugs and human trafficking, smuggling, ML, terrorism and currency counterfeiting with the scale of their activities posing a serious threat to institutional development in this area. GIABA claims that "[c]ounterfeiting in the region has the capacity to generate very large quantities of illicit funds, and in its most extreme forms, to de-stabilise and weaken local currency"[31]. Between June 2008 and June 2009 the total value of counterfeit notes seized in Nigeria was 1.3 billion principally in US dollars, but also in other currencies such as the euro, Pound sterling, Canadian dollar and Nigerian naira[32].

In Canada, the OCGs "have adapted their structure to facilitate the production and distribution of counterfeit currency"[33]. According to the RCMP[34], these groups operate both domestically and internationally. The major cities, where they are generally based, provide them with anonymity and the market for their product. They are also involved in forged payment cards, weapons, drugs, stolen vehicles and forged identity documents.

In the US counterfeit currency is one of the crimes in which a number of OCGs are involved. Some of these OCGs are also involved in other illegal activities such as gambling, extortion, robbery, drug trafficking, trafficking in human beings and ML. During the Financial Year 2011 the USSS "recovered USD 154.7 million in passed and seized counterfeit currency, arresting 2 471 individuals domestically and 386 suspects in foreign countries for counterfeiting offenses"[35].

Europol's OCTA suggests that "the euro continues to be a target for organised crime groups active in the forgery of money, not only in Europe but also in other regions of the world such as South America"[36]. Colombia "has historically been one of the largest producers of counterfeit [US] currency"[37] and "has been the chief supplier of counterfeit notes to the [US] market"[38]. In Financial

29 Zhang, X. (2001), *p.* 69.

30 Europol (2011a), *p.* 34.

31 GIABA (2010), *p.* 68.

32 GIABA (2010), *pp.* 68-69.

33 RCMP (2007), *p.* 14.

34 RCMP (2007).

35 USSS (2011), *p.* 4.

36 Europol (2011a), *p.*34.

37 USSS (2011), *p.* 35.

Year 2011 "more than $ [USD]4.1 million Colombian-originated counterfeit was passed within the United States. This accounts for five percent of the total dollar amount of counterfeit passed domestically"[39].

Apart from the global market, the so called "temporary criminal markets" are of special interest. They work on the fact that counterfeit currency distributors often circulate their products in tourist areas and during special events (*e.g.,* in major sports events like the Olympic Games or World Championships). Experience has shown that the distribution of certain kinds of counterfeits is linked to an event where the suspected country of production is represented by a sport team. Distributors of counterfeits find favourable conditions, such as unfamiliarity with the design and security features of foreign banknotes, fast handling of cash transaction because of long queues of spectators, etc.

In the process of the enlargement of the Euro area it has also been seen in some instances that OCGs took the opportunity to produce and introduce counterfeit euro banknotes in the transition period when the level of confusion is high.

B. STRUCTURE WITHIN OCGS INVOLVED IN CURRENCY COUNTERFEITING

Generally, the OCGs that are involved in currency counterfeiting "are characterised by their rigid organisation, with a strict distribution of tasks to cells operating independently in order to minimise risk"[40] to the persons at the upper echelons of the criminal organisation and the production source. Evidence suggests that these OCGs strictly separate the production from the distribution site. The hierarchy within the organisation is commonly referred to as a "pyramid-like structure".

The pyramid-like construction makes it inherently difficult for LEAs to tackle the criminal organisation and to locate the illegal production facilities. The ones most likely to be caught by the police are those that actually cause the damage by distributing counterfeit currency to ordinary and unsuspecting citizens. Low-level distributors are recruited in a random way, most of them young people looking for quick profits (especially when compared to their national salary). In addition, this field of criminal activity usually has only low priority for LEAs compared to higher priority activity such as trafficking in human beings, drugs trafficking or cybercrime.

It seems that only very few OCGs exclusively deal with currency counterfeiting. These groups attempt to work independently; however, they must exist alongside and compete with other well-established OCGs. These independent OCGs try to establish their own criminal networks, which are usually operated by low profile and inexperienced criminals. The structure of these groups is normally not characterised by rigorous internal rules which make the whole network porous, weak and susceptible to infiltration. The weakness of these OCGs reflects their overall resources and skills not only in negotiating and distribution of CCN but also in producing them. The CCNs of such groups are often of poor quality, and their members are constantly running out of money and thus become easily susceptible to disloyalty.

38 US Treasury Department (2006), *p.* 60.

39 USSS (2011), *p.* 35.

40 Europol (2011a), *p.*34

Typically, the evolution of a criminal group into a criminal network, where independent groups are brought together by so-called facilitators, results when the criminal co-operation is based on mutual benefits to all of the groups involved. OCGs use their illegal print shops not only for the purpose of counterfeiting money but also for gaining other profits, *e.g.,* forging tax stamps or tax labels, forging payment cards, or by facilitating their criminal activities with the production of forged documents. The operations of OCGs also cross ethnic dividing lines. They co-operate without regard to nationality; their main incentive is profit.

The real threat comes from criminal groups sponsored or financed by well-established OCGs. Though there is very little information regarding the top level of these organisations, it can be stated that it involves powerful criminals who are in control of large "mafia-style" organisations for whom counterfeiting is only one of the activities which contributes to the overall profit. "In Italy, the production and transnational distribution of counterfeit money is often tolerated, and in some cases orchestrated, by mafia-type organisations such as the Camorra in the Neapolitan region"[41].

Frequently OCGs involved in currency counterfeiting activity are a branch of criminal activity or part of bigger criminal networks engaging in all kinds of illicit activities. Those groups and all branches within can rely on long-existing, reliable and well working facilitating networks. It is also seen that groups overlap; for example, drugs traffickers use currency counterfeiting channels and vice versa. A significant characteristic of these groups is their ability to adapt: if one branch is disrupted, another branch takes over the activity within a very short period of time. The fact that most of the criminals arrested have criminal records for a wide variety of criminal activities supports the theory that counterfeiting activities are only part of the entire criminal business of these organisations.

As for the links of currency counterfeiting to other forms of criminal activity, the majority of survey responses from FATF members refer to illicit trafficking in narcotic drugs and psychotropic substances (11), followed by participation in an OCG and racketeering (9), smuggling (4), trafficking in human beings and migrant smuggling (4), small-scale and street-level deception cases committed by individual criminals (1), and illicit arms trafficking (1). The fact that currency counterfeiting activity comes almost always along with other criminal activity is also strongly supported by the various case studies received.

Box 1. **Seizure of counterfeit currency with arms and drugs**

The Border Guarding Force along with the Police intercepted five individuals on the border, from whom following were seized, 11 kilograms of heroin, one Beretta pistol along with eight live cartridges, and high-quality counterfeit Indian currency notes having face value of INR 500 000. Investigation has revealed that these persons are smugglers with international connections and had received these contraband goods from their accomplice from across India's western border. The accused have been charged under various provisions of Narcotics Drugs and Psychotropic Substances Act, Arms Act and Indian Penal Code.

Source: India and presented in the FATF/GIABA joint experts' meeting on ML and TF Typologies, Dakar, Senegal, 26-28 November 2012

41 Europol (2011a°), *p*. 35

Box 2. **Seizure of Counterfeit printing facility with counterfeit US dollars and drugs**

On 17 February 2012, the Dominican Republic National Drug Control Agency (NDCA) contacted the Secret Service San Juan Resident Office requesting assistance regarding a counterfeit US currency investigation. The investigation was initiated based on information provided by a reliable confidential informant.

The NDCA gathered additional intelligence through surveillance operations and other investigative techniques identifying that a residence in Mata San Juan, Dominican Republic, possibly contained 500 kilos of cocaine. The NDCA executed a search warrant revealing two suspects and an offset printing press. A search disclosed negatives containing images of USD 100 currency, paper similar to genuine money, jars of ink and USD 2.6 million in counterfeit currency. San Juan agents conducted a check of the Secret Service Counterfeit Tracking Application identifying the notes as being of record under Circular - 24806. Based on the passing history of this circular, agents believe that C-24806 is manufactured in the Dominican Republic. On 17 February 2012, two suspects were arrested under Dominican Republic law for fraud and distribution of counterfeit currency. This case is continued pending further investigation and judicial action

Source: USSS (2012).

C. TECHNOLOGY, SPECIALISATION AND THE USE OF LEGITIMATE BUSINESS STRUCTURES

The activities of some OCGs involved in printing, circulating, smuggling and distributing of CCN have a high level of sophistication which cannot be attained by ordinary criminals, such as comprehensive and covert distribution channels, transnational operations, high volumes of CCN and the use of logistics of highly sophisticated ML networks.

The production of CCN is not only restricted to illegal laboratories. The owners and employees of legitimate printing firms have also been detected in this illicit activity[42]. Legal print shops have been, and certainly continue to be, used to counterfeit currency. In some cases, the owner was aware of this, while in others, employees were on the payroll of a criminal organisation without the knowledge of the owner.

Box 3. **Euro counterfeiting case**

Spanish authorities, working with Europol, dismantled a criminal group responsible for drug trafficking and distributing more than two million counterfeit euros in 20 EU countries. In total 25 people from the criminal group were arrested. This criminal group had been under investigation by the Spanish National Police since 2010, for drug trafficking and euro counterfeiting. In June 2011, Spanish authorities dismantled the first part of the criminal network when they seized 1 018 tonnes of cannabis and arrested 11 suspects. The investigations nevertheless continued, and focused on euro counterfeiting. Europol played an important role in

42 Europol (2011a), *p.*34

the operation, as the European central office for the protection of the euro, by coordinating investigations among the countries affected by the activities of the counterfeiters. The main counterfeiter was the owner of a canned food distribution company, where the clandestine print shop was found. He used the company as a cover for the illicit print shop, where 50 EUR notes were printed. The criminal group also imported fake 20, 50 and 100 EUR notes from criminal counterparts in Italy for further distribution around Europe.

In this part of the operation, 9 search warrants were carried out in different Spanish cities, 14 suspects were arrested and EUR 1.5 million in counterfeit banknotes were seized, as well as materials for the mass production of more counterfeit euro notes. Machinery and tools to counterfeit Spanish identification documents were also found.

Source: Europol (2011b)

Typically, in a counterfeit currency operation, the printing facility is centralised in one location, often in a country other than the country to which the counterfeited currency belongs for reasons related to risk perception. Although a certain degree of job rotation is seen, it is rather unlikely to have printing operations at numerous locations because of the levels of technological sophistication and investments involved. It normally tends to be a high-volume operation because once the printing facilities and capabilities are in place the marginal cost of printing additional notes is very low as compared to the profits they fetch.

Production on demand avoids the exposure to LEA attention and minimises the risk of losses when depots are raided. Furthermore, the producer of CCN needs specific skills and knowledge in all different stages of the production process. The skills of those people are so sophisticated that OCGs tend to "employ" the same printer again even after serving prison sentences. Computers are increasingly used, either alone or in combination with the traditional printing method of offset for the production of counterfeits, though several preventive measures have been taken to inhibit high-tech reproduction of counterfeit banknotes. However, most of the CCN in circulation throughout the world is of such quality that it is difficult for a non-expert to distinguish the counterfeits from genuine currency.

Incorporation of such sophisticated level of security features, which require not only technologically advanced production processes but also access to restricted material, entails high levels of capital expenditure and investment. Such advanced level of production capability suggests that there may sometimes be close links between OCGs and the state apparatus.

It is no longer necessary to physically hide films and printing plates. A rapid and growing problem is the use of web-based platforms where criminals share their knowledge and deposit files and images for the production of counterfeits. Moreover, web-based companies offer counterfeit currencies of all kind. Furthermore, the jurisdictional ambiguities tend to discourage the authorities from taking up the investigations.

Operations related to ultimate infiltration of counterfeit currency in the regular financial stream must be spread over a large area, not only in the country to which the currency belongs, but also in the countries where there is a high demand for the currency. The trafficking operations from the

stage of printing to the stage of infiltration therefore require a well-organised covert distribution network, which also takes care of cross-border smuggling of CCN.

In a typical operation, several layers of intermediaries might be involved, each one dealing with one or more of the following intermediate processes:

- Procurement of CCN from printing facility.
- Distribution to a stocking facility.
- Stocking of CCN (often located in a neighbouring country and close to the borders/ports/airports for ease of smuggling to the country to which the counterfeit currency belongs).
- Smuggling of CCN to the country in which it is to be circulated.
- Distribution and integration of the CCN into the financial system of the target country.
- Ensuring collection and repatriation of the proceeds generated to all stakeholders in the chain.
- Laundering the proceeds of crime.

3. COUNTERFEIT CURRENCY AND ML

There are many factors affecting the printing, distribution and circulation of CCN across jurisdictions. The first such factor is that of "jurisdictional arbitrage". Many countries do not consider counterfeiting activity involving non-national currency as a significant problem, as such activity does not have a direct impact on them. Ultimately, the foreign financial system suffers the loss, but the “blame” goes to the jurisdiction whose currency is being counterfeited, as well as the country where OCGs are operating. Moreover, the capabilities for detection of counterfeiting foreign currencies may sometimes be lower in foreign jurisdictions simply because the financial institutions and the population in general are not familiar with security features on these currencies. As already explained, the risks associated with operations like printing and stocking of CCN are therefore much less if carried out in other countries, thus making overseas operations attractive. In addition, there is a demand for foreign currencies in cash form in every jurisdiction generated by demand factors such as the payment of wages to illegal foreign migrant workers, payments for procuring goods for smuggling, requirements of international travellers etc.

Large scale trafficking in counterfeit currency is closely and inextricably linked with ML. The increasingly global nature of the counterfeiting activity results in the requirement to move CCN and subsequent proceeds of crime across national borders. This will be illustrated in the cases in this chapter.

While illegal transactions in any product that generates proceeds or profits would entail the need for ML, the linkage of ML with illicit trafficking in counterfeit currency operates at two distinct levels. Firstly, like any other criminal activity, illicit trafficking in counterfeit currency generates proceeds of crime which need to be laundered for their integration into the regular financial stream. Secondly, the very activity involved in illicit trafficking in counterfeit currency is placement of

currency notes, albeit fake, into the same regular financial stream. This can only be done through an effective laundering process, which not only conceals and camouflages the origin of the fake currency, but also the fact that they are counterfeits.

The following sections are based on the survey responses from countries regarding the ML techniques that are used to place counterfeit currency into the regular financial network, to transfer proceeds of crime and ultimately to integrate proceeds of crime into that network.

A. PLACEMENT OF CCN

In the process of distributing CCN, each intermediary stage in the process has its share of profits or remuneration which may be given in the form of a commission or a discount on the face value of the currency. For example, counterfeit currency would be sold from the printing facilities at a discount ranging from 75% to 80%, *i.e.,* counterfeit currency equivalent to USD 100 would be sold to the first stage distributor at USD 20 to USD 25 depending upon the quality of counterfeiting. Thereafter each stage will have its margin of profit/commission depending on the risk perception associated with each stage. For example, the courier smuggling counterfeit notes across a border would demand a higher commission as compared to a courier transporting it within the country. Finally, at the end-user level the counterfeit currency sells at a discount ranging from 25% to 35%, *i.e.,* counterfeit currency equivalent to USD 100 would be sold at the end user stage at USD 65 to USD 75. The actual commission or discount given would vary from case to case, given the various factors and nuances of the activity.

As explained earlier there are only a few people on top level and numerous low level distributors. While in sum all the low level distributors generate huge profits, the profit for a single perpetrator is quite small. Hence, those profits for a single perpetrator might not raise any suspicion at all and do not necessarily need to be laundered. Considering that every stage in the process of distribution has its profits and that the higher you go up in the hierarchy of the organisation the fewer people there are, there is a stage where profits no longer go undetected and illicit profits need to be laundered.

The methods used for the placement of counterfeit currency note are numerous and vary. Chart 5 identifies the most commonly used methods reported by the responding countries:

Chart 5. **Methods used for placement of counterfeit currency**

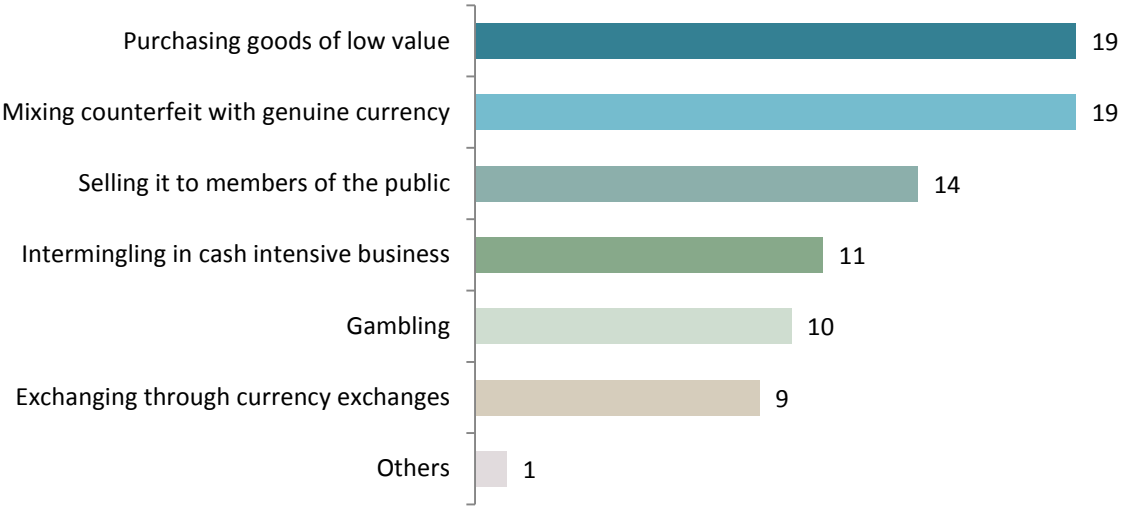
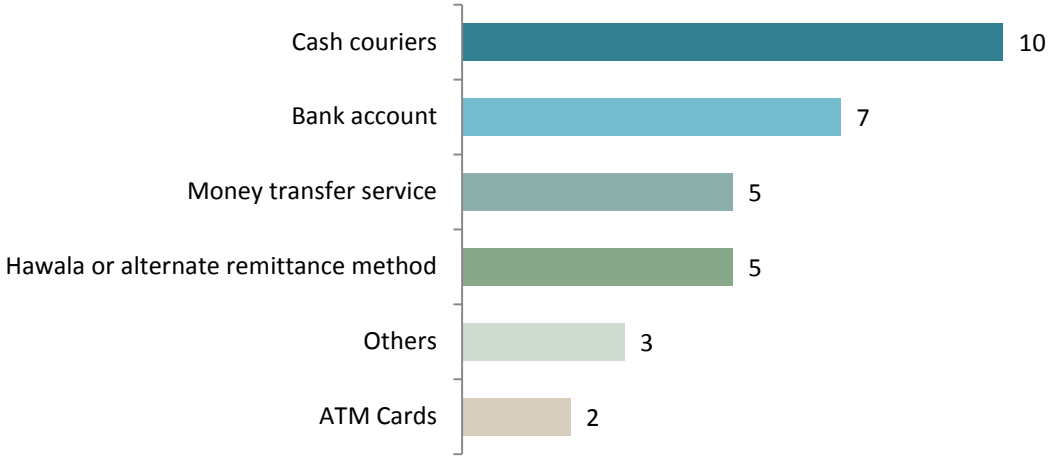


Chart 5 indicates that the most common method used for placement are mixing of counterfeit notes with genuine currency and/or purchasing of goods of low value. The risk of detection in these methods is low and hence preferred by the criminals. Selling it to children considerably lowers the risk in getting caught, while children might not be punished because they are minors.

B. TRANSFER OF PROCEEDS OF CRIME

Chart 6 identifies these methods used for the transfer of proceeds of crime related to counterfeit currency.

Chart 6. **Methods used for transfer of proceeds of crime related to counterfeit currency**



It should be noted that all techniques identified are similar to the ones associated to any other types of criminal activities. The most used method is the system of the cash couriers. The term “cash

couriers" refers to the natural persons who physically transport currency and bearer negotiable instruments on their person or accompanying luggage from one jurisdiction to another[43].

Box 4: **Selling of Counterfeit currency of third country smuggled by a foreigner through use of money exchange**

The police in India have registered a case against two Omani nationals and counterfeit Indian currency notes having face value of INR 25 000 from their possession. It was revealed that the accused had exchanged an amount of INR 40 000 from Asia Express Exchange, Khaboura, Oman on 29 January 2013 and came to India on 30 January 2013. The case is under investigation.

Another case was registered against an Omani national by the police in India for possessing eight counterfeit Indian currency notes of INR 1 000 denomination. As per the statement of the accused, he had exchanged his Oman currency to Indian currency from an exchange centre situated at Oman airport. The accused came to India on 7 February 2013. The case is under investigation.

The police in India have also registered a case on against one Indian National who remitted an amount of counterfeit Indian currency notes for INR 17 000 for treatment of her daughter at a hospital in India. According to the statement of the suspected accused she exchanged UAE Dirhams into Indian currency of INR 20 000 from AI Fala Plaza situated at Lulu Centre, Sharjah and she got 20 notes of INR 1 000 denomination.

According to the statements of the suspected accused in the above three cases, the counterfeit notes possessed by them were received from the currency exchange centre in foreign countries, *i.e.,* two offences from Oman and one offence from Sharjah.

An investigation by the Royal Oman police identified a Pakistani national for involvement in the circulation of counterfeit Indian currency notes in Oman, possession of which led to the detention of the Omani nationals in India. An arrest warrant has been issued in Oman against the Pakistani suspect, who is understood to have left Oman. Omani authorities have obtained confirmation that the Pakistani national was also involved in circulation of counterfeit Indian currency notes in other countries.

Source: India

C. LAYERING AND INTEGRATION

Concerning the methods for layering and integration of proceeds of crime related to counterfeit currency, the following techniques are currently seen:

[43] FATF (2005).

Chart 7. **Methods used for layering and integration of proceeds of crime related to counterfeit currency**

The survey indicates that vulnerabilities of the financial system for the purpose of ML are being misused by adopting different methods. In a given case, there may be more than one method used for placement and integration of illegal proceeds, usually also associated with cash-intensive businesses. The other methods are general in nature. All techniques identified are similar to the ones associated to many other types of criminal activities too. Intermingling in cash intensive business, not surprisingly, leads the chart because it comprises two actions at one time:

(1) introducing the counterfeit currency into the legal financial flow by exchanging it with genuine currency, generating the profit; and

(2) integrating the proceeds of crime.

There are various types of techniques used for ML. It is important to highlight some of them in order to understand the nature of techniques for integration of not only the proceeds of crime relating to counterfeit currency but also the integration of counterfeit notes in the regular financial stream. Some of the techniques used for laundering of money related to currency counterfeiting activity are highlighted in the following chapters.

Use of bank accounts, multiple bank accounts, different type of bank accounts, debit cards, credit cards, etc.

This technique is used to escape detection of the proceeds of crime by the reporting entities, because the deposits may not match with the profile of the account holder: the beneficiary of the proceeds of crime. The criminals, therefore, are known to use multiple bank accounts into which to deposit the proceeds of crime. These multiple bank accounts are also opened and operated by the sellers of counterfeit currency in the name of other gullible individuals. A common typology that has been seen is that the seller of the counterfeit currency asks his buyers to deposit the proceeds of crime in different bank accounts, which are established outside the geographical area in which the seller operates. The seller in turn withdraws the proceeds of crime by use of ATM cards. In this manner, the seller evades the reporting entities by keeping the deposits below the threshold, in each of the multiple bank accounts.

Box 5: **Transfer of proceeds using bank accounts and ATM cards**

On the basis of information received, the Police searched four persons and found counterfeit Indian currency having face value of INR 40 000 (Indian rupees). Subsequent search of the residential premises of one of these four apprehended persons led to the recovery of counterfeit currency having face value of INR 110 000. The verification of the backgrounds of the arrested persons revealed that two of them were dedicated members of a banned terrorist organisation. In fact, one of them was involved in raising and collecting funds for the banned terrorist organisation. The CCN were to be used to finance terrorist activities and for providing to terrorists and their sympathisers. Later, another person who provided the counterfeit currency to these arrested persons and in return accepted the proceeds of the counterfeit currency was also arrested.

The investigations revealed that the counterfeit currency was brought in from a neighbouring country into a border town by one counterfeit currency dealer. One of the accused procured the CCN from this dealer and provided it to activists of terrorist groups. His standard *modus operandi* to collect the proceeds of the counterfeit currency was use of ATM cards of the recipients of the counterfeit currency to withdraw payments in the border town, which was deposited by the recipients of counterfeit currency in bank accounts located at various places. The other *modus operandi* was the use of bank accounts held in the name of other persons (not directly connected with the underlying activity) to receive and withdraw the payments deposited by the recipients of counterfeit currency at different places.

Source: India

Another practice involving the use of bank accounts is the use of accounts maintained by the bank for individuals who are residing in a foreign country. Such accounts are maintained in convertible foreign exchange and can be accessed from anywhere in the world. Hence, the dealer of counterfeit currency, who is located in a foreign country, deposits his proceeds of crime in this account and then transfers it to different (normal) domestic bank accounts. The domestic reporting entities do not suspect any wrongdoing on the part of the account holder based abroad, as they feel that the deposits are coming through banking channels and that the requisite due diligence has been performed by the bank in which the deposits were made initially. The criminals take advantage of the fact that the domestic banks are not aware of the activities of the sellers abroad and the banks abroad are not aware of the various nuances of trade in counterfeit currency of a different country. This is accentuated by the lack of international co-operation amongst LEAs and also lack of exchange of information on risk between financial regulators and banks.

The beneficiary of such bank accounts also resort to use of credit cards, linked to these particular bank accounts, to access these funds. The use of ATM/ debit cards and credit cards are typical of non-face-to-face transactions. It effectively circumvents the effect of CDD measures by the banks.

Smuggling of cash

Smuggling of cash involves physical movement of cash from one country to another in a clandestine manner. This method avoids the banking system, so that the proceeds of crime go undetected by the

reporting entities. One simple *modus operandi*, where the borders between countries are fenced, is to throw the purchase price in genuine currency of the counterfeit currency over the fence and similarly the counterfeit is thrown over the fence from the other side of the border. In such cases, the seller uses the proceeds of crime to convert it in the currency of the native country of the seller, using money changers, including those operating underground. On the other hand, the buyer of the counterfeit sells the same to lower rung of operators who use it or sell it further. These persons get their proceeds of crime, either by collecting the cost of the counterfeit currency directly or by use of bank accounts, as explained above.

The other *modus operandi* used is to smuggle physical cash in genuine currency to a foreign country, in which the criminal syndicate is located, to buy the counterfeit currency. The counterfeit currency is also smuggled either in baggage or on the person into the country where it is to be circulated. The cash so smuggled is then either deposited in the bank in the recipient country or laundered through other techniques in the recipient country.

Box 6: **Smuggling of proceeds in cash**

The customs authorities seized an amount of about INR 7 million at the airport from baggage checked in for a Middle East bound flight. The investigations revealed that this represented the proceeds derived from selling CCN and was meant for the top level players of the syndicate abroad. In another case, the customs authorities, similarly intercepted and examined baggage of a Middle East airline and recovered Indian currency of approximately INR 10 million. The said amount was the proceeds derived from selling CCN and was meant for the top-level players of the syndicate abroad.

Source: India

Box 7: **Conversion of proceeds in foreign exchange and smuggling**

At times, the proceeds of crime derived in genuine currency are converted into foreign currency from underground money changers which is smuggled to the foreign-based criminal syndicates. The foreign currency chosen is one which has very high exchange rate compared to Indian rupee, as this reduces the volume of the currency to be smuggled and facilitates further conversion in the local currency of the country in which the syndicate is based. The use of this *modus operandi* has come to the notice of LEAs. In one case, the LEA seized assorted foreign currency, equivalent to about INR 3 million, from a South East Asia bound passenger at an Indian airport. On another occasion, the LEA seized USD 79 200 (equivalent to about INR 3.4 million) from two passengers at an Indian airport.

Source: India

False Description of Goods

In this method, the cargo containing the CCN is generally falsely declared on the invoices, bill of lading and other shipping documents, including the letter of credit for settling the transaction of the imported consignment that contains the counterfeit currency.

Box 8: **False Description of Goods**

In this case, an importer from a company based in a foreign country attempted to import a container full of waste paper. The importer was under the control of criminal syndicates who concealed a huge quantity of fake Indian currency in the container. The importer was the subject of an intelligence-led operation and an intense search of the cargo led to the discovery of the counterfeit Indian currency. The payment to the foreign syndicate (both for junk cargo as well as for fake Indian currency) was to be paid through banking channels by opening the letter of credit, based on false declaration of the goods contained in the cargo and by over-invoicing the falsely declared goods on the documents.

Source: India

Use of bank for placement and deriving the proceeds of crime

The use of banks to place counterfeit currency in the system, its circulation and replacing the counterfeit currency with genuine currency notes, thereby generating the proceeds of crime, is an extremely rare phenomenon.

Box 9: **Use of bank for placement and deriving the proceeds of crime**

The police intercepted a person with counterfeit Indian currency notes with a face value of about INR 500 000. Interrogation of this person revealed that he used to receive the CCN from two persons, who in turn smuggled the counterfeit currency from a neighbouring country, for delivery to the cashier at a bank. Investigations at the currency chest of the bank revealed the presence of fake Indian currency notes with a face value of about INR 40 million in the currency chest. There was also a shortage of genuine currency of about INR 7 million in the currency chest. It is understood that the counterfeits were used to replace the genuine notes in the currency chest and the counterfeits were circulated through ATMs.

Source: India

Use of Alternate Remittance System

The most common method to remit the proceeds of crime (cost of counterfeit currency) to a foreign country from where the counterfeit currency is to be purchased is by use of an alternate remittance system. The buyer pays the cost of the counterfeit currency to a *hawala* dealer, and the seller receives the same in his country of residence or any other country of choice, in the currency of that country. The CCN is then smuggled or sent to the buyer concealed in cargo. The buyer sells the

counterfeit currency to other criminals and the proceeds of crime generated at each stage are brought into the system by various techniques.

Box 10: **Transfer of proceeds through informal channel**

In one case, the proceeds of crime were transferred from a foreign jurisdiction by a criminal syndicate through informal channels. The proceeds of crime received in cash were put into the bank account of another person, who then transferred it out of his account by cheque, which was used as legitimate money by the criminal syndicate. In an another case, the cash amount which was in fact the proceeds of crime (genuine money) was used to purchase the bank draft to make payment towards a life insurance policy.

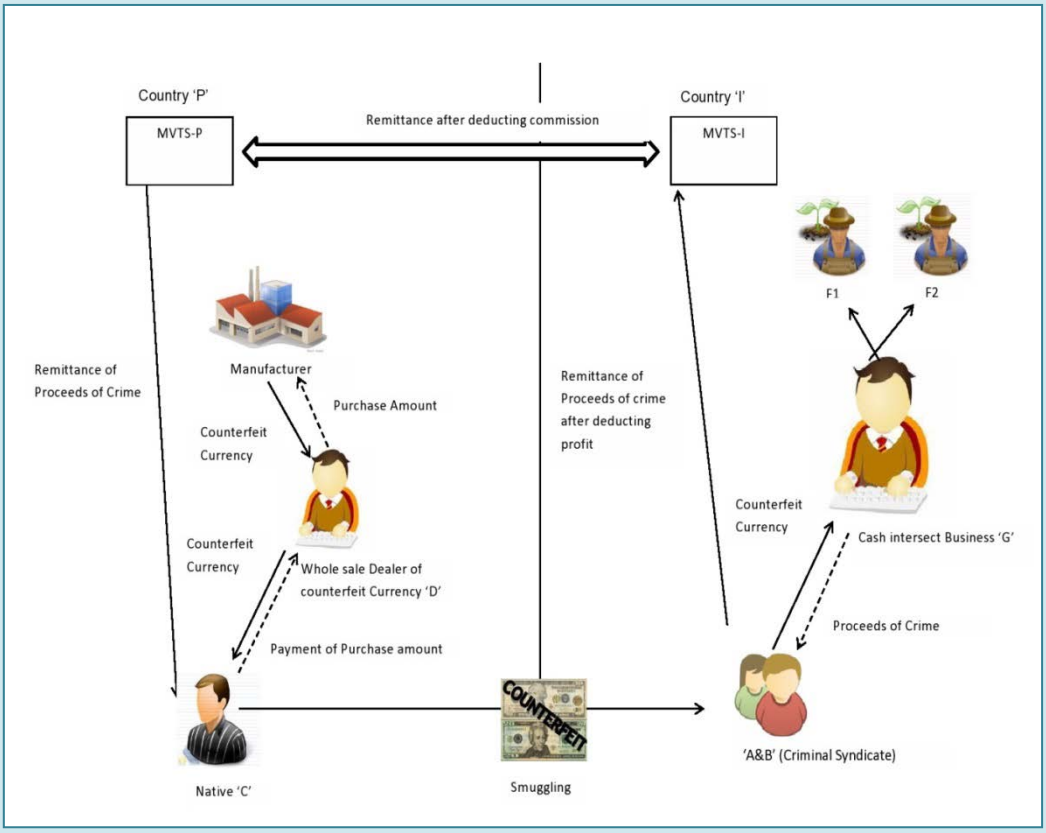
Source: India

Box 11: **Use of MVTs**

Person 'A' was intercepted by the Customs authorities of Country 'I'. Search of the said person resulted in the recovery and seizure of CCN of country 'I' with face value equivalent to USD 4 000. The search at his residence resulted in the recovery and seizure of more CCN of country 'I' with face value equivalent to USD 27 500 as well as the arrest of 'B', an accomplice of 'A'. During interrogation 'A' revealed that he had received the consignment of counterfeit currency equivalent to USD 135 000 from his uncle/associate 'C' a resident of a neighbouring country. The consignment of counterfeit currency was handed over to 'A' and 'B' by a person who had smuggled the currency from the neighbouring country 'P' on the directions of 'C'. Investigation further revealed that the remaining consignment of counterfeit currency equivalent to USD 103 500 had shifted to another safe place. Domestic co-operation between the different LEAs led to further recovery of counterfeit currency of face value equivalent to USD 68 500.The matrix of the case that has been constructed based on the facts revealed during investigations is as follows:

The investigations revealed that 'D' is the main counterfeit currency operator in Country 'P' who deals in the counterfeit currency of Country 'I'. 'C', also a resident of country 'P', procures counterfeit currency valued at USD 135 000 at a discount of 60% *i.e.,* currency worth USD 100 is purchased for USD 40. 'C' contacts criminal syndicate/relative in country 'I' and enters into a contract with them to distribute counterfeit currency in country 'I' for a commission of 10% *i.e.,* USD 10 for every distribution equivalent to USD 100. These natives of country 'I' sell the currency notes at a discount of 30% to cash intensive businesses in Country 'I' like sugar manufacturers ('G') who have to pay the farmers ('F1' &'F2') they procure sugar from in cash. 'G' mixes CCN with genuine currency notes while making payment to the farmers. This is the ML activity taking place in the course of placement of CCN in the regular financial stream. The proceeds of crime or the proceeds of sale of CCN are to be remitted to 'C' in country 'P'. After retaining a commission of 10%, for counterfeit currency equivalent to USD 100 distributed in country 'I' USD 50 has to be remitted back. 'A' gets in touch with *hawala* or 'money or value Transfer service or, 'MVTS-I'. 'MVTS –I along with *hawala* operator 'MVTS-P' in country 'P' runs

an MVTS or a *hawala* operation wherein for a commission of 1.5% they transfer money between countries 'I' and 'P'.



Source: India

Use of high denomination banknotes

The Annual Report 2010 on the "Suspicious Activity Report Regime" of the United Kingdom Serious Organised Crime Agency (SOCA) states that the United Kingdom banned the use of the EUR 500 banknote from retail foreign exchange within the country, based on evidence of significant use by criminals[44]. The report indicates that over 90% of the UK demand for EUR 500 banknotes came from criminals. UK authorities developed evidence of this usage by criminals through analysis of suspicious activity reports (SARs) filed by financial institutions and through information obtained from successful investigations. The SAR analysis indicated that individuals were regularly exchanging in single transactions lower denomination banknotes for the EUR 500 notes. Often these individuals requesting such transactions offered reasons for needing such large volumes of cash. Because of the ban on exchanging small denominations for the EUR 500 notes, the smuggling of funds in cash out of the country has become a bulkier process and thus more susceptible to detection. This experience of the UK reinforces the evidence that the demand in large volumes for

44 SOCA (2010), *p.*35.

high-denomination banknotes, when not justified by clear legitimate economic reasons, can serve as a potential indicator of criminal activity[45].

The fact that EUR 500 and EUR 200 banknotes have been, and are still, counterfeited, attracts particular interest to this phenomenon on the use of high denomination banknotes and would seem to justify further consideration as an indicator for counterfeiting activity.

4. COUNTERFEIT CURRENCY AND FINANCING OF TERRORISM

Most jurisdictions have not reported TF patterns involving CCN. However, Nepal and Kyrgyzstan have instances of currency counterfeiting as a method used for financing of terrorist act and/or terrorists. India, Bangladesh and the United States, have seen a similar development. The United States and India have both reported that individual terrorists use counterfeit currency and distribute it through terrorist networks. The proceeds are invested to strengthen a terrorist support infrastructure and to finance individual attacks.

Box 12: **Use of counterfeit currency in Mumbai terrorist attack by Lashkar- e-Taiba, a proscribed organisation in India**

Person X who was involved in the 26/11 attacks in Mumbai, said that for doing the reconnaissance of Mumbai before 26/11 attacks, an agency of a neighbouring country provided him INR 40 000 (approx. USD 1 000) of high quality Fake Indian currency notes for his expenses by his handlers based in a neighbouring country, which includes the top rung of Lashkar-e-Taiba a terrorist organisation. Person X has been charged, and non-bailable warrants have been issued against him.

Source: India

The United States, India and Tajikistan have reported that counterfeit currency is also used as a method of economic warfare and is used to liaison with OCGs. In addition, India has reported that counterfeit currency is produced in liaison with sovereign states. The role of state actors is apparent, based on forensic examination of the counterfeit currencies seized by the LEAs. Russia, has reported that according to its intelligence agencies, the counterfeit currency manufactured in Dagestan was used to finance extremist groups, purchase arms and in settlements for terrorist activities conducted.

Box 13: **Use of CCN of different countries by terrorists in Russia**

On 15 May 2011, two residents of Dagestan engaged in the distribution of fake Ukrainian hryvnias (UAH) and Russian rubbles (RUB), were detained in Rostov region. Four lots of RUB 1000 banknotes, eleven lots of UAH 200 bills and 12 lots of USD 100 bills were seized. Searches of their premises in Dagestan yielded printing equipment, along with 30 and 100 lots of

45 SOCA (2010), *p.*35.

RUB 1000 and UAH 200 notes respectively. The maker of the fake bills escaped. During a special operation conducted 1 December 2012 in the city of Makhachkala, law enforcement units eliminated a group of militants, including a maker of fake banknotes, and seized Makarov pistols, improvised explosive devices, RUB 734 000 in fake roubles, UAH 580 200 and USD 1 200. Operative intelligence showed that one of the militants killed was linked to the explosion in Kaspisk in 2009.

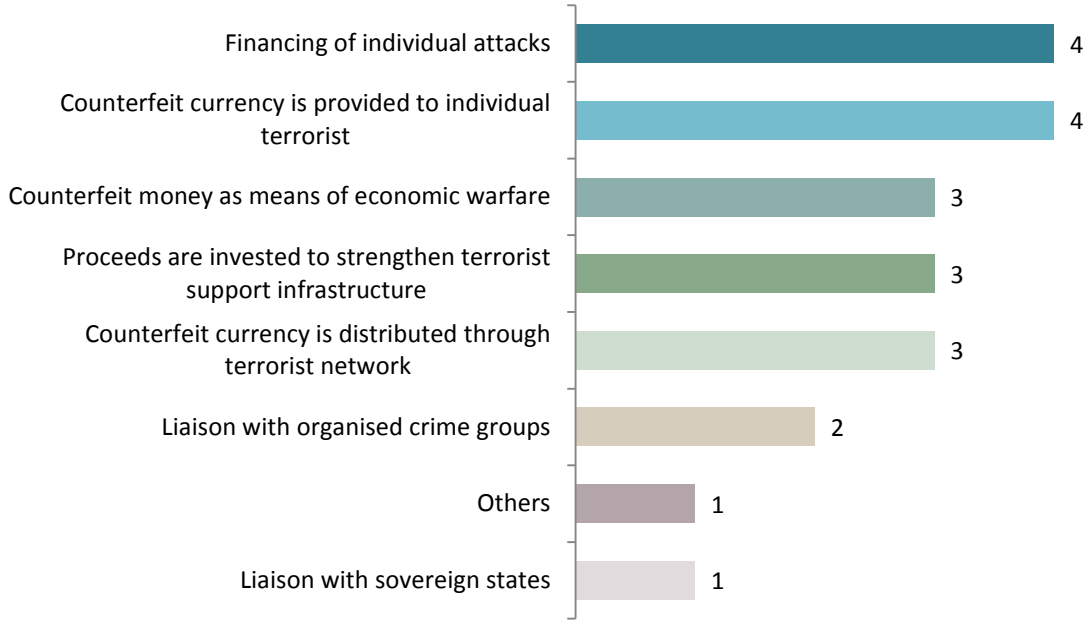
Source: Russia

Before looking more closely at the link between TF and counterfeiting, it makes sense to consider the motives that terrorist groups might have for getting involved in such activity, a realm that is far away from their ideological principles and dominated by medium to large-scale OCGs.

A starting point to explain this – at first glance – strange relationship could be chapter "Crime-Terrorism Toolbox" in Rollins, Wyler, and Rosen's report *International Terrorism and Transnational Crime* from 2010[46]. They split criminal activities associated with terrorist groups in three main categories:

- Fundraising through criminal activities;
- Materials and logistics support; and
- Exploitation of corruption and gaps in the rule of law.

Chart 8. **Methods used for resourcing/financing of terrorism from counterfeit currency**



46 Rollins, J. Wyler, L.S. & Rosen, S. (2010), *p.* 8.

Fundraising by different means is an important factor for terrorist organisations to ensure their continued existence and for the purpose of achieving their goals. Experience of LEAs has clearly shown that terrorists need relatively small amounts of funding for the actual execution of the terror attack. However, the architecture of the entire activity, which includes: recruitment, training, motivation, planning, etc., requires a big amount of funding. They need large sums of funds to recruit, train and maintain their infrastructure. Terrorist organisations are open to accepting funds from any source and therefore, raise funds from a variety of sources ranging from extortion to arms and drug trafficking to counterfeit currency, smuggling, human trafficking, kidnapping for ransom and other criminal activities. They are also known to accept donations from charities and use non-profit organisations, front companies and state sponsorship to meet their funding requirements. It is believed that it was the proceeds from drug trafficking that helped Taliban to support and protect Osama bin Laden and the Al Qaida network[47].

The terrorist organisations have the propensity to be attracted to any 'enterprise' provided that it is lucrative and comparatively unnoticed by the LEAs. The reason for the close association between the terrorists and OCGs is the high profit that organised crime yields and this profit is too attractive for the terrorist organisation to ignore. "Terrorist groups find trading in counterfeit or pirated goods as an easy way to finance their operations with low-entry costs and high-profit margins"[48]. It is widely believed that the IRA was the first terrorist organisation that took to use the profit from counterfeiting of currency as a major source to generate funds. The Hezbollah has also used counterfeiting of currency to generate funds.

Box 14: **Use of Counterfeit currency by terrorists of Hizb-ul-Mujahideen, a proscribed organisation in India**

A network of overground workers were used to collect counterfeit Indian currency notes from Bangladesh and transfer it to Jammu, India (1 500 km away) to be further handed over to the terrorists of the Hizb-ul-Mujahideen. (Proscribed terrorist organisation in India and EU.)

Source: India

While criminal activity as a means of financing terrorism is found in terrorist groups throughout the world, counterfeiting as a mode of terrorist financing appears to occur only in certain regions. There is a wealth of academic literature that suggests terrorist organisations, such as those in Europe, East Asia, and Latin America, rely on common criminal activities, such as extortion, kidnapping, narcotics trafficking, counterfeiting and fraud, to support their operations.[49]

47 Wright, A. (2006), *p.* 87.

48 Bedi, R. (2005), *p.* 3.

49 Wesley, A.J.L. (2007), *p.* 15.

Box 15: **Conspiring to Provide Material Support to Terrorist Organisation Hezbollah**

In a complaint brought before the US District Court for the Eastern District of Pennsylvania, the jury detailed efforts by defendants X, Y, and Z to sell the co-operating witness (CW) counterfeit United States currency for the purpose of raising funds for terrorist organisation A. In total, the conspirators provided the CW with approximately USD 9 800 in counterfeit US currency. From around July 2008 through to around November 2009, in the Eastern District of Pennsylvania and elsewhere, the accused conspired and agreed with others known and unknown to the grand jury to commit offences against the United States, that is, to provide "material support or resources," including false documentation, false identification, currency, monetary instruments and financial securities, to a designated foreign terrorist organisation.

This conspiracy led the accused and others known and unknown to the grand jury to commit the following overt acts, among others, in the Eastern District of Pennsylvania and elsewhere:

Around 18 September 2008, X met with CW and stated that the Country P manufactured high-quality counterfeit US currency for the benefit of terrorist organisation A and that, consequently, representatives of A would need to approve the sale of this type of counterfeit currency.

Around 25 November 2008, Y met with the CW in Philadelphia to discuss the sale of counterfeit United States currency.

Around 24 February 2009, Z caused his assistant ("Individual A") to deliver a sample of counterfeit EUR 200 and USD 100 notes to the CW.

Around 25 April 2009, defendant X met with the CW in Florida and told the CW, among other things, that Hezbollah's representatives worked 18 to 20 hours a day counterfeiting many currencies, including those of the United States, Kuwait, Saudi Arabia and the European Union.

Around 3 September 2009, X confirmed to the CW via telephone that he had mailed a package that the CW received in Philadelphia that same day containing approximately USD 9 200 counterfeit US currency hidden inside a photo album.

Source: Charges brought before the United States District Court for the Eastern District of Pennsylvania, United States of America v. Hassan Hodroj & Others, Date filed: November 24, 2009.

The counterfeiting rackets run by Hezbollah and Hamas are active in different parts of the world and they have apparently co-located with a variety of other OCGs in the tri-border region of Argentina, Brazil and Paraguay[50]. Tamil networks are also believed to be involved in wide range of criminal activities including currency counterfeiting[51]. The Al Qaida's training manual *"Declaration of Jihad against the Country's Tyrants*", seized by the Manchester Metropolitan Police in May 2000 declares currency counterfeiting a requirement "to assist in confrontation and endurance"[52].

50 Lowe (2006), *p*. 256 and Rollins, J., Wyler, L.S., & Rosen. S.. (2010), *p*.8.

51 Biersteker, T.J. & Eckert, S.E. (2008), *p*. 139.

52 US Department of Justice (*n.d.*), UK/BM-12 TRANSLATION.

A. THE TERRORISM – ORGANISED CRIME NEXUS

LEAs around the globe have come across a close nexus between the OCGs and terrorist organisations. One of the characteristics of terrorism is that this relationship between OCGs and the terrorist organisations is growing. The sleeper cells and OCGs conspire in fundraising as well as the organisation of crimes to raise funds for their activities. As the LEAs focus on state sponsored terrorism, the sleeper cells use the lack of focus on them to conduct their nefarious activities.

The terrorist organisations have drawn on the structure and activities of OCGs as models to structure their organisations and to finance their operations, although for different purposes; OCGs focus on profiteering while the terrorist organisations use it to accomplish their 'ideological' goals. Crimes such as drug or arms trafficking, trafficking in human beings, counterfeiting, and credit card fraud, etc. have proved to be profitable to both the OCGs and the terrorist organisations. Apart from sharing their profits with terrorist groups in certain cases, OCGs also assist the terrorist organisations by providing fake identity documents, arms, illicit border crossing for men and material.

"The newly emerging hybrid group of 'organised criminal terrorists' would be the group of individuals to sponsor, support, and actively engage in terrorist activity, and thus to try to promote their own personal interests or strive to acquire more power and wealth from their organised crime-linked activities"[53]. However, Galeotti in his study of OC in light of the financial crises says that connections between OC and terrorists "have tended to be essentially short-lived and low level"[54].

There are specific instances, *e.g,.* in India, which show the close nexus between terrorist financing and the use of hawala for routing the funds to terrorists. The *hawala* networks, in many a case, are controlled by OCGs or have close operational linkages with them. The close nexus between the OCGs and terrorist organisations is best exemplified by the use of counterfeit Indian currency notes by terrorists to fund their activities, which is printed, distributed and circulated by the OCGs.

The report of the Asia/Pacific Group on ML on "Timor-Leste" summarises AML and counter TF measures in place. Its "Key Findings" say that the country "is vulnerable as a target for organised crime smuggling and potentially terrorist activities, particularly given that the economy is 'dollarised' and cash-based, providing an attractive environment for the placement and layering of funds. The risk are intensified given controls at the land border with Indonesia are weak as are the maritime border controls in respect to the cross border movement of currency, goods and/or persons. In this environment, assessments suggest that the majority of proceeds of crime could stem from corruption, tax avoidance, smuggling, human trafficking, counterfeiting of currency, illegal gambling and prostitution".[55]

It is not necessary that the link between counterfeiting and terrorism should always be direct. Such nexus between the two is also indirect where the terrorist sympathizers involved in counterfeiting

53 Bovenkerk, F. & Chakra, B.A. (2007), *p.* 39.

54 Galeotti, M. (2009), *p.* 6.

55 Asia/Pacific Group on Money Laundering (2012), *p.* 2.

transfer part of the proceeds of counterfeiting to the terrorists or terrorist organisations through third parties, by way of donations (Zakat).

B. ECONOMIC WARFARE

Currency counterfeiting and ML have the potential to destabilise national economies and threaten global security as they are key ways in which terrorists and other criminals finance their activities and conceal their profits[56]. However, the character of counterfeiting has undergone transformation over time. It has transitioned from a mere criminal activity, into an activity to replace real currency. In certain instances, particularly during wartime, it has become the 'act' in itself, where the infusion of high quality counterfeit currency has been used to attack the economy of a country by eroding faith in its currency. The most prominent and commonly known cases are Operation Bernhard in World War II when Germany tried to destroy the British economy by counterfeiting huge amounts of British pounds; and the Hungarian plot to destabilise the economy in France as an act of revenge after having lost huge parts of their territories in the Peace Treaty of Versailles in 1919 after World War I. The plot and the level of political involvement in Hungary were of such a magnitude that it triggered the international community to establish the CCC 1929.

In recent times, India has also reported large scale use of counterfeit currency, by both State and non-State actors, to assist/fund terrorist acts. The case studies in this regard furnished by India, expose the scale and intensity of the problem. In particular, there is evidence of multiple bases being used to flood the country with counterfeit notes, thereby attempting to attack the 'economic security' of the country, besides, using it to fund/ assist specific terrorist acts. This in turn, constitutes a new dimension to the phenomenon of criminal activity related to currency counterfeiting. It is in this light that India has taken measures to amend laws relating to terrorism, to include within its ambit, trafficking of high quality counterfeit currency, as a 'terrorist act' (PRS Legislative Research India, 2013). The amendments redefine "raising funds" to mean, raising, collecting, and providing funds through the production, smuggling, and circulation of counterfeit currency.

The involvement of some state actors in counterfeiting of currency also in other parts of the world has been suspected; e.g., there have been reports of North Korea being involved in production and smuggling abroad of counterfeit US currency, as well as other contraband items[57].

India's experience shows that counterfeit Indian currency notes have been known to be a source of terrorist financing in India. Apart from the trade being a profitable business venture, the protracted involvement of agencies located abroad in the manufacture and supply of counterfeit Indian currency notes has revealed its usage in terror financing activities in India. These instances uncovered the TF element of counterfeit Indian currency notes for terrorist groups such as:

- Lashkar-e- Taiba LeT
- Al-Badr
- Harkat-ul–Jehad–E–Islami/*Harkatul Jihad al Islami (* HuJI)

56 UNODC (2012).

57 Hesterman, J.L. (2004) and US Government (2011).

- Jamait-ul-Mujahidden Bangladesh (JMB), and
- Specially designated global terrorist Dawood Ibrahim and his associates.

Box 16: **Seizure of Counterfeit Currency with Explosives from Terrorists in Bangladesh and linkage with terror outfit**

On 30 March 2013, Dhaka Metropolitan police arrested four Pakistani and 7 Bangladeshi nationals from Mirpur, Dhaka on charges of conspiring to carry out subversive activities in Bangladesh and illegal possession of counterfeit Indian currency notes. The seizure included counterfeit Indian currency notes with a face value of INR 12.9 million, USD 4 000 in cash, a small amount of Pakistani currency and some explosive materials. The arrested Pakistani nationals were professional counterfeit Indian currency notes carriers and had visited Bangladesh on several occasions in the past. Two of the arrested persons also functioned as Hawala operators besides engaging in counterfeit currency notes trafficking. One of the arrested Bangladesh nationals had figured in several cases in the past and frequently travelled to Pakistan, Singapore, Thailand and India in connection with counterfeit currency notes business. Two of the arrested were in possession of both Pakistani and Bangladesh citizenship documents.

Source: India

In conclusion, and by answering the question raised at the beginning of this chapter it can be said that although terrorists may not be directly involved in the production of counterfeit currency, they are known to circulate it and benefit from the proceeds of currency counterfeiting. The combination of high profits stemming from currency counterfeiting crimes, coupled with comparatively low priority assigned to it by the LEAs, has attracted both terrorists and their sympathisers.

III. PREVENTING AND COMBATING COUNTERFEITING OF CURRENCY AND RELATED CRIMINAL ACTIVITY

The success of any counterfeit currency trafficking operation depends on several factors. Foremost amongst them is the quality of the counterfeit currency. The more security features a banknote has, the more difficult it is to be counterfeited. Governments around the world continually review the security features of their currency to protect it against the threat of counterfeiting. Regular assessment of the usefulness and public acceptance as well as upgrading of visible and machine-readable security features are found to be very effective preventive measures in most jurisdictions.

Useful security features for banknotes include *inter alia* security paper and embedded features such as fibres and security threads, different types of watermarks, the use of optical variable inks (OVI), micro and macro lettering, the use of *intaglio* printing techniques and hologram patches. Currently, it is very difficult for criminals to produce counterfeits by incorporating imitated security features in a manner that will go undetected. Nevertheless, their level of sophistication and innovation is getting better by the day.

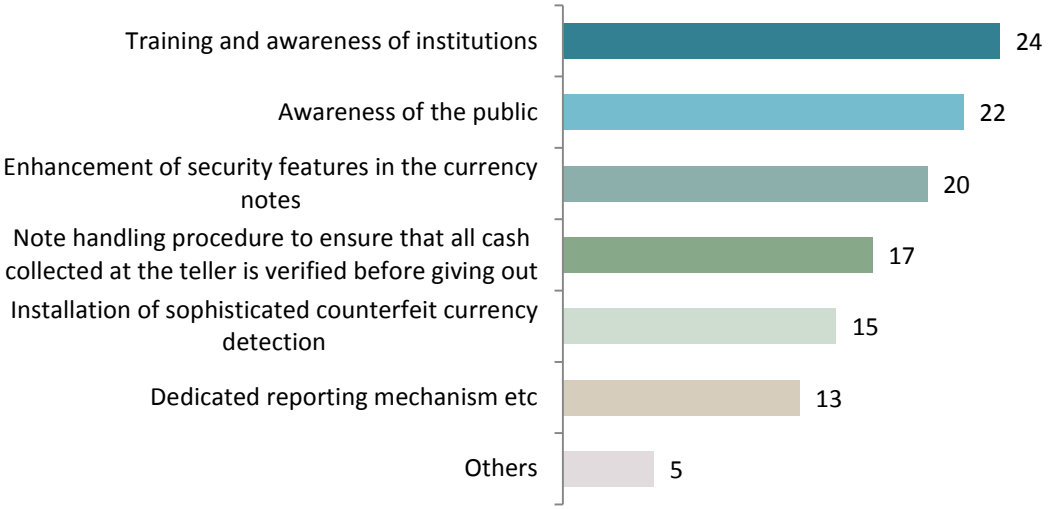
Other factors that help prevent easy introduction of counterfeit currency into the financial system include an alert and knowledgeable public that is familiar with the features of the genuine currency, and the availability of cheap and user-friendly technology capable of aiding identification of counterfeits.

Preventive measures therefore need to encompass all measures mentioned above and need a multidisciplinary approach involving close co-operation between banknote issuing authorities, LEAs, financial institutions and DNFBPs. Such measures need to be applied in several ways including measures to, design banknotes to make them difficult to replicate, train the public and raise their awareness, and monitor currency in circulation to detect counterfeits.

Financial institutions and DNFBPs by virtue of handling large volumes of physical currency have to be particularly alert in ensuring that counterfeit currency does not enter the legal money flow. The survey responses revealed that banks, MVTS, foreign exchange agencies, post offices, dealers in precious metals and stones, insurance companies and real estate agents are some of the key actors dealing with large volumes of currency. The preventive measures taken by the financial institutions and DNFBPs therefore mainly involve detection, reporting, training and awareness.

All currency notes generally have machine-readable features which can be used for detection of counterfeit notes. Ultraviolet light is an easy and common method used in the detection of counterfeit notes. Financial institutions dealing in large amounts of currency notes therefore generally use high precision and sophisticated note sorting machines and/or desktop sorters through which all currency notes tendered are passed. ATMs frequently also have inbuilt features that ensure detection of CCN and consequently do not disburse them in ATMs. The 'Cassette Swap System' which enables tamper proof transportation of cash to the ATMs and other destinations could be more widely used while transporting currency notes through cash transport companies to avoid possibility of substitution en route. Further, on detection, the counterfeit notes should be impounded and defaced/stamped as counterfeit and should under no circumstances be allowed to re-enter the financial system.

Chart 9. **Preventive measures employed to combat to counterfeit currency**



After detection of the CCN, the next logical step is reporting to the police as well as a central agency for investigation and/or feeding of a database for later cross-referencing abilities. Most of the jurisdictions which responded to the survey have a system of reporting to the police as well as to a central agency, generally the central bank or finance ministry. The detections are reported to the police for investigation and prosecution depending on the legal system in each jurisdiction.

A joint Europol/Dutch National Bank study indicates that the reporting can be quite influential in whether prosecuting a counterfeiting case is mandatory following the principle of legality opposed to the mere principle of opportunity.

Training and awareness are crucial to the success of the preventive measures adopted for all parties involved in dealing with the recognition of genuine and counterfeit currencies. The best way the public can protect itself from counterfeit currency is to be familiar with security features. A large number of countries have reported lack of awareness amongst the population as the main impediment to the effective detection of CCN. Almost all countries responding to the survey reported the use of one or several awareness-raising programmes, such as using posters, pamphlets, and brochures. Some countries also reported using short documentary films and web pages having audio visual contents on genuine and counterfeit notes. Interactive games are another media used for that purpose. Seminars, exhibitions, and press conferences by LEAs; direct enquiry hot line, student ambassadors, workshops and display of signage at traffic signals have also been used to spread awareness among members of the public. The impediments in effective detection of counterfeit currency are shown in the following chart.

Chart 10. **Impediments to effective detection of counterfeit currency by the financial institutions and DNFBPs**

1. ROLE OF REGULATORS AND FIUS

According to information collected from the questionnaires, FIUs are currently not involved in combating currency counterfeiting but nevertheless have an important role to play in its prevention in association with ML.

Financial sector regulators, such as central banks, play a major role in detecting and reporting CCN. Based on the reports received, regulators can assess the requirement and need for training and awareness programmes as well as for increased or more widespread use of devices for detection of counterfeit notes. The assessment and feedback is used for taking policy decisions and issuing necessary instructions to the financial institutions regarding detection, impounding, defacing and reporting of the CCN. Most regulators also put a proper oversight mechanism in place in all financial institutions, particularly where large amounts of currency notes are handled, to ensure that effective measures are in place for detection and reporting of the counterfeit notes.

FIUs can use the reports of detections of CCN for trend analysis (temporal as well as geographical/spatial) and to identify scenarios and possible red flag indicators from a ML and TF perspectives. From the analysis of the reports and information received from the financial institutions and with the help of possible red flag indicators (see below), important inferences can be drawn about the locations, accounts and suspected persons that might be involved in dealing with CCNs. This analysis can be further exploited with supporting information from LEAs that undertake enforcement functions in respect of the CCN, to identify suspects engaged in currency counterfeiting. The results of analysis can then be used either to collect more intelligence, if necessary, or for the LEA to undertake investigations against the suspected persons. The information that the financial institutions have about these suspects may also be obtained to help identify their assets. This information could then be used as justification for the use of provisional

measures (for example, the attachment of properties) in the event that a ML and/or TF case is established.

A. RED FLAG INDICATORS

In general, red flag indicators that apply to counterfeiting also apply to most of the predicate offences. Red flag indicators for detection of suspicious transactions relating, *inter alia*, also to counterfeit currency have been identified as follows ('e' and 'h' relate specifically to counterfeit currency):

a) Activity inconsistent with customer profile;

b) Multiple deposits below a certain threshold;

c) Same day transactions conducted at different bank branches;

d) Deposit from different counters under the designated threshold;

e) Cash deposits made to one account at the same place by multiple individuals;

f) Splitting large currency deposits among several accounts.

g) Customer makes frequent deposits or withdrawals of large amounts of currencies for no apparent business reason or for a business that generally does not generate large amounts of cash;

h) Small value cash deposits in multiple locations followed by immediate cash withdrawals in locations where counterfeit currency groups are active;

i) Subjects wanted by the authority for currency counterfeiting offences;

j) Cash deposits with small denomination banknotes, to perform wire transfers;

k) The banknotes brought by customers; being small denominated and dirty, existence of stains demonstrating that it has been carried concealing in various elements and giving off smell, packaged carelessly and precipitately, lacking or exceeding substantially than the declaration of customer when counted, coming across with counterfeit banknotes in the bankroll;

l) The involvement of high denomination banknotes – this is by virtue of the fact that high denomination bank notes carry larger intrinsic value (see SOCA, 2010).

2. ROLE OF LEA AND OTHER INVESTIGATIVE AUTHORITIES

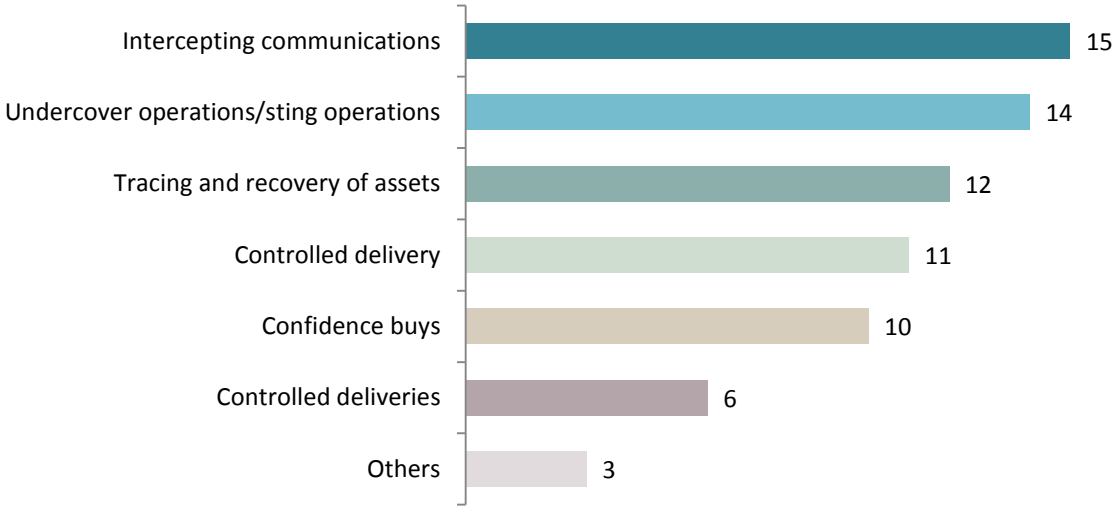
LEAs play a very important role. Firstly, by preventing physical entry of CCNs into the jurisdictions in case of cross-border movements and into the economy in case of domestically CCN. Secondly, by taking effective action against the offenders involved in currency counterfeiting. Such LEAs that are established as a national contact point for other branches within and across one jurisdiction are often associated to the National Central Office with regard to Article 12 of the CCC 1929. Those LEAs collect and produce information and intelligence, co-operate with other key institutions and with counterparts across borders. The data obtained is analysed to study trends, profile persons and routes, to identify possible *modus operandi*, and to identify possible weaknesses and risk areas for

further suitable preventive measures and, although rarely seen, socio-economic reports on the phenomenon.

Effective prosecution ensuring timely and commensurate punishment, including financial sanctions and attachment of properties, can serve as a major deterrent to the offenders.

The situation regarding the possibility of using 'special investigative techniques' to combat counterfeit currency: namely undercover/sting operations, intercepting communications, controlled deliveries, tracing and recovery of assets, confidence buys or fictitious purchases, varies from jurisdiction to jurisdiction. However, it seems that the most important of those techniques are – if not widely used – at least allowed by the legislation in many countries. The Survey responses provide some detail on the frequency of usage of these techniques by countries as shown in the chart below.

Chart 11. **Special investigative techniques used to combat counterfeit currency**



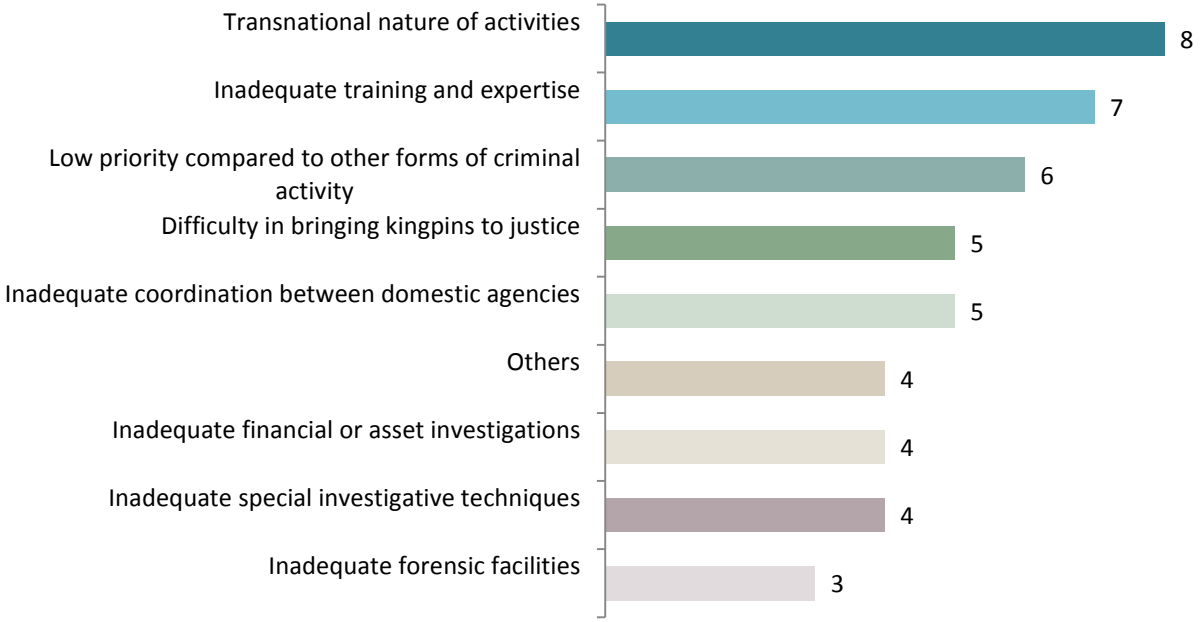
The survey responses also provided some indication of the obstacles facing countries in investigations which need to be considered in assessing the effectiveness of the domestic legal regime.

LEAs and other key institutions in the fight against currency counterfeiting such as central banks, and finance or treasury ministries also develop tailor-made strategic analysis products to combat currency counterfeiting such as:

- Trends over time in detection of counterfeit currency in terms of face value and number of notes of each denomination;
- Geographical distribution in detection of counterfeit currency in terms of face value and number of notes of each denomination;
- Statistics showing sudden increase in detection of counterfeit currency in terms of face value and number of notes of each denomination in a particular geographical area;

- Periodic identification of reports related to currency counterfeiting, and trends of information contained in said reports;

Chart 12. **Impediments encountered when conducting investigations related to counterfeiting of currency**



Having efficient reporting mechanisms in place is the primary basis for analysis of any kind of criminal phenomenon. At national and international level, obligations regarding the reporting of counterfeit money and the establishment of a specific chain of reporting should exist. Another critical aspect is the legal obligation to withdraw counterfeits from circulation. In most jurisdictions, unsurprisingly, both obligations are in place. It is also seen that the reporting obligation is widely used with few exceptions. For example, EU member states have the obligation to report to Europol in its role as being European Central Office for combating euro counterfeiting[58].

There are shortcomings in LEAs and their preventive measures, the following have been identified: the lack of reinforced controls at strategic advantageous locations such as airports, train and bus stations or border crossing points, specialised research and studies (e.g. socio-economic reports on the phenomenon), forecasting and scenario planning, training including the education of money sniffing dogs, and in the light of advanced technology and digital offset also enhanced co-operation with manufacturers such as the Japan Business Machine and Information System Industries Association (JBMIA) or the Central Banks Counterfeit Deterrence Group (CBCDG).

3. ROLE OF CUSTOMS AUTHORITIES

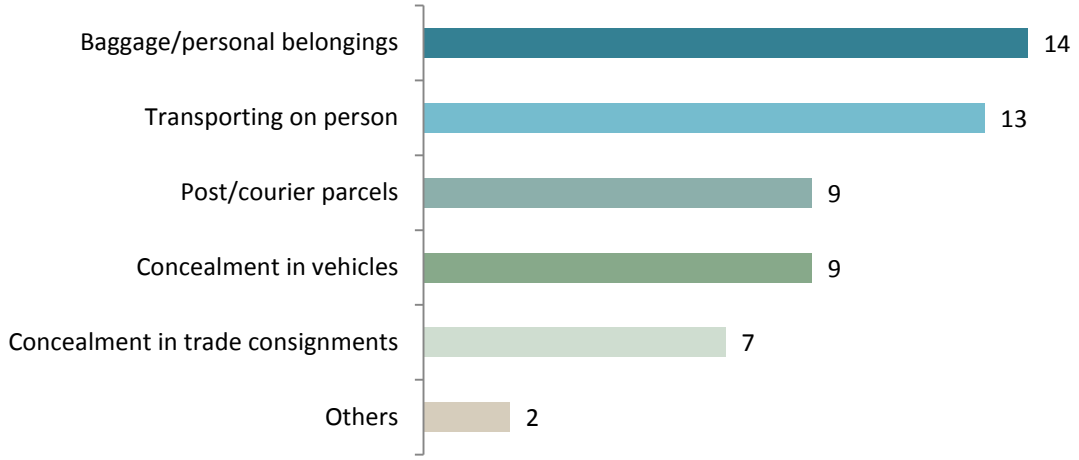
Customs authorities have a primary responsibility in preventing the entry of CCN into the country. Pre-entry measures include developing intelligence about routes, criminals, and criminal gangs

[58] See Council Decision 2005/511/JHA of 12 July 2005 on protecting the euro against counterfeiting, by designating Europol as the Central Office for combating euro counterfeiting.

involved in production, movement or distribution of CCN and *modus operandi* adopted. This may be done through risk-based screening of goods and persons entering into their jurisdiction, border management and patrolling. As part of the strategy, sea, land or air routes susceptible to misuse need to be identified on a dynamic basis. Proper co-ordination with other LEAs and necessary domestic as well as international cooperation is the key to any effective preventive strategy.

The transnational character of currency counterfeiting implies the use of techniques for cross border smuggling. Those techniques are diversified but are in principal comparable to the techniques used to smuggle genuine money:

Chart 13. **Modes used for cross border smuggling of counterfeit currency**



However, the first two techniques, that is to say transporting CNN on person and baggage/personal belongings, are by far the most used by smugglers of CCN. The nature of the methods used for the transport also depends on the geography of the country concerned.

The role of customs in investigations is similar to that of other LEAs as discussed in the previous section. Since the seizures by customs of CCNs are essentially transnational in nature, international co-operation and mutual assistance amongst various customs formations become imperative in combating counterfeiting. Various international conventions such as the Nairobi Convention of 1977 and the Johannesburg Convention of 2003 emphasise the need for bilateral co-operation on enforcement of customs laws. Mutual assistance between customs authorities can significantly mitigate risk and limitations of jurisdiction thereby leading to improvement in detection, interdiction and prosecution of such activity.

In any case, all the provisions of FATF Recommendation 32, which requires jurisdictions to implement measures to detect and prevent the physical cross-border transportation of currency and bearer negotiable instruments, cover both incoming and outgoing cross-border transportations of currency (and bearer negotiable instruments) by any of the following three methods of transportation: (1) by cash couriers, (2) through the post or (3) by containerised cargo. Based on the experience of jurisdictions with the implementation of Recommendation 32, the FATF published a revised best practices paper on the subject in 2010 (replacing an older paper from 2005[59]).

[59] FATF (2005).

IV. LEGAL FRAMEWORK AND INTERNATIONAL COOPERATION

The study has so far shown that currency counterfeiting activities carried out by OCGs and to a certain degree by terrorist groups have an international dimension.

Box 17: **Smuggling of counterfeit Algerian dinars printed on stolen fiduciary paper, disruption of offset illegal print shop**

In September 2008, two Turkish citizens were inspected by the French customs at the airport of Marignane as they were about to fly back to Turkey. They were in possession of 51 103 counterfeit DZD 1 000 (Algerian dinars) banknotes with a face value of EUR 520 000.

The individuals denied knowing the counterfeit aspects of those dinar banknotes. They argued that the money represented the payment of an invoice by an Algerian client having bought some possessions in Turkey and having given mandate to one of the two Turkish citizens arrested for the recovering in France of his claim.

The first parallels tend to draw a link between this case and the armed robbery, committed in November 2006 in Marseille (South East of France) by a commando of 3 armed men. They robbed a road convoy transporting 22 tons of Algerian fiduciary paper.

Italian Central Office (UCIFM) informed the French police that an illegal print-shop of counterfeit dinar banknotes was broken up in January 2009 in the south of Italy by the Italian *Guardia di Finanza*. During this break-up operation, 345 000 counterfeit banknotes of DZD 1 000 were found with a roll (400 kg) of genuine Algerian fiduciary paper (including the watermark and the complete hologram of the Algerian State) produced in Germany.

It was established that the arrested Turkish citizen had a contact in Marseille who received Algerian counterfeit banknotes from an Italian citizen considered to be the supervisor of the production of counterfeit dinar banknotes within the Camorra's organisation.

In conclusion, after an armed robbery of dinar fiduciary paper rolls (for the Central bank of Algeria), two illegal print-shops manufacturing fake DZD 1 000 were discovered in Naples, Italy (in January 2009) and in Lyon, France (in October 2009). There were many arrests of "Naples group" members in Italy and organised crime gangs in France. The judgment of this case in France was delivered in December 2012 with sentences of 2 to 10 years of imprisonment.

Sources: France & Italy

In this scenario, special attention should be paid to two aspects which are key points in enhancing the efficiency and effectiveness of trans-border investigation, namely: (1) the legal framework - with particular attention to the available international instruments; and (2) the way the competent national authorities take advantage of those (international) tools by carrying out and putting in place international co-operation.

1. LEGAL FRAMEWORK

It would be impossible, or rather not that practical, to list all international and national rules and regulations established with regard to the legal provisions referring to counterfeiting of currency and/or aspects linked to ML and TF. Practical experience of the members of the project team and the information collected through the survey circulated prior to the drafting of this report, indicated that from the national point of view, the legal provisions about the way the (predicate) offence of counterfeit currency is tackled are generally adequate. This is in particular evident if one refers to the level of the penalties/punishments of criminal offences linked to counterfeit currency (including printing, circulation, smuggling, possession) or, in the case of ML and/or TF (related or not) to counterfeiting currency. The range of penalties - from three to more than 20 years of imprisonment can be in general terms considered as dissuasive and proportionate.

However, based on the survey responses, it seems that national legislation is more focussed on the ML and/or TF activity by itself and covers currency counterfeiting by default as one of the predicate offences rather than foreseeing specific ML/TF provisions relating to counterfeit currency.

For national provisions, the situation varies when it concerns the possibility of using the so-called special investigative techniques to combat counterfeit currency, namely: undercover operations/sting operations, intercepting communication, controlled delivery, tracing and recovery of assets, confidence buys, and controlled deliveries. Great prudence should be given to the fact that the number of survey response received cannot support a definitive conclusion. However, it seems that the most important of those techniques are - if not widely used - at least allowed by national legislation. This consideration also takes into account the practical experience of the experts of the project team. A different evaluation is possible when referring to the practical use of those special forms of investigation, but in this case, the questions did not request any figures on the use of those tools.

Investigations on counterfeit currency almost always require the need for establishing contacts with counterparts abroad, with the aim of making the investigation effective, researching evidence of an offence, apprehending fugitives, etc.

It is not by chance that the international community identified the need for establishing an international specific multilateral instrument: the CCC 1929, which is still “the” convention by definition in this field. Other instruments are of course in force at regional and/or bilateral level but it is still the most important reference in force worldwide. The Geneva Convention is a reference to look at with regards to the basic principle of co-operation, including binding measures (with some exceptions) that contribute to create a system and ensure important multidisciplinary tools, useful for enhancing the defence of national currencies.

The CCC 1929 actually includes important concepts for co-operation reflected in its articles enhancing identification, investigation, prosecution of counterfeit currency with a transnational dimension, the establishment of contacts between competent authorities, the provisions for the establishment and function of central offices to facilitate the exchange of information and or experience, etc.

Specific figures on the use of the CCC 1929 are not available. The last conference of the high contracting parties took place more than ten years ago, organised by INTERPOL. According to some

of the replies and the experience in the field, it seems that the concepts and tools offered by the CCC 1929 are in use in many contracting parties, next to other instruments at regional or bilateral level. Its ratification and use should be further supported and promoted, since it contributes to creating a system, and the multidisciplinary tools, for protecting currency and fighting against its counterfeiting at national and international co-operation level.

When referring to the issue of regional legal instruments in place that supplement the provisions of the CCC 1929, it is interesting to note the system in place within the EU, in particular for the protection of the euro (see Box 18). The EU legal instruments for the protection of the euro are in particular useful as one possible example of legal mechanism that national legislators could take into account when addressing the issue of administrative and criminal protection of their national currency, including by means of specific training programmes like the Pericles funding programme, managed by OLAF, the Anti-Fraud Office of the European Commission. Even if the EU legislation itself requires continuous updates to address new challenges and threats caused by the counterfeiters (and specific legislative initiatives in the field have been recently proposed by the European Commission), it represents today a valid basis for supplementing the provisions under the CCC 1929 and facilitates its application, without prejudice to the obligations under the CCC 1929 itself.

The legal instruments of the EU allow for co-operation and exchange of a wide range of information:

- exchange of technical and operational information
- harmonisation of laws,
- definitions
- co-operation between LEAs, judicial authorities and central banks, and
- technical expert analyses:,
    - EU expert analysis authorities (Counterfeit Analysis Centre for banknotes at the ECB and the coin analysis centre at the European Technical and Scientific Centre)
    - National analysis centres (National Analysis Centres for banknotes and Coin National Analysis Centres).

Box 18. **Examples provided by the EU instruments**

Council Framework Decision 2000/383/JHA of 29 May 2000 on increasing protection by establishing penal sanctions and other sanctions against money counterfeiting in connection with the introduction of the euro;

Council Framework Decision 2001/888/JHA of 6 December 2001 amending Framework Decision 2000/383/JHA on increasing protection by criminal penalties and other sanctions against counterfeiting in connection with the introduction of the euro;

Council Regulation (EC) 1338/2001 of 28 June 2001 laying down measures necessary for the protection of the euro against counterfeiting;

Council Regulation (EC) 1339/2001 of 28 June 2001 extending the effects of Regulation 1338/2001 laying down measures necessary for the protection of the euro against counterfeiting to those member states which have not adopted the euro as their single currency;

Council Regulation (EC) No 44/2009 of 18 December 2008 amending Regulation (EC) No 1338/2001 laying down measures necessary for the protection of the euro against counterfeiting;

Council Regulation (EC) No 45/2009 of 18 December 2008 amending Regulation (EC) No 1339/2001 extending the effects of Regulation (EC) No 1338/2001 laying down measures necessary for the protection of the euro against counterfeiting to those member states which have not adopted the euro as their single currency;

Council Decision 2001/887/JHA of 6 December 2001 on the protection of the euro against counterfeiting;

Council Decision 2001/923/EC of 17 December 2001 establishing an exchange, assistance and training programme for the protection of the euro against counterfeiting (the so called 'Pericles' funding programme, managed by the Anti-fraud Office of the European Commission/OLAF);

Council Decision 2001/924/EC of 17 December 2001 extending the effects of the Decision establishing the "Pericles" programme to the member states which have not adopted the euro as the single currency;

Council Decision 2005/511/JHA dated 12 July 2005 on protecting the euro against counterfeiting, by designating Europol as the Central Office for combating euro counterfeiting (based on which, Europol is also allowed to support - from a special budget – specific euro counterfeiting operations);

Commission Decision 2005/37/EC of 29 October 2004 establishing the ETSC and providing for coordination of technical actions to protect euro coins against counterfeiting;

Regulation (EU) No 1210/2010 of the European Parliament and of the Council of 15 December 2010 concerning authentication of euro coins and handling of euro coins unfit for circulation;

Council Regulation (EC) No 2182/2004 of 6 December 2004 concerning medals and tokens similar to euro coins;

Council Regulation (EC) No 46/2009 of 18 December 2008 amending Regulation (EC) No 2182/2004 concerning medals and tokens similar to euro coins;

Council Regulation (EC) No 2183/2004 of 6 December 2004 extending to the non-participating member states the application of Regulation (EC) No 2182/2004 concerning medals and tokens similar to euro coins;

Council Regulation (EC) No 47/2009 of 18 December 2008 amending Regulation (EC) No 2183/2004 extending to the non-participating member states the application of Regulation (EC) No 2182/2004 concerning medals and tokens similar to euro coins.

Additional instruments are also quite interesting in terms of judicial co-operation, namely the "European Arrest Warrant", applicable to counterfeiting and ML irrespectively of the dual criminality principle.

With respect to international instruments available for fighting the (possible) ML aspects linked to currency counterfeiting cases, it is appropriate to highlight that generally speaking – also according to the survey responses – the national legal frameworks do not address the ML or TF aspects of currency counterfeit *per se*, but rather by considering it in the framework of "predicate offences".

2. INTERNATIONAL CO-OPERATION

Given the trans-national characteristics of currency counterfeiting, it is important to address the issue of international cooperation. The UN Palermo Convention 2000, provides tools for international co-operation on prevention, investigation and prosecution, once a criminal offence is established and once the recognition of the requirements for making it applicable are satisfied

The survey in support of this research included specific questions not only on the role played by FIUs, LEA and customs, but also referred to some of the tools established through the international instruments mentioned in the previous section. Unfortunately, the picture is not complete, due to the limited number of replies received, including (for those who gave some feedback) with reference to possible comprehensive figures for example on the number of requests for co-operation or assistance sent or received.

Nevertheless, even in the absence of comprehensive replies, some conclusions can be drawn from the information obtained. With regard to the interaction between FIUs, customs and, LEA, the legal frameworks at national level are heterogeneous. If the view is limited to the analysis of currency counterfeiting and related ML or TF aspects, the majority of the cases appear to indicate either that there is no specific role played by one or more institution (FIU/customs), or that the role is not specifically recognised by the legislation but was undertaken as one of the core tasks of the agency, for example:

- ML provisions address any predicate offence, not exclusively currency counterfeiting.
- Cash controls at border lead to the detection of counterfeiting currency.
- Special forms of co-operation are used (also at international level) in the presence of certain types of criminal activity (for example when minimum thresholds enable the use of special investigative techniques, rather than specific provisions on currency counterfeiting).

In general terms, when it comes to international co-operation (to send/receive assistance), it seems the FIUs and customs play a limited role in purely counterfeit currency cases, since in the majority of the countries such cases fall under the competence of LEAs. The international LEA community is used to benefit from the opportunity offered by the contact with counterparts abroad.

However, the figures provided by those who replied are not enough to be considered as a representative sample of the actual situation. This is the reason why, for example, the project team could not focus more on the exchange of information, joint investigation, mutual legal assistance etc.

It is also true that there is a feeling that international co-operation resulting from informal, or not officially recorded, statistics is wider than what is said by official figures. This is an aspect of the international mutual assistance which is very well known to international law enforcement

"practitioners", whose networks of informal contacts are often used or based on personal relationships and thus are not reflected in official figures.

Box 19: **Counterfeiting of US dollars and euros**

On 19 December 2012, the Peruvian National Police (DIRINCRI - *Direccion de Investigacion Criminal*), in co-operation with the *Brigada de Investigación Del Banco de España* (BIBE), the US Secret Service and Europol, dismantled a counterfeit banknote print shop in Lima and arrested one suspect. A total amount of EUR 4 437 000 and USD 4 460 000 in counterfeit banknotes were seized, all 100 denomination notes. Printing equipment, including an offset press and materials for the production of banknotes, were also confiscated. The raid was the culmination of an extensive operation that has been ongoing for a number of months and has involved information sharing across a number of international law enforcement agencies. A Europol expert was on location to provide technical support to Peruvian authorities and to evaluate the counterfeit euro notes and machinery seized.

Source: Europol (2013)

Moreover, even if not addressing exclusively the currency counterfeiting sector, the experience made within some regions of the use of joint investigation teams or the network of liaison officers are evidence of a level of international co-operation that is most probably much higher than those expressed by available figures. Examples of structure and legal procedures for the establishment and conduct of such joint investigation actions or on the use of international liaison office/officers network are again offered also by the EU legislation/initiatives.[60]

On the other hand, the case studies collected by the project group about the use of special investigative techniques and/or the use of international co-operation testify of the significant cross-border aspects of currency counterfeiting and the benefits of international co-operation to the effectiveness of an investigation.

Box 20: **Organised crime syndicate involved in smuggling and distribution of counterfeit US dollars**

In September 2012, Secret Service agents in Lima, working closely with the Peruvian National Police (PNP) Dirincri "Estafas" unit, obtained investigative intelligence from a confidential informant regarding a transnational organised group distributing counterfeit US currency. The investigation identified "A" as the primary suspect, a former PNP officer and cousin of the "godfather" of the *Familia Nique* crime syndicate and creator of the Peruvian counterfeit note

[60] Examples involving joint investigation team structures and use of liaison officers:

www.europol.europa.eu/content/page/joint-investigation-teams-989

http://eurojust.europa.eu/Practitioners/Eurojust-Support-JITs/JITs/Pages/history.aspx

http://eurojust.europa.eu/Practitioners/Eurojust-Support-JITs/JITS-Funding/Pages/jits-funding-project.aspx

family.

Through extensive surveillance and the use of other electronic investigative techniques, Lima agents and PNP investigators discovered a group of co-conspirators who distributed large quantities of counterfeit US currency through commercial ground transportation. The suspects concealed the counterfeit notes in boxes of pastries and shipped the contraband on buses that travelled from Peru to Ecuador, Colombia and Venezuela. Once in Venezuela, the suspects transported the counterfeit cash, through various smuggling methods, such as hiding the notes in false bottom luggage and children's toys and bibles on commercial flights, to locations in the United States, primarily New York and Miami. During surveillance in Lima, agents and PNP officers observed three suspects smuggle counterfeit currency onto a passenger bus. The investigative coalition force executed a search warrant on the vehicle and seized USD 600 000 in USD 100 Federal Reserve Notes and arrested "A". A query of the Secret Service Counterfeit Tracking Application identified the seized currency as a member of circular family C-23985. These notes first appeared in Detroit, Michigan in 2009, and are forensically linked to the Peruvian note family, with a total passing history in excess of USD 26 million. On 6 October 2012, Lima agents and the PNP arrested under Peruvian Criminal Code for possessing and distributing counterfeit currency.

Source: USSS (2012)

Most jurisdictions have identified impediments in respect of international co-operation. In the study questionnaire, the following six issues were identified:

- Different types, operating standards, and powers of individual FIUs/LEAs;
- Different priorities of the countries;
- Differing quality and credibility of information exchanged;
- Late or no responses to requests; insufficient/ low quality of responses; unduly rejected requests;
- Lengthy and complicated (time-consuming) procedures for implementation of MoUs and other agreements on international cooperation;
- Language barriers make communication more difficult (especially for non-English speaking jurisdictions).

Box 21: **Project Colombia**

Since 1996, the US Secret Service has had a significant presence in Colombia working in collaboration with Colombian law enforcement officials toward the suppression of counterfeit US currency. Success in the fight against criminal organisations dedicated to the manufacturing of counterfeit US currency is a direct result of the Secret Service's commitment to providing support and leadership within both the law enforcement and prosecutorial entities in Colombia. The Secret Service operates and maintains a "Vetted Anti-Counterfeiting Task Force" (VACF) in Colombia, comprised of Colombian law enforcement officials from both their federal and national police

forces. Members of the VACF Task force undergo background investigations and ultimately are required to pass a polygraph examination given by a certified US Secret Service polygrapher before he/she can become a certified member of the VACF. This vetting process ensures the integrity of the VACF unit, and allows members to receive specific training including wire tracking, counterfeit detection, firearms training and tactical strategies.

Since the inception of the VACF Task force, the Secret Service has not only provided continued financial support but has worked with Colombian Government Officials to change Colombian Federal Statutes, ensuring criminals and criminal organisations responsible for counterfeiting can be punished appropriately within their judicial system. This relationship between the Secret Service and the Colombian Law Enforcement has proven so successful it has served as a model for forming additional Secret Service led anti-counterfeiting task forces throughout the world.

Since the Bogota Resident Office opened in 1996 thru 2011, total counterfeit currency related to the Colombian Note, seized is USD 372 319 095. The establishment of the Secret Service Resident Office in Bogota, Colombia and formation of the VACF has had a significant impact on the production of counterfeit US currency in Colombia. These successes, coupled with the ability to cripple organisations manufacturing US counterfeit currency would not have been possible without the establishment of the VACF and the noted cooperation between the Secret Service and Colombian law enforcement officials.

Source: United States

INTERPOL provides forensic support, operational assistance, and technical databases, in order to assist member countries in addressing counterfeit currency. The agency seeks to provide partnerships between LEAs, financial institutions, and central banks, as well as with security printing industry and high grade suppliers. Interpol provides the following services[61]:

- Classifying, analysing and storing genuine currency specimens and counterfeit banknotes;
- Circulating analytical reports among INTERPOL member countries;
- Determining whether suspect specimens are genuine or counterfeit;
- Allocating international indicatives to newly discovered counterfeits;
- Publishing descriptions of new counterfeit banknotes;
- Preparing and circulating tables of statistics on worldwide counterfeit
- Organising best practices exchanges.

Of particular interest are the yearly statistics published by INTERPOL for all counterfeit currencies discovered in INTERPOL member countries.[62]

61 Interpol (2013).

62 For detailed analysis of trends in counterfeiting please see Annexes.

One INTERPOL project to counter counterfeiting is Project S-Print – an international monitoring system on the security printing industry and suppliers, including the verification of second-hand *intaglio* machines, security printing equipment and suspicious purchase orders. The objective of the project is to reduce currency counterfeiting and altered security documents by preventing the necessary production materials and supplies from reaching the counterfeiters. The project has also formulated a checklist to help suppliers of printing materials identify orders that could be related to the manufacture of banknotes or identity documents[63].

In the FATF AML/CFT regime, counterfeiting finds a place. The interpretative note to the FATF Recommendation 3 (which deals with ML), states that countries should include a range of offences within each of the 'designated categories of offences'. The offence of ML should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence[64]. 'Counterfeiting currency' is one of the designated categories of offences[65]. This is in addition to the regulations in respect of terror financing which find a place in Recommendation 5-8 of the FATF Recommendations and the International Convention for the Suppression of the Financing of Terrorism.

Europol plays an important role in the efforts of the EU in combatting euro counterfeiting. Europol acts as the Central Office for combating euro-counterfeiting within the meaning of Article 12 of the Geneva Convention[66]. Within the context of its mandate, Europol:

- Works closely together with key playing institutions such as the ECB, the European Commission/OLAF, Eurojust and Interpol.
- Centralises, processes and analyses all information of a nature to facilitate the investigation, prevention and combating of euro counterfeiting and shares this information with the National Central Offices of the EU member states.
- Corresponds through the EU Liaison Office network with the National Central Offices of third countries in accordance with the rules on the transmission of personal data.
- Forwards on requests, and in line with the provisions of the CCC 1929, to the National Central Offices of third countries a set of specimens of actual euros.

Where counterfeiting of all other currencies is concerned, the National Central Offices retain their respective competence. The EU seeks to step up co-operation among member states and between member states and Europol with a view to protecting the euro against counterfeiting at

63 Interpol (2013).

64 FATF (2012), *p.* 34.

65 FATF (2012), *p.* 112.

66 See Council Decision 2005/511/JHA of 12 July 2005 on protecting the euro against counterfeiting, by designating Europol as the central office for combating euro counterfeiting.

international level. Third countries need a central contact for information on counterfeit euros. All such information is to be brought together for purposes of analysis at Europol.

The purpose of the Pericles Programme is to strengthen the protection of the euro against counterfeiting, taking into consideration transnational and multidisciplinary aspects. It seeks to promote content-convergence of the measures taken at European level to combat the counterfeiting of the euro and to ensure equivalence and homogeneity of the protection while observing the distinct traditions of each EU member states.

The programme envisages a four pronged strategy- of

- strengthening co-operation,
- technical, scientific and operational assistance,
- providing training and
- raising awareness to combat euro counterfeiting.

The programme seeks to closely support the establishment and completion of relevant protection structures (for example, national central offices against counterfeiting) in "relevant" third countries, enhance co-operation between countries as well between enforcement/financial structures, establish homogeneous and effective frameworks (legislation, procedures, and offices), support intelligence gathering, training, studies etc.[67].

The nature and scale of counterfeiting makes it obvious that counterfeiting cannot be exclusively tackled at the domestic level but needs sustained and substantial international co-operation. This is more so in the case of TF through counterfeiting, where the actors are often based in multiple jurisdictions.

International co-operation amongst states to combat counterfeiting with AML/CFT dimensions is usually based on time tested legal instruments such as bilateral treaties and multilateral conventions. Co-operation in individual cases is mostly through the processes of mutual legal assistance and extradition. Specifically, Recommendations 36-40 of the FATF Recommendations provide mechanisms for international co-operation in ML and TF cases. Mutual legal assistance could encompass a range of activity, from freezing/ confiscation/ evidence collection/ aids to investigation to prosecution assistance, extradition etc. Domestically, the agencies seeking such co-operation could be FIUs/LEAs.

FIUs seek co-operation through the Egmont Group, as well as the FATF or FSRBs[68]. The police typically use the extensive Interpol system for mutual assistance.

---

67 See European Commission (2012a).

68 There are 8 FSRBs which include The Eurasian Group (EAG), Asia/Pacific Group on combating money laundering (APG), Caribbean Financial Action Task Force (CFATF), Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe (MONEYVAL), Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Financial Action Task Force on Money Laundering in South America (GAFISUD), Intergovernmental Action Group against Money-Laundering in West Africa (GIABA), Middle East and North Africa Financial Action Task Force (MENAFATF).

Import of counterfeit currency is also covered by customs laws in most jurisdictions, and international co-operation mechanism in respect of customs laws therefore also apply. Besides the World Customs Organisation, the International Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offences (Nairobi Convention 1977), and the International Convention on Mutual Administrative Assistance in Customs Matters (Johannesburg Convention 2003) provide a framework mechanism in this regard. This is in addition to bilateral and regional customs agreements, as well as regular informal channels of communication. Mutual legal assistance between customs administrations significantly mitigates risk and limitations of countries, thereby leading to an increase in detection, interdiction and prosecution of such activity.

In respect of the role of FIUs, these units have dealt with counterfeit currency queries in Australia, India, Spain, Tajikistan and the United States. No such queries had been dealt with in France, Mexico, Nepal and Turkey.

In respect of LEAs, all countries which responded to the survey have suggested that LEAs do send/ receive requests for international co-operation in counterfeit currency cases. Particularly, with regard to exchange of information, Belgium has substantial engagement, having sent 58, and received 96 requests. In respect of requests for conducting enquiries/ trials, France (1 sent, 12 received) and Belgium (3 sent, 75 received), have utilised this mode of co-operation. In respect of joint investigations, Turkey was the only country which reported use of this method.

Box 22: **International co-operation and exchange of information**

A planned operation was initiated in accordance with the analysis based on the information given by German liaison officers about the suspects of counterfeiting of currency who were arrested in Germany.

A meeting was held with German officials at the later stages of the investigation. Thanks to the international co-operation, many suspects were arrested in the operation and counterfeit Russian rubbles (valued at USD 994 500) were seized.

Source: Turkey

Italy in particular, stated that since it is a country known for producing counterfeit currency, there is a continuous flow of information from/to foreign countries both in and outside Europe. Furthermore, operational meetings between investigators are quite frequently organised and, in some cases, joint investigations conducted by Italian and foreign law enforcement agencies have been carried out, sometimes with the involvement of their respective judicial authorities. In this regard, the most active co-operation has been with France, Germany and Spain due to the importance of these countries from the standpoint of economy, finance, circulation of money as well as the statistical impact of currency counterfeiting within their national territories. Italy submitted 893 requests for information in 2012 and received 1554.

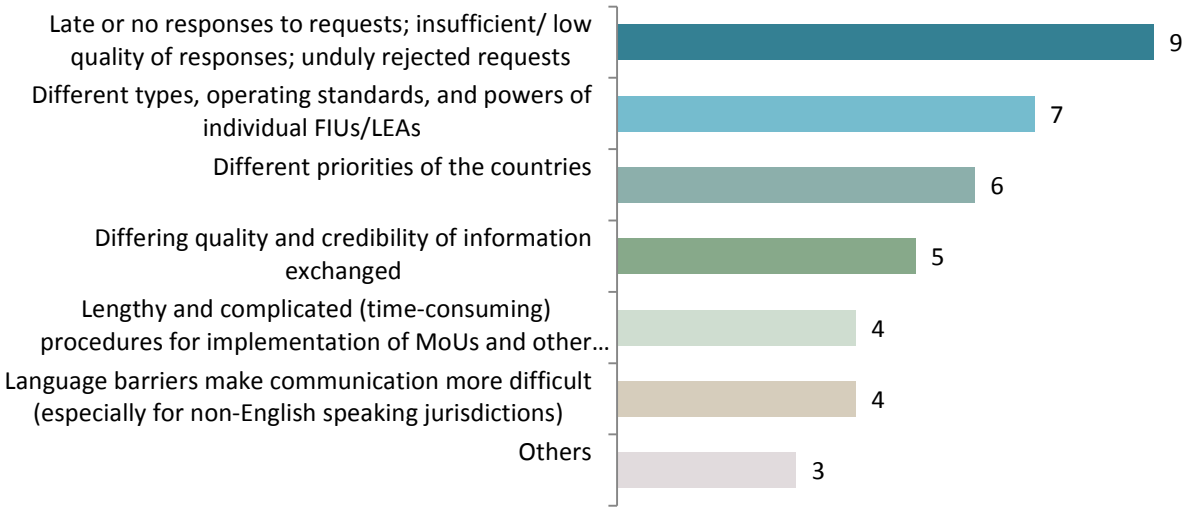
Box 23: **International co-operation (Printing of counterfeit US dollars)**

In October 2011, Italian law enforcement officials from the *Polizia di Stato* contacted the US Secret Service Rome Field Office requesting assistance with a counterfeit US currency investigation. The initial investigation identified a primary suspect. *Polizia di Stato* informed the Secret Service Rome Field Office of an investigation regarding an organised criminal group involved in a series of bank robberies throughout Italy. Utilising electronic investigative techniques and surveillance conducted during the investigation, *Polizia di Stato* identified an apartment located in La Spezia, Italy believed to contain counterfeit US currency. On 7 October 2011, members of the *Polizia di Stato* executed a search warrant revealing USD 1.78 million in counterfeit USD 100 banknotes, an offset printer, printing plates and negatives. On 7 October 2011, the primary suspect was arrested by Italian law enforcement and was charged with manufacturing counterfeit foreign currency. Criminal and MCI checks of the suspect revealed that suspect was of record with the Secret Service regarding previous counterfeit investigations dating back to 1986 and 1989.

Source: USSS (2012)

Survey responses to the question on the impediments encountered in providing or receiving international co-operation are indicated in the chart below.

Chart 14. **Impediments to international co-operation related to counterfeit currency**



The United States, in addition to the above, suggested that participation by inappropriate government officials as another matter of concern.

V. CONCLUSIONS

Currency counterfeiting is as old as money as a unit of exchange itself. With the internationalisation of money and its acceptance beyond local markets, currency became more attractive to counterfeiters. The US dollar, the euro or the British pound sterling are being circulated worldwide and trusted to hold their value. Favourable conditions such as inflation, political and economic instability, an underdeveloped banking sector, or a lack of convertibility of the domestic currency, prompt people to use such "hard currencies". As seen by the example of Bulgarian based OCGs, changing preferences for certain hard currencies has the potential to make counterfeiters switch to the production of other currencies.

The importance of currency as a symbol of sovereignty and main contributor to economic stability triggered the international community to establish the CCC 1929. Still today, currency counterfeiting presents a threat to national economies. It is not so much the financial damage, which in fact is quite low compared to other forms of criminal activity, but the impact it has on the "trustworthiness" of the currency. In contrast, and as the survey results show, it seems that governments, LEAs and FIUs give a relatively low priority to combating currency counterfeiting. The problem is further accentuated by the fact that hardly any scientific research has been undertaken on this subject and its relationship to other forms of criminal activity. Estimates of the related proceeds of crime are rare, incomplete (only 100 out of 190 Interpol members reported actual figures), difficult to calculate and mainly reflect circulated counterfeit banknotes that have been seized, while police seizures in print-shops dismantled are not taken into account for statistical purposes. For understandable reasons, regulatory bodies and central banks are not in favour of attracting big media attention to the issue of counterfeiting. There is an apparent underestimation of how much attention is needed to protect currencies and the way resources should be allocated to achieve an adequate level of protection against counterfeiting. Furthermore, that counterfeiting receives lower priority may in part be due to the fact that a number of jurisdictions have not yet felt the impact of this activity on their domestic economy.

Improvements in digital printing techniques play an increasing role in facilitating the business of counterfeiting. Today, in principle, anyone with basic computer skills has the tools at hand to become a counterfeiter. Cheap, but sophisticated, printers and software make counterfeiting a lucrative, easy and opportunistic activity.

Currency counterfeiting crimes generate high profits only when powerful mafia-style OCGs are involved. The research appears to indicate that internationally operating OCGs are heavily involved in the illegal business of currency counterfeiting on a global scale. The complexities involved in the large-scale printing, smuggling and distribution of counterfeit currency when produced by offset printing machines requires the involvement of organised criminal syndicates with international linkages. The study confirms the strong links between currency counterfeiting and other forms of criminal activity, such as drug trafficking and arms smuggling.

The involvement of international OCGs makes it extremely difficult for a single country to address counterfeiting on its own, and an urgent need for enhanced international co-operation appears to be necessary.

This report has focussed on the ML and TF aspects of this currency counterfeiting and concludes that there is a lack of awareness on this activity and its links to ML, and thus taking a closer look at the relationship between currency counterfeiting and ML appears to be justified. One important aspect is the fact that proceeds generated by currency counterfeiting are often "laundered" by investing them in other criminal enterprises, especially in relation to drugs trafficking and actual figures originating from the proceeds of counterfeiting are lost.

The survey responses indicate that various methods, such as intermingling counterfeit with genuine currency, purchasing goods of low value or use of cash-intensive business as a front for introducing counterfeit currency into the financial system are preferred *modus operandi*. Similarly, various methods such as, use of cash couriers; bank account; *hawala* or other types of alternate remittance methods are employed by criminal syndicates to move the proceeds of crime related to counterfeit currency. The proceeds of this activity are integrated by intermingling in cash intensive business, movement through multiple jurisdictions, movement through multiple accounts/entities, use of corporate structure and false declaration of goods and services. The study did not identify distinctive methods only used to transfer proceeds of crime generated by currency counterfeiting or their integration into the legal financial flow. More likely, methods associated with counterfeiting follow the same patterns as those for other forms of criminal activity. Among a number of red flag indicators, the use of high-denomination banknotes such as the EUR 200 and the EUR 500 banknotes raised some suspicion. The fact that they are object of counterfeiters in principle contradicts the finding that the commonly used denominations are also the most counterfeited ones.

The study concludes that terrorist organisations have resorted to the use of counterfeit currency for a variety of reasons. Training, recruitment, attacks and propaganda require large amount of funds; and terrorist groups have often resorted to the business of counterfeiting of currency as one of the means to fund such activities. While currency counterfeiting in relation to OCGs is a global phenomenon, its relation to TF is seen only in some regions around the globe and in isolated cases. There is growing evidence that some terrorist groups co-operate with OCG to produce counterfeit currency in order to fund their activities.

It has also been observed that in some instances, counterfeit currency has been used as a tool to destabilize the economy of a country. Huge quantities of high quality CCN are being infused into the financial system of a country which lowers the value of the currency, triggers inflation and thus does not only erode the faith of the people in their currency but might have the power – in its worst case scenario – to make the whole economic system collapse.

The survey responses indicate that international instruments of co-operation exist between countries for criminal matters in general. International co-operation is continuously evolving, and there are still substantial, unresolved challenges. Some of the responses indicate that there is still considerable room for improvement at international level with regard to co-operation, in order to ensure a wider awareness of the existence of specific legal tools, the use of such instruments and enhancement of mutual trust. To ensure wider acceptance and use of the international co-operation mechanisms indicated above, there is an urgent need for international funding programmes for training and staff exchanges. Significantly, there is also a need for better understanding of the fact that in international co-operation- “the more you give the more you receive”.

While many countries are dealing with the problem of counterfeit currency, some are still not signatories to the CCC 1929, and some of them are not even aware of the existence of such a convention. The responses also indicate that LEAs have so far, largely dealt with counterfeit currency as a distinct form of criminal activity but have rarely focussed on the ML and TF aspects associated with it.

All countries who responded to the survey indicated that they have their own internal reporting mechanisms in place regarding counterfeit currency; but there appears to be room for improvement here too. The need to report and compile all the information pertaining to counterfeit currency in each jurisdiction by a single authority, a national central office, is stipulated in Article 12 of the CCC 1929. The role of FIUs and customs in collecting and compiling this data needs to be explored. Countries also undertake training programmes for the LEAs, improving and upgrading security features and conduct public awareness programmes.

The laws pertaining to counterfeit currency seem to be in place and sufficient but need international/regional harmonisation to avoid the creation of "safe havens". The case studies and international examples show that special investigative techniques are very efficient tools in dealing with currency counterfeiting. Considering the involvement of OCGs and terrorist groups which operate in an inherently highly secret environment, it makes sense to encourage further use of these techniques in the context of currency counterfeiting investigations.

VI. POLICY IMPLICATIONS

The project has identified several policy implications for possible improvements:

There is an urgent need for enhanced international co-operation between all the actors involved, at different levels of responsibility such as: regulators, LEAs and judicial authorities, and other stakeholders in the field, including financial intermediaries. All jurisdictions need to consider ratifying and/or acceding to the CCC 1929 and consequently put in place all its required legal and organisational measures, in particular those on the establishment of a national central office as outlined in Article 12.

The findings of this study clearly indicate that counterfeiting currency and associated ML and TF risks are transnational in character. The activity is carried out by organized criminal syndicates with a transnational presence. The transnational nature of the risk could be further considered by the FATF and FSRB assessors during a country's assessment of compliance with the FATF Recommendations. This includes any information with respect to the use of that country for producing and/or smuggling of counterfeit currency of another country. This information would help to form an objective, authentic and comprehensive view for addressing transnational risk by the country under assessment.

For the purpose of getting a more complete picture of the subject matter, Interpol could be encouraged to expand its relevant questionnaire to include more on ML and TF issues.

At the national level, efficient reporting mechanisms and establishment of adequate institutional frameworks could also be further promoted. These mechanisms and institutions could help to achieve more effective co-operation amongst regulatory bodies, FIUs and LEAs. This could then also reinforce efforts to detect currency counterfeiting within entities dealing with large amount of cash (*i.e.,* financial institutions and DNFBPs).

Countries could focus on setting up national training programmes and multidisciplinary working groups. National authorities could also look at improving mechanisms for monitoring convicted "printers"/producers of counterfeit currency. Within such monitoring frameworks, authorities could also consider extending the length of time for data retention on currency counterfeiting activity to ensure that known criminals do not escape LEA and judicial attention. Within this framework, the possibility of launching regional or international funding programmes such as the European Commission's Pericles programme could be explored.

The continuous review and enhancement of security features of national currency as an effective preventive measure for combating counterfeiting seems to be an essential element of addressing the issue. The development of such security features should, to the extent possible, take advantage of the practical knowledge gained by LEAs.

LEAs – and in particular – customs authorities – need to pay greater attention to shipments of any material which can be used for printing counterfeit currency such as security inks, security paper and holograms. Manufacturers of key raw material used for printing money, such as security paper and security ink, could be encouraged to take more responsibility in ensuring that their products do

not fall in the hands of criminal enterprises. This could also facilitate investigations undertaken by the LEAs across the world. The Interpol S-PRINT project could help to reinforce this effort.

LEAs and other public authorities or initiatives, such as the Central Banks Counterfeit Deterrence Group (CBCDG), may wish to further develop co-operation with business machine manufacturers such as the Japan Business Machine and Information System Industries Association (JBMIA). It is necessary that the FIUs receive the information not only from the financial institutions where CCN is detected and impounded but also from the LEAs that intercept, seize and confiscate CCN and prosecute the offenders.

Due to the lack of knowledge and understanding on the subject matter, countries should consider undertaking multidisciplinary studies on the economic and social impact of counterfeiting by putting focus on ML and TF related issues. Scenario planning could also help to address possible unforeseen/unexpected new challenges.

Countries may also want to examine more closely the OCG pyramid-like structure and identify the level at which ML takes place. Finally, future studies of currency counterfeiting and associated money laundering could assist in better understanding how the use of high denomination banknotes is related to both activities.

ANNEX 1: RESPONDING JURISDICTIONS TO THE QUESTIONNAIRE[69]

No.	Jurisdiction
1	Anguilla
2	Australia
3	Austria
4	Bangladesh
5	Belarus
6	Belgium
7	Brazil
8	Curaçao
9	France
10	Germany
11	Hong Kong, China
12	India
13	Italy
14	Japan
15	Kyrgyz Republic
16	Latvia
17	México
18	Nepal
19	Russia
20	South Africa
21	Spain
22	Tajikistan
23	Turkey
24	United States
25	Uzbekistan

69 Austria, Belgium, France, Germany, Italy, and Spain have the same currency: the euro.

ANNEX 2: LIST OF 100 COUNTRIES, WHICH PROVIDED STATISTICS TO INTERPOL ON DISCOVERY OF COUNTERFEIT NOTES IN 2011

No.	Country
1	Andorra
2	Argentina
3	Armenia
4	Australia
5	Austria
6	Azerbaijan
7	Bahamas
8	Bahrain
9	Bangladesh
10	Belarus
11	Belgium
12	Benin
13	Bolivia
14	Bosnia and Herzegovina
15	Botswana
16	Brazil
17	Brunei Darussalam
18	Bulgaria
19	Burkina Faso
20	Cameroon
21	Canada
22	Chad
23	Chile
24	Colombia
25	Croatia
26	Cuba
27	Cyprus

No.	Country
28	Czech Republic
29	Denmark
30	Egypt
31	El Salvador
32	Estonia
33	Fiji
34	Finland
35	France
36	Germany
37	Hong Kong, China
38	Hungary
39	Iceland
40	India
41	Iran
42	Israel
43	Italy
44	Japan
45	Jordan
46	Kenya
47	Kuwait
48	Latvia
49	Lebanon
50	Liechtenstein
51	Lithuania
52	Luxembourg
53	Macao, China
54	Malaysia

No.	Country
55	Malta
56	Mauritius
57	Monaco
58	Mongolia
59	Montenegro
60	Morocco
61	Mozambique
62	Namibia
63	Nepal
64	New Zealand
65	Norway
66	Oman
67	Paraguay
68	Peru
69	Philippines
70	Poland
71	Portugal
72	Qatar
73	Romania
74	Russian Federation
75	San Marino
76	Saudi Arabia
77	Serbia
78	Seychelles
79	Singapore
80	Slovakia
81	Slovenia
82	South Africa
83	Spain
84	Sudan
85	Swaziland
86	Sweden
87	Switzerland
88	Syrian Arab Republic
89	The Former Yugoslav Republic of Macedonia
90	The Netherlands
91	Trinidad and Tobago
92	Tunisia
93	Turkey
94	Turkmenistan
95	Ukraine
96	United Kingdom
97	Uruguay
98	Uzbekistan
99	Venezuela
100	Zimbabwe

ANNEX 3: RESEARCH SURVEY

FATF TYPOLOGIES PROJECT

MONEY LAUNDERING AND TERRORIST FINANCING RELATED TO COUNTERFEITING OF CURRENCY

Initial Questionnaire

The goals of the FATF typologies project on counterfeiting of currency are:

- To identify and describe money laundering and terrorist financing methods associated with counterfeit currency
- To contrast the methods of placement of counterfeit currency with those of other criminal proceeds
- To study the linkage of counterfeiting of currency with organised crime, terrorist financing and other types of criminal activity.
- To identify AML/CFT measures that are useful in detection of counterfeiting of currency and associated ML/TF
- To identify red flag indicators for detection of suspicious transactions relating to counterfeit currency
- To identify gaps in the legal framework and/or mismatch in the operational interaction of LEAs, customs and FIUs preventing successful investigation and prosecution of ML/TF arising from counterfeit currency

A questionnaire has been developed to solicit basic information from FATF members and other participants. The information obtained through this questionnaire will assist the Project Team in establishing the general parameters of its work and in focusing its requests for further information.

The typology project does not cover counterfeit coins.

The questionnaire is divided into following sections:

- Section A: About Counterfeiting of Currency in general
- Section B: Money Laundering
- Section C: Terrorist Financing
- Section D: Preventive Measures
- Section E: Financial Intelligence Unit
- Section F: Customs Authorities
- Section G: Law Enforcement and Investigative Authorities
- Section H: International Cooperation

■ Section I: Legal Framework

Respondents are requested to return their completed questionnaires by December 11, 2012 to the FATF Secretariat.

THANK YOU FOR PARTICIPATING IN THE PROJECT.

October 26, 2012

	Country or Jurisdiction	
	Contact name and organisation	
	Contact Email	

SECTION A: GENERAL

Q.1	What is the national currency[70] / legal tender of your jurisdiction?
Q.2	What is the face value of the counterfeit currency (in USD) detected/seized in your jurisdiction in and before circulation? (The following two tables capture counterfeit currency detected by the financial institutions/DNFBPs 71and seizure by the law enforcement agencies separately. Please make a copy of the table if there are more than one counterfeit currency in the jurisdiction)

Name of Currency:			Exchange rate to USD as on July 1, 2012:			
	In circulation[72]					
	Detected by financial institutions or DNFBPs		Seized by Law Enforcement (excluding detection by financial institutions or DNFBPs)		Total counterfeit currency detected/seized	
	Number of Notes	Face Value (in USD[73])	Number of Notes	Face Value (in USD[73])	Number of Notes (1+3)	Face Value (in USD[73]) (2+4)
	(1)	(2)	(3)	(4)	(5)	(6)
2009						
2010						
2011						
Total						

70 National currency means, a currency which is issued by the sovereign Government of the country.

71 DNFBPs: Designated Non-Financial Businesses and Professions.

72 Counterfeit banknotes seized after they had caused damage (financial loss).

73 The face value has been sought in USD and the rate of conversion for all three years should be taken at the exchange rate of the national currency vis-à-vis USD as at 1 July 2012.

Name of Currency:			Exchange rate to USD as on July 1, 2012:			
	Before[74] circulation					
	Detected by financial institutions or DNFBPs		Seized by Law Enforcement (excluding detection by financial institutions or DNFBPs)		Total counterfeit currency detected/seized	
	Number of Notes	Face Value (in USD[75])	Number of Notes	Face Value (in USD[75])	Number of Notes (1+3)	Face Value (in USD[75]) (2+4)
	(1)	(2)	(3)	(4)	(5)	(6)
2009						
2010						
2011						
Total						

Q.3	What is the threat rating for counterfeiting of currency in your jurisdiction? Please check the relevant rating.	☐ Very High ☐ High ☐ Medium ☐ Low ☐ Very Low ☐ Others (Please use the space below to specify)
Q.4	What are the factors underlying the threat assessment of counterfeiting of currency in your jurisdiction? Please check all that apply.	☐ Adverse impact on the integrity of the financial sector ☐ Loss of trust in currency ☐ Large quantum of proceeds of crime generated/ laundered ☐ Linkage with financing of terrorism ☐ Linkage with drugs and other offences ☐ Others (Please use the space below to specify)
Q.5	Is there one currency production facility or multiple facilities that produce the currency notes?	
Q.6	Is there a methodology to estimate for the value of counterfeit currency in circulation in your jurisdiction? If yes, please provide the salient features of the methodology.	
Q.7	Is there an estimate as to how much of your domestic currency in circulation is counterfeit? If yes, please provide estimates of the value of such counterfeit currency in circulation in your jurisdiction?	
Q.8	Is there a national strategy to combat counterfeiting of currency? If yes, please provide the salient features of the strategy.	
Q.9	What is the competent authority for identifying and verifying that the suspected currency is counterfeit?	
Q.10	Name of the competent authority(ies) responsible for combating currency counterfeiting.	
Q.11	What is the name of the unit designated as the dedicated Nation Central Office (NCO) for combating currency counterfeiting according to Article 12 of the International Convention for the Suppression of Counterfeiting Currency of 1929?	

74 Counterfeit banknotes seized before they caused damage (financial loss), *e.g,.* seizures in confidence buys/sting operations, counterfeits seized in illegal print-shops or deposits.

75 The face value has been sought in USD and the rate of conversion for all three years should be taken at the exchange rate of the national currency vis-à-vis USD as at 1 July 2012.

Q.12	What equipment is utilized to examine the suspected counterfeit currency? (Microscopes, various light sources, magnetic detector, scanning electron microscope, RAMAN, GC/MS?)	
Q.13	Is there a certain special budget available for combating currency counterfeiting? Who provides this budget (police, national bank, international organisation or funding programmes, etc.?)	
Q.14	Are currency counterfeiting cases reported and administered at a central body?	
Q.15	Name of the competent authority(ies) responsible for combating money laundering related to counterfeit currency.	
Q.16	Name of the competent authority(ies) responsible for combating financing of terrorism related to counterfeit currency.	
Q.17	Is counterfeit currency linked with other predicate offences? Please check all that apply.	☐ Participation in an organised criminal group and racketeering ☐ Terrorism, including terrorist financing ☐ Trafficking in human beings and migrant smuggling ☐ Illicit trafficking in narcotic drugs and psychotropic substances ☐ Illicit arms trafficking ☐ Smuggling ☐ Others (Please use the space below to specify)
Q.18	Please provide case studies to show linkage of counterfeiting of currency with other predicate offences. (E.g. Cases in which counterfeit currency was seized along with drugs, illicit arms etc.)	
SECTION B: MONEY LAUNDERING		
Q.19	Are domestic organised criminal groups involved in printing and / or circulation of counterfeit currency as a profit-making activity? If yes, please provide percentage share of organised criminal groups in counterfeit currency.	
Q.20	Are international organised criminal groups involved in printing and / or circulation of counterfeit currency as a profit-making activity? If yes, please provide percentage share of organised criminal groups in counterfeit currency.	
Q.21	What methods are used for placement of counterfeit currency? Please check all that apply.	☐ Mixing counterfeit with genuine currency ☐ Intermingling in cash intensive business ☐ Gambling ☐ Purchasing goods of low value ☐ Selling it to people/kids ☐ Exchanging through currency exchanges ☐ Others (Please use the space below to specify)
Q.22	What methods are used for transfer of proceeds of crime related to counterfeit currency? Please check all that apply.	☐ Cash couriers ☐ Hawala or alternate remittance method ☐ Bank account ☐ Money transfer service ☐ ATM[76] Cards ☐ Others (Please use the space below to specify)
Q.23	What methods are used for layering and integration of proceeds of crime related to counterfeit currency? Please check all that apply.	☐ Movement through multiple accounts/entities ☐ Movement through multiple jurisdictions ☐ Mis-declaration of goods and services ☐ Intermingling in cash intensive business ☐ Use of corporate structures ☐ Others (Please use the space below to specify)

[76] ATM : Automated Teller Machine.

Q.24	Is there any estimate of proceeds of crime generated by the main operators in the chain of counterfeiting currency distribution chain (printer, distributor, retailer etc.)? (E.g. Distributors of counterfeit currency collect X% of the face value of the counterfeit currency from the retailer)		
Q.25	Please provide the quantum of counterfeit currency involved in top few (around five) cases (based on the number of counterfeit notes) that were investigated by your jurisdiction in last three years (2009, 2010 and 2011) and the quantum of counterfeit currency involved?		
	Year	No. of cases	Value of counterfeit currency involved (in USD)
	2009		
	2010		
	2011		
Q.26	How many cases of money laundering were investigated by your jurisdiction in last three years (2009, 2010 and 2011) and the quantum of counterfeit currency involved?		
	Year	No. of cases	Value of counterfeit currency involved (in USD)
	2009		
	2010		
	2011		
Q.27	Please provide case studies to show use of ML methods and techniques in counterfeit currency.		

SECTION C: TERRORIST FINANCING

Q.28	Is counterfeit currency used for resourcing/financing of terrorism?	
Q.29	What methods are used for resourcing/financing of terrorism from counterfeit currency? Please check all that apply.	☐ Counterfeit currency is provided to individual terrorist ☐ Counterfeit currency is distributed through terrorist network ☐ Proceeds are invested to strengthen terrorist support infrastructure ☐ Counterfeit money as means of economical warfare ☐ Financing of individual attacks ☐ Liaison with Organised Crime Groups ☐ Liaison with sovereign states ☐ Others (Please use the space below to specify)
Q.30	How many cases of terrorist financing related to counterfeit currency have been investigated by your jurisdiction in last three years (2009, 2010 and 2011)?	
	Year	No. of cases / Value of counterfeit currency involved (in USD)
	2009	
	2010	
	2011	
Q.31	Please provide case studies to show linkage of counterfeit currency with resourcing/ financing of terrorism.	

SECTION D: PREVENTIVE MEASURES		
Q.32	What preventive measures are employed by your jurisdiction to combat counterfeit currency? Please check all that apply.	☐ Enhancement of security features in the currency notes ☐ Installation of sophisticated counterfeit currency detection ☐ Note handling procedure to ensure that all cash collected at the teller is verified before giving out ☐ Dedicated reporting mechanism etc. ☐ Training and awareness of institutions ☐ Awareness of the public ☐ Others (Please use the space below to specify)
Q.33	Describe any education or awareness-raising provided to the public on genuine and/or counterfeit currency?	
Q.34	What type of financial institutions and DNFBPs deal with large amount of cash in your jurisdiction? Please check all that apply.	☐ Banks ☐ Insurance companies ☐ Money transfer service providers ☐ Foreign exchange agents ☐ Securities market intermediaries ☐ Post offices ☐ Real estate agents ☐ Dealers in precious metals and stones ☐ Others (Please use the space below to specify)
Q.35	What are the impediments in effective detection of counterfeit currency by the financial institutions and DNFBPs? Please check all that apply.	☐ Lack of awareness and training ☐ Gaps in currency handling procedures ☐ Inadequacy of mechanism to detect counterfeit currency ☐ Lack of expertise to detect counterfeit currency ☐ Compliance cost in handling/reporting seized counterfeit currency ☐ Fear of losing bona fide customers ☐ Apprehension of getting involved in legal proceedings ☐ Others (Please use the space below to specify)
Q.36	Is detection of counterfeit currency reported to the central authority such as Central Bank/ Ministry of Finance/Department of Treasury?	
Q.37	In the last two decades, how many times the security features of the national currency has been redesigned?	
Q.38	Are there machine readable components in your national currency?	
Q.39	Are law enforcement officials involved in the currency design and production process?	
Q.40	What happens to the counterfeits after examination (destruction, deposit, court, etc.)? Whether counterfeit currency is turned over to law enforcement officials?	
Q.41	Whether the counterfeit currency is subsequently collected and stored in a centralised location? If so, who maintains custody of the counterfeit specimens?	
SECTION E: FINANCIAL INTELLIGENCE UNIT (FIU)		
Q.42	Do financial institutions and DNFBPs report detection of counterfeit currency to the FIU in STRs[77]?	
Q.43	How many reports (including STR) related to counterfeit currency were received by the FIU in last three years (2009, 2010 and 2011) and the quantum of counterfeit currency involved?	

[77] STRs: Suspicious Transaction Reports.

	Year	No. of reports	Value of counterfeit currency involved (in USD)
	2009		
	2010		
	2011		
Q.44	Does FIU conduct outreach and training relating to counterfeit currency? If yes, please provide details.		
Q.45	What red flag indicators are used by the financial institutions/DNFBPs to detect proceeds of counterfeit currency? (E.g.: Small value cash deposits in multiple locations followed by immediate cash withdrawals in specific location, etc.)		
Q.46	What type of operational analysis is conducted by FIU to combat counterfeit currency? (E.g. Large value of counterfeit currency detected in one incident; Repeated incidents of counterfeit currency linked to the same person etc.)		
Q.47	What type of strategic analysis products are developed by the FIU to combat currency counterfeiting? (E.g. Identification of temporal and geographical trends and patterns in detection of counterfeit currency; Identification of localities showing sudden increase in detection of counterfeit currency for a period, etc.)		
SECTION F: CUSTOMS AUTHORITIES			
Q.48	Does Currency counterfeiting have a transnational character? Please check all that apply.	☐ Counterfeit national currency is printed abroad ☐ Counterfeit foreign currency is in circulation in the jurisdiction ☐ Others (Please use the space below to specify)	
Q.49	What are modes used for cross border smuggling of counterfeit currency? Please check all that apply.	☐ Carriage on person ☐ Baggage / Personal belongings ☐ Post/courier parcels ☐ Concealment in trade consignments ☐ Concealment in vehicles ☐ Others (Please use the space below to specify)	
Q.50	Do customs authorities give special attention to shipment of materials (e.g. security inks, security paper, printing-presses etc.) which can be used for printing counterfeit currency? If yes, please provide details.		
Q.51	Do customs authorities investigate cases of counterfeit currency?		
Q.52	Do customs authorities conduct the money laundering aspect of this investigation, or is it referred to a law enforcement agency?		
Q.53	Do customs authorities conduct the terrorist financing aspect of this investigation, or is it referred to a law enforcement agency?		
Q.54	Please provide case studies to show the role of customs authorities in combating counterfeit currency.		
SECTION G: LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES			
Q.55	Are special investigative techniques used to combat counterfeit currency? Please check all that apply.	☐ Undercover operations/sting operations ☐ Intercepting communications ☐ Controlled delivery ☐ Tracing and recovery of assets ☐ Confidence buys ☐ Controlled deliveries ☐ Others (Please use the space below to specify)	
Q.56	Are permanent or temporary multi-disciplinary groups specialised in financial or asset investigations formed to combat currency counterfeiting.		
Q.57	Is there any evidence available to suggest that counterfeit currency production is being sponsored by a foreign government?		

Q.58	Is there an analytical procedure in place to determine how suspected counterfeit has been produced and where the components for production are located?	
Q.59	What are the penalties/punishments related to following activities? Please mention penalty and punishment for the following.	
	Printing of counterfeit currency	
	Circulation of counterfeit currency	
	Smuggling of counterfeit currency	
	Possession of counterfeit currency	
	Money laundering related to counterfeit currency	
	Financing of terrorism related to counterfeit currency	
	Possession of equipment and raw material to produce counterfeits	
	Others (please specify)	
Q.60	Please mention any impediments encountered when conducting investigations related to counterfeiting of currency? Please check all that apply.	☐ Inadequate special investigative techniques ☐ Inadequate financial or asset investigations ☐ Inadequate training and expertise ☐ Inadequate forensic facilities ☐ Inadequate coordination between domestic agencies ☐ Transnational nature of activities ☐ Difficulty in bringing kingpins to justice ☐ Low priority compared to other fields of crime ☐ Others (Please use the space below to specify)
Q.61	Please provide case studies to show use of special investigative technique, multi-disciplinary coordination for combating counterfeit currency.	

SECTION H: INTERNATIONAL COOPERATION

Q.62	Does the FIU send or receive requests for information with international counterparts related to counterfeit currency? If yes, please provide number of requests		
Q.63	Do Law enforcement authorities send or receive request for international cooperation with international counterparts related to counterfeit currency? Please mention whether request for following types of international cooperation was sent or received.		
	Type of international cooperation	Number of Requests sent	Number of Requests received
	Exchange of information		
	Conduct inquiries and obtain information		
	Joint investigation to conduct cooperative investigations		
	Establish bilateral or multilateral arrangements to enable joint investigations		
	Others (please specify)		

Q.64	What are the impediments encountered in providing or receiving international cooperation related to counterfeit currency? Please check all that apply.	☐ Different types, operating standards, and powers of individual FIUs/LEAs ☐ Different priorities of the countries ☐ Differing quality and credibility of information exchanged ☐ Late or no responses to requests; insufficient/ low quality of responses; unduly rejected requests ☐ Lengthy and complicated (time-consuming) procedures for implementation of MoUs and other agreements on international cooperation ☐ Language barriers make communication more difficult (especially for non-English speaking jurisdictions) ☐ Others (Please use the space below to specify)
Q.65	Please provide case studies to show use of international cooperation for combating counterfeit currency.	
SECTION I: LEGAL FRAMEWORK		
Q. 66	Did your country ratify the International Convention for the Suppression of Counterfeiting Currency of 1929 (commonly known by "Geneva Convention" of 1929)?	
Q. 67	On which basis (legal framework) does you country combat currency counterfeiting?	
Q. 68	Are there any obligations as regards the transmission of international law into you domestic law?	
Q. 69	Are there any obligations about the reporting of counterfeit money or is there a specific chain of reporting (e.g. to a superior office, institution, organisation)?	
Q. 70	Are there any legal obligations to withdraw counterfeits from circulation after detection?	

ANNEX 4: STATISTICAL ANALYSIS OF QUESTIONNAIRE

Q. No.	Question	Options	Selected	Total	Percentage
Q.3	**What is the threat rating for counterfeiting of currency in your jurisdiction? Please check the relevant rating.**	Very High	1	22	5%
		High	4		18%
		Medium	4		18%
		Low	5		23%
		Very Low	8		**36%**
		Others	0		0%
Q.4	**What are the factors underlying the threat assessment of counterfeiting of currency in your jurisdiction? Please check all that apply.**	Adverse impact on the integrity of the financial sector	14	25	56%
		Loss of trust in currency	15		**60%**
		Large quantum of proceeds of crime generated/ laundered	4		16%
		Linkage with financing of terrorism	5		20%
		Linkage with drugs and other offences	12		48%
		Others	3		12%
Q.17	**Is counterfeit currency linked with other predicate offences? Please check all that apply.**	Participation in an organised criminal group and racketeering	12	25	48%
		Terrorism, including terrorist financing	5		20%
		Trafficking in human beings and migrant smuggling	5		20%
		Illicit trafficking in narcotic drugs and psychotropic substances	13		**52%**
		Illicit arms trafficking	3		12%
		Smuggling	9		36%
		Others	3		12%
Q.21	**What methods are used for placement of counterfeit currency? Please check all that apply.**	Mixing counterfeit with genuine currency	19	25	**76%**
		Intermingling in cash intensive business	11		44%
		Gambling	10		40%
		Purchasing goods of low value	19		**76%**
		Selling it to people/kids	14		56%
		Exchanging through currency exchanges	9		36%
		Others	1		4%
Q.22	**What methods are used for transfer of proceeds of crime**	Cash couriers	10	25	**40%**
		Hawala or alternate remittance method	5		20%

Q. No.	Question	Options	Selected	Total	Percentage
	related to counterfeit currency? Please check all that apply.	Bank account	7		28%
		Money transfer service	5		20%
		ATM Cards	2		8%
		Others	3		12%
Q.23	**What methods are used for layering and integration of proceeds of crime related to counterfeit currency? Please check all that apply.**	Movement through multiple accounts/entities	5	25	20%
		Movement through multiple jurisdictions	6		24%
		Mis-declaration of goods and services	4		16%
		Intermingling in cash intensive business	11		**44%**
		Use of corporate structures	5		20%
		Others	6		24%
Q.29	**What methods are used for resourcing/financing of terrorism from counterfeit currency? Please check all that apply.**	Counterfeit currency is provided to individual terrorist	4	25	**16%**
		Counterfeit currency is distributed through terrorist network	3		12%
		Proceeds are invested to strengthen terrorist support infrastructure	3		12%
		Counterfeit money as means of economical warfare	3		12%
		Financing of individual attacks	4		**16%**
		Liaison with Organised Crime Groups	2		8%
		Liaison with sovereign states	1		4%
		Others	1		4%
Q.32	**What preventive measures are employed by your jurisdiction to combat counterfeit currency? Please check all that apply.**	Enhancement of security features in the currency notes	20	25	80%
		Installation of sophisticated counterfeit currency detection	15		60%
		Note handling procedure to ensure that all cash collected at the teller is verified before giving out	17		68%
		Dedicated reporting mechanism etc	13		52%
		Training and awareness of institutions	24		**96%**
		Awareness of the public	22		88%
		Others	5		20%
Q.34	**What type of financial institutions and DNFBPs deal with large amount of cash in your jurisdiction? Please check all that**	Banks	24	25	**96%**
		Insurance companies	7		28%
		Money transfer service providers	19		76%
		Foreign exchange agents	15		60%

Q. No.	Question	Options	Selected	Total	Percentage
	apply.	Securities market intermediaries	3		12%
		Post offices	12		48%
		Real estate agents	7		28%
		Dealers in precious metals and stones	9		36%
		Others	7		28%
Q.35	**What are the impediments in effective detection of counterfeit currency by the financial institutions and DNFBPs? Please check all that apply.**	Lack of awareness and training	14	25	56%
		Gaps in currency handling procedures	10		40%
		Inadequacy of mechanism to detect counterfeit currency	10		40%
		Lack of expertise to detect counterfeit currency	15		**60%**
		Compliance cost in handling/reporting seized counterfeit currency	4		16%
		Fear of losing bona fide customers	9		36%
		Apprehension of getting involved in legal proceedings	8		32%
		Others	2		8%
Q.48	**Does Currency counterfeiting have a transnational character? Please check all that apply.**	Counterfeit national currency is printed abroad	10	25	40%
		Counterfeit foreign currency is in circulation in the jurisdiction	13		**52%**
		Others	2		8%
Q.49	**What are modes used for cross border smuggling of counterfeit currency? Please check all that apply.**	Carriage on person	13	25	52%
		Baggage / Personal belongings	14		**56%**
		Post/courier parcels	9		36%
		Concealment in trade consignments	7		28%
		Concealment in vehicles	9		36%
		Others	2		8%
Q.55	**Are special investigative techniques used to combat counterfeit currency? Please check all that apply.**	Undercover operations/sting operations	14	25	56%
		Intercepting communications	15		**60%**
		Controlled delivery	11		44%
		Tracing and recovery of assets	12		48%
		Confidence buys	10		40%
		Controlled deliveries	6		24%
		Others	3		12%
Q.60	**Please mention any impediments**	Inadequate special investigative techniques	4	25	16%

Q. No.	Question	Options	Selected	Total	Percentage
	encountered when conducting investigations related to counterfeiting of currency? Please check all that apply.	Inadequate financial or asset investigations	4		16%
		Inadequate training and expertise	7		28%
		Inadequate forensic facilities	3		12%
		Inadequate coordination between domestic agencies	5		20%
		Transnational nature of activities	8		**32%**
		Difficulty in bringing kingpins to justice	5		20%
		Low priority compared to other fields of crime	6		24%
		Others	4		16%
Q.64	**What are the impediments encountered in providing or receiving international cooperation related to counterfeit currency? Please check all that apply.**	Different types, operating standards, and powers of individual FIUs/LEAs	7	25	28%
		Different priorities of the countries	6		24%
		Differing quality and credibility of information exchanged	5		20%
		Late or no responses to requests; insufficient/ low quality of responses; unduly rejected requests	9		**36%**
		Lengthy and complicated (time-consuming) procedures for implementation of MoUs and other agreements on international cooperation	4		16%
		Language barriers make communication more difficult (especially for non-English speaking jurisdictions)	4		16%
		Others	3		12%

BIBLIOGRAPHY

Asia/Pacific Group on Money Laundering (2012), *Timor-Leste – Anti-Money Laundering and the Financing of Terrorism, Mutual Evaluation Report*, APG, Sydney, Australia

Bedi, R. (September/October 2005), *A new front – IPR theft, Money Laundering and Terrorist Financing*, International Centre for Political Violence and Terrorism Research IDSS Singapore, www.pvtr.org/pdf/Financial%20Response/IPR%20Theft%20and%20AML-CFT%20_IDSS_.pdf, accessed 25 October 2012

Berry, L., et al (October 2003), *Nations Hospitable to Organised Crime and Terrorism*, A Report Prepared by the Federal Research Division, Library of Congress under an Interagency Agreement with the United States Government., www.loc.gov/rr/frd/pdf-files/Nats_Hospitable.pdf, accessed 25 October 2012

Biersteker, T. J., & Eckert, S. E. (2008), *Countering the financing of terrorism,* Routledge, London.

Bovenkerk, F., & Chakra, B. A. (2007), "Terrorism and Organised Crime", In L. Holmes (Ed.), *Terrorism, organised crime and corruption: networks and linkages* (*pp.* 29-41), Elgar, Cheltenham

ECB (2013), *Biannual information on euro banknote counterfeiting*, www.ecb.int/press/pr/date/2013/html/pr130110_2.en.html, accessed 14 January 2013

European Commission (2012a), *OLAF, The 'Pericles' programme, Call for proposals*, http://ec.europa.eu/anti_fraud/documents/pericles-2012/call_for_proposals_2012.pdf, accessed 14 January 2013

European Commission (2012b), "Bulgaria: Technical Report Accompanying the document: Report from the Commission to the European Parliament and the Council on Progress in Bulgaria under the Co-operation and Verification mechanism {COM(2012) 411 final}", *Commission Staff Working Document*, http://ec.europa.eu/cvm/docs/swd_2012_232_en.pdf, accessed 14 January 2013

Europol (2011a), *OCTA 2011: EU Organised Crime Threat Assessment*, https://www.europol.europa.eu/content/publication/octa-2011-eu-organised-crime-threat-assesment-1465, accessed 14 November 2012

Europol (2011b), *25 arrested in joint counterfeit euro and drug trafficking investigation*, www.europol.europa.eu/content/press/25-arrested-joint-counterfeit-euro-and-drug-trafficking-investigation-1217, accessed 9 January 2013

FATF (2005), *Detecting and Protecting and Preventing the Cross-Border Transportation of Cash by Terrorist and other Criminals and other Criminals: International Best Practices*, FATF, Paris.

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: the FATF Recommendations*, FATF, Paris, www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html

Galeotti, M. (July 2009), Hard times – Organised crime and the financial crisis, *Jane's Intelligence Review* [electronic version not published in a periodical magazine]

GIABA (2010), *Threat Assessment of Money Laundering and Terrorist Financing in West Africa*, GIABA, Ponty Dakar, Senegal

Haken, J. (2011), *Transnational Crime In The Developing World*, *Transnational Crime In The Developing World*, Global Financial Integrity, Washington, www.gfintegrity.org/storage/gfip/documents/reports/transcrime/gfi_transnational_crime_web.pdf, accessed 14 January 2013

Hesterman, J.L. (2004), *Transnational Crime and the Criminal-terrorist nexus: Synergies and Corporate Trends*, USAF, April 2004, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA424418, accessed 25 October 2012

Interpol (2013), *Counterfeit currency and security documents*, www.interpol.int/Crime-areas/Financial-crime/Counterfeit-currency-and-security-documents/Counterfeit-currency, accessed 13 January 2013

Krylov, O.V. (2012), *Отдельные аспекты криминогенной обстановки в финансово-кредитной сфере* [Seperate aspects in criminal situations in financial and credit sphere], www.cbr.ru/publ/MoneyAndCredit/krylov_12_12.pdf, accessed 15 January 2013

Lowe, P. (2006), "Counterfeiting: links to organised crime and terrorist funding", *Journal of Financial Crime,* Vol. 13, Issue 2, *pp.* 255-257, DOI 10.1108/13590790610660944

RCMP (2007), *Counterfeit Currency in Canada*, RCMP, Canada, www.rcmp-grc.gc.ca/pubs/ci-rc/cf/cf-2007-eng.pdf, accessed 15 January 2013

Rollins, J., Wyler, L. S., & Rosen, S. (2010), *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress*, Congressional Research Service, CRS Report for Congress, http://de.scribd.com/doc/25018334/CRS-Report-International-Terrorism-and-Transnational-Crime-2010#page=12, accessed 25 October 2012

Schneider, S. (2002), *Predicting Crime: A Review of the Research, Summary Report*, Department of Justice, Canada, www.justice.gc.ca/eng/rp-pr/csj-sjc/jsp-sjp/rr02_7/rr02_7.pdf, accessed 15 January 2013

Shanty, F. (2008), *Organized crime: from trafficking to terrorism,* Vol. 1, ABC-Clio, Santa Barbara, CA.

SOCA (2010), *Suspicious Activity Reports Regime Annual Report 2010*, SOCA, UK

UNODC (2012), *Global congress tackles financial and Internet fraud*, www.unodc.org/newsletter/en/perspectives/no03/page011.html, accessed 25 October 2012

US Department of Justice. (n.d.), *Al Qaeda Training Manual*, www.au.af.mil/au/awc/awcgate/terrorism/alqaida_manual/manualpart1_1.pdf, accessed 2 February 2013

US Government (2011), *Strategy to Combat Transnational Organized crime, addressing threats converging to National Security*, July 2011, www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf, accessed 25 October 2012

US Treasury Department (2006), *The Use and Counterfeiting of United States Currency Abroad, Part 3*, www.federalreserve.gov/boarddocs/rptcongress/counterfeit/counterfeit2006.pdf, accessed 11 January 2013

USSS (2011), *United States Secret Service Fiscal Year 2011 Annual Report*, www.secretservice.gov/USSS_FY2011AR.pdf, accessed 11 January 2013

Wesley, A.J.L. (2007), *Disrupting Threat Finances: Utilization of Financial Information to Disrupt Terrorist Organizations in the Twenty-First Century*, School of Advanced Military Studies, Fort Leavensworth, www.investigativeproject.org/documents/testimony/342.pdf, accessed 25 October 2012

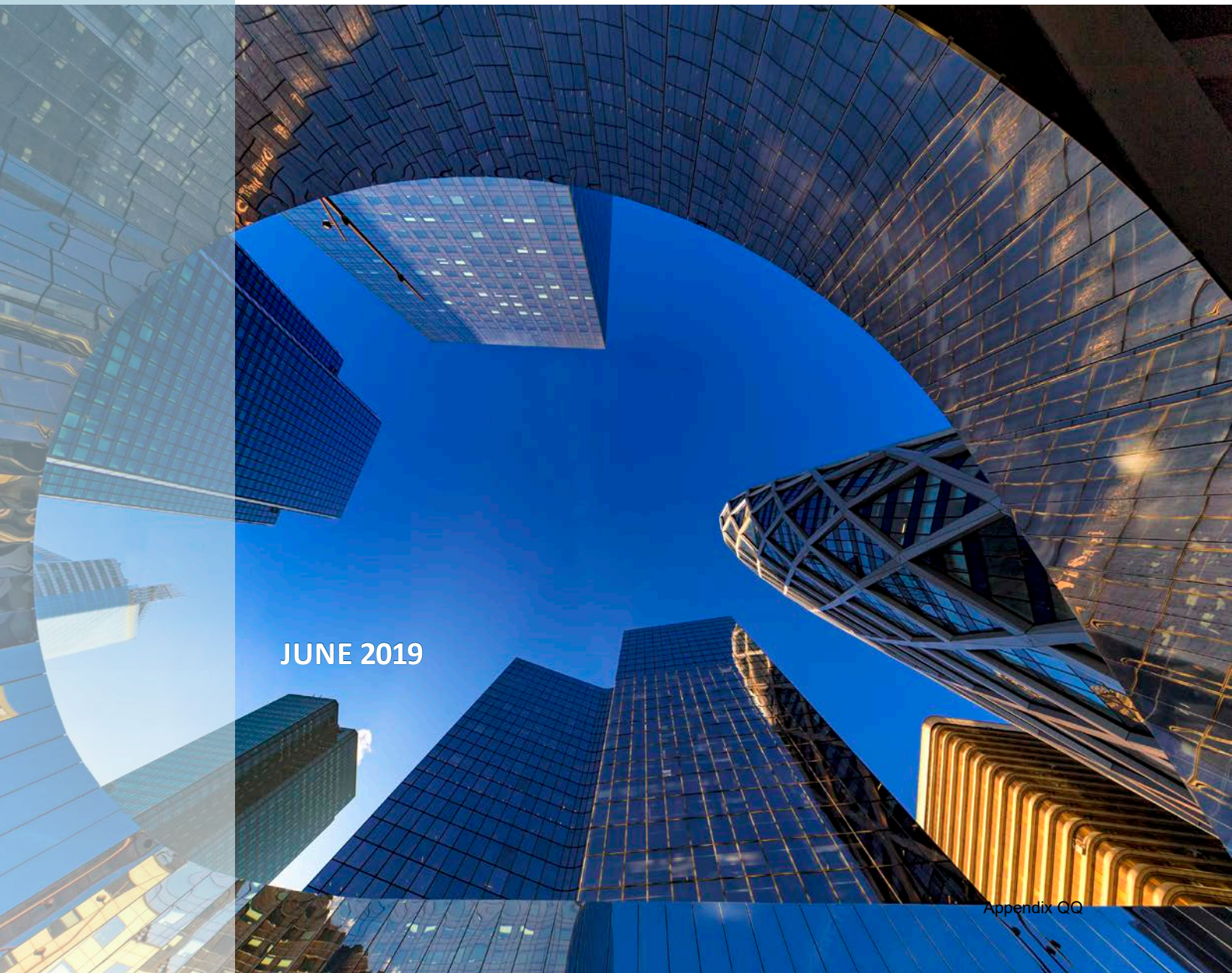
Wright, A. (2006*), Organised Crime,* Willan Publishing, Cullompton and Portland OR

Zhang, X. (2001), "The Emergence of "Black Society", *Forum on Crime and Society, Vol. 1, No.* 2, *pp*. 53-72, UN Centre for International Crime Prevention (Ed.), UN, New York, https://www.unodc.org/pdf/crime/publications/forum1vol2.pdf, accessed 11 January 2013

FATF

GUIDANCE FOR A RISK-BASED APPROACH

TRUST AND COMPANY SERVICE PROVIDERS



JUNE 2019

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2019), *Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs),* FATF, Paris, www.fatf-gafi.org/publications/documents/rba-trust-company-service-providers.html

TABLE OF CONTENT

Table of acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Client[1] due diligence
DNFBP	Designated non-financial businesses and professions
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
ML	Money laundering
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-based approach
SRB	Self-regulatory body
STR	Suspicious transaction report
TCSP	Trust and company service providers
TF	Terrorist financing

[1] In some jurisdictions or professions, the term "customer" is used, which has the same meaning as "client" for the purposes of this document

Executive Summary

1. The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. It means that supervisors, financial institutions, and trust and company service providers (TCSPs) identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed, and implement the most appropriate mitigation measures. This approach enables them to focus their resources where the risks are higher.

2. The FATF RBA Guidance aims to support the implementation of the RBA, taking into account national ML/TF risk assessments and AML/CFT legal and regulatory frameworks. It includes a general presentation of the RBA and provides specific guidance for the TCSP sector and for their supervisors. The Guidance was developed in partnership with the profession, to make sure it reflects expertise and good practices from within the industry.

3. The development of the ML/TF risk assessment is a key starting point for the application of the RBA. It should be commensurate with the nature, size and complexity of the business. The most commonly used risk criteria are country or geographic risk, client risk, service/transaction risk. The Guidance provides examples of risk factors under these risk categories.

4. The Guidance highlights that it is the responsibility of the senior management of TCSPs to foster and promote a culture of compliance as a core business value. They should ensure that TCSPs are committed to manage ML/TF risks when establishing or maintaining business relationships.

5. The Guidance highlights that TCSPs should design their policies and procedures so that the level of initial and ongoing client due diligence measures addresses the ML/TF risks they are exposed to. In this regard, the Guidance explains the obligations for TCSPs regarding identification and verification of beneficial ownership information and provides examples of standard, simplified and enhanced CDD measures based on ML/TF risk.

6. The Guidance has a section for supervisors of the TCSP sector and highlights the role of self-regulatory bodies (SRBs) in supervising and monitoring. It explains the risk-based approach to supervision as well as supervision of the risk-based approach by providing specific guidance on licensing or registration requirements for the TCSP sector, mechanisms for on-site and off-site supervision, enforcement, guidance, training and value of information-exchange between the public and private sector.

7. The Guidance also highlights the importance of supervision of beneficial ownership requirements and nominee arrangements. It underscores how supervisory frameworks can help ascertain whether accurate and up-to-date beneficial ownership information on legal persons and legal arrangements is maintained by TCSPs and made available in a timely manner to competent authorities when required.

Section I- Introduction and Key Concepts

This Guidance should be read in conjunction with the following, which are available on the FATF website: www.fatf-gafi.org:

a) The FATF Recommendations, especially Recommendations 1, 10, 11, 12, 17, 19, 20, 21, 22, 23, 24, 25 and 28 and their Interpretive Notes (INR), and the Glossary.

b) Other relevant FATF Guidance documents such as:

- The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)
- FATF Guidance on the Risk-Based Approach for Accountants
- FATF Guidance on the Risk-Based Approach for Legal Professionals
- FATF Guidance on Transparency and Beneficial Ownership (October 2014)

c) Other relevant FATF Reports such as:

- Money Laundering Using Trust and Company Service Providers (October 2010)
- The Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018)

Background and context

8. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism* and *Proliferation*, which were adopted in 2012[2]. The FATF has reviewed its 2009 RBA Guidance for trust and company service providers (TCSPs), in order to bring it in line with the new FATF requirements[3] and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version applies to the TCSP sector[4] as well as, accountant and legal professionals who provide TCSP services, and financial institutions who are engaged in TCSP activity (e.g. through subsidiaries that conduct TCSP activity).

9. Reference in this Guidance to TCSPs refers to trust and company service providers acting in the course of a business.

10. The RBA Guidance for the TCSP sector was drafted by a project group comprising FATF members, FATF observer member - the Group of International Finance Centre Supervisors and representatives of the private sector. The project group was co-led by the UK, the United States, the Institute of Chartered Accountants in England and Wales, the International Bar Association and the Society of Trust and Estate Practitioners. Membership of the project group is set out in Annex 4.

2 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

3 These services are included in the FATF Glossary under "Designated non-financial businesses and professions at (f)

4 Including both legal and natural persons, see definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary

11. The FATF adopted this updated RBA Guidance for TCSP at its June 2019 Plenary.

Purpose of the Guidance

12. The purpose of this Guidance is to:

a) Support a common understanding of a RBA for TCSPs, financial institutions and designated non-financial businesses and professions (DNFBPs)[5] that maintain relationships with TCSPs, competent authorities and self-regulatory bodies (SRBs)[6] responsible for monitoring the compliance of TCSPs with their AML/CFT obligations;

b) Assist countries, competent authorities and TCSPs in the design and implementation of a RBA to AML/CFT by providing guidelines and examples of current practice, with a particular focus on providing advice to small firms;

c) Recognise the difference in the RBA for different TCSPs who are establishing trusts, companies or other legal entities for the benefit of clients or who are acting as trustees or directors (or providing persons to act as trustees or directors) of such trusts, companies or other legal entities as against TCSPs who are providing more limited services (e.g. registered office services);

d) Outline the key elements involved in applying a RBA to AML/CFT related to TCSPs;

e) Assist financial institutions and DNFBPs that have TCSPs as customers in their role as directors or trustees of a legal person or legal arrangement customer of the financial institution or DNFBP, in identifying, assessing and managing the ML/TF risk associated with TCSPs and their services;

f) Assist countries, competent authorities and SRBs in the implementation of the FATF Recommendations with respect to TCSPs, particularly Recommendations 22, 23 and 28;

g) Assist countries, SRBs and the private sector to meet the requirements expected of them, particularly under IO.3 and IO.4;

h) Support the effective implementation of action plans of NRAs conducted by countries; and

i) Support the effective implementation and supervision by countries of national AML/CFT measures, by focusing on risks as well as preventive and mitigating measures.

Target audience, status and content of the Guidance

13. This Guidance is aimed at the following audience:

a) Practitioners in the TCSP sector;

---

5 See definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary

6 See definition of the term 'Self-regulatory body' in the FATF Glossary

b) Countries and their competent authorities, including AML/CFT supervisors of TCSPs, SRBs, AML/CFT supervisors of banks and other financial institutions that have TCSPs as customers, and Financial Intelligence Units (FIU); and

c) Practitioners in the banking sector and other financial services sectors and DNFBPs that have TCSPs as customers.

14. The Guidance consists of four sections. Section I sets out introduction and the key concepts. Section II contains key elements of the RBA and should be read in conjunction with specific Guidance to TCSPs (Section III) and guidance to supervisors of TCSPs on the effective implementation of a RBA (Section IV). There are four annexes:

a) Beneficial ownership information in relation to a company, trust or other legal arrangements to whom a TCSP provides services (Annex 1);

b) Glossary of Terminology (Annex 2);

c) Supervisory practices for implementation of the RBA (Annex 3); and

d) Members of the RBA Drafting Group (Annex 4).

15. This Guidance recognises that an effective RBA will take account of the national context, consider the legal and regulatory approach and relevant sector guidance in each country, and reflect the nature, diversity, maturity and risk profile of a country's TCSP sector and the risk profile of individual TCSPs operating in the sector. The Guidance sets out different elements that countries and TCSPs could consider when designing and implementing an effective RBA.

16. This Guidance is non-binding and does not overrule the purview of national authorities[7], including on their local assessment and categorisation of the TCSP sector based on the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector to assist competent authorities and TCSPs to implement applicable FATF Recommendations effectively. National authorities may take this Guidance into account while drawing up their own Guidance for the sector. DNFBPs should also refer to relevant legislation and sector guidance for the country in which a TCSP customer is based.

Scope of the Guidance: terminology, key features and business models

Terminology

17. Under the FATF definition, Trust and Company Service Providers refers to all persons[8] or businesses that are not covered elsewhere under the Recommendations, and which as a business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons;

7 National authorities should however take the Guidance into account when carrying out their supervisory functions.

8 Including both legal and natural persons, see definition for Designated Non-Financial Businesses and Professions in the FATF Glossary

- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

18. The FATF definition of TCSP relates to providers of trust and company services that are not covered elsewhere by the FATF Recommendations, and therefore excludes financial institutions, lawyers, notaries, other independent legal professionals and accountants. Separate guidance has been issued for those sectors, and they should therefore apply that guidance when providing services covered by R.22. However, all those professions/entities engaged in TCSP activities should also refer to the TCSPs guidance, as it is more specifically tailored to TCSP services.

Key features

19. TCSPs can take different forms. In some countries, they may be predominantly legal professionals and accountants. In other countries – particularly in countries with a high concentration of non-resident business – TCSPs are independent trust companies which may be owned and operated by their directors/senior managers, or trust companies that are subsidiaries of financial institutions and DNFBPs. In some cases, these may form part of international non-bank financial groups which provide TCSP services from more than one jurisdiction, or who may be other professionals. In other countries, trust service providers (e.g. trust companies) and company service providers are separate and distinct categories of entities subject to separate regulatory requirements. As a result, not all persons and businesses active in the TCSP industries provide all of the services listed in the definition of a TCSP. Accordingly, risk should be identified and managed on a service-by-service basis.

20. The roles and therefore risks of the different DNFBP constituents, including TCSPs frequently differ. However, in some areas, there are inter-relationships between different DNFBP sectors, and between the DNFBPs and financial institutions. For example, in addition to specialised trust and company service providers, financial institutions, legal professionals, and accountants may also undertake the trust and company services covered by the FATF Recommendations.

Activities carried out by TCSPs

21. TCSPs provide a range of services and activities that differ vastly, e.g. in their methods of delivery, in the depth and duration of the relationships formed with customers, and the size of the operation. For example, some of these entities are single person operations. This Guidance is intended for all TCSPs and sets out a risk-based approach to ensure compliance with FATF's Recommendations.

Vulnerabilities of TCSP services

22. Criminals may seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and often trusts and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies[9], which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy. Criminals may also seek to misuse shelf companies[10] formed by TCSPs by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be in an attempt to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

23. Many aspects of this guidance on applying a RBA to AML/CFT may also apply in the context of predicate offences, particularly for other financial crimes such as tax crimes. The ability to apply the RBA effectively to relevant predicate offences will also reinforce the AML/CFT obligations. TCSPs may also have specific obligations in respect of identifying risks of predicate offences such as tax crimes, and supervisors may have a role to play in oversight and enforcement against those crimes. Therefore, in addition to this guidance, TCSPs and supervisors should have regard to other sources of guidance that may be relevant in managing the risks of predicate offences.

FATF Recommendations applicable to TCSPs

24. The basic intent behind the FATF Recommendations as it relates to TCSPs is to ensure that their operations and services are not abused for facilitating criminal activities and ML/TF. The requirements of R.22 regarding CDD, record-keeping, PEPs, new technologies and reliance on third parties set out in R.10, 11, 12, 15 and 17 should apply to TCSPs in certain circumstances.

25. R.22 applies to TCSPs when they prepare for or carry out transactions for a client concerning the activities set out in paragraph 17 above.

26. R.23 requires that R.18, 19, 20 and 21 should apply to TCSPs when on behalf of or for a client, they engage in a transaction in relation to the activities described to in R.22 above. These Recommendations relate to internal AML/CFT controls, measures to be taken for countries that do not or insufficiently comply with the FATF Recommendations, reporting of suspicious activity and associated prohibitions on tipping off and confidentiality provisions. Section III provides further guidance on the application of R.22 and R.23 obligations to TCSPs.

---

9 A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.

10 A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established.

27. Countries should establish the most appropriate regulatory regime, tailored to address relevant ML/TF risks, which takes into consideration the activities and applicable code of conduct for TCSPs.

Section II – The RBA to AML/CFT

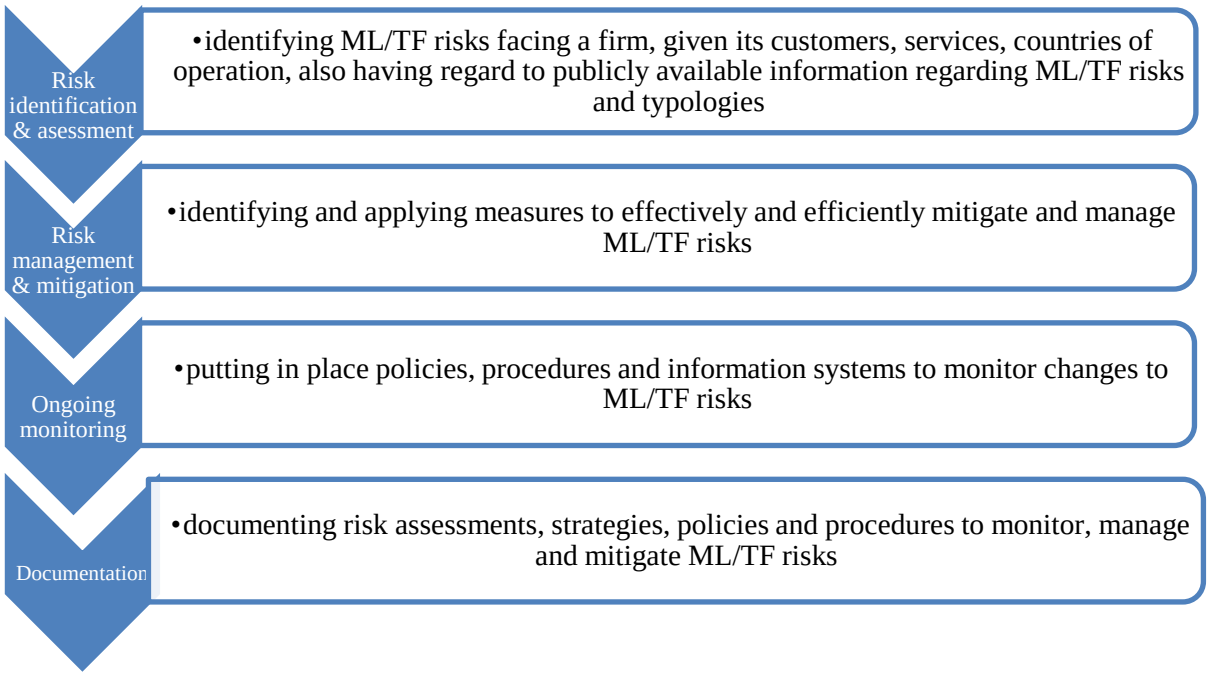
What is the risk-based approach?

28. The RBA to AML/CFT means that countries, competent authorities and DNFBPs, which include TCSPs should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures to effectively and efficiently mitigate and manage the risks.

29. For TCSPs, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, jurisdictions in which they operate and the effectiveness of actual and potential risk controls that are or can be put in place, will require the investment of resources and training. For supervisors, this will also require maintaining an understanding of the ML/TF risks specific to their area of supervision, and the degree to which AML/CFT measures can reasonably be expected to mitigate such risks.

30. The RBA is not a "zero failure" approach; there may be occasions where a TCSP has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks, but is still used for ML or TF purposes in isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that TCSPs must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

31. Key elements of a RBA can be summarised as follows:



The rationale for the RBA

32. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards. Its purposes remain to protect the integrity of the financial system by providing governments with updated tools needed to take action against financial crime.

33. There was an increased emphasis on the RBA to AML/CFT, especially in preventive measures and supervision. Though the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations considered the RBA to be an essential foundation of a country's AML/CFT framework.[11]

34. The RBA allows countries, within the framework of the FATF Standards, to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are commensurate with the nature of risks.

35. The application of a RBA is therefore essential for the effective implementation of the FATF Standards by countries and TCSPs.[12]

Application of the risk-based approach

36. The FATF Recommendations do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF. The overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of factors including services, products, customers, geography, preventive measures and the strength of an entity's compliance program.

37. R.1 sets out the scope of application of the RBA as follows:

a) Who should be subject to a country's AML/CFT regime? In addition to the sectors and activities already included in the scope of the FATF Recommendations[13], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.[14]

---

11 R.1.

12 The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take into account the risks and the flexibility allowed by the RBA, when determining whether there are deficiencies in a country's AML/CFT measures, and their importance *(FATF, 2013f).*

13 See Glossary, definitions of "Designated non-financial businesses and professions" and "Financial institutions".

14 See INR.1.

b) How should those subject to the AML/CFT regime be supervised or monitored for compliance with this regime? Supervisors should ensure that TCSPs are implementing their obligations under R.1. AML/CFT supervisors should consider a TCSP's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA.

c) How should those subject to the AML/CFT regime be required to comply? The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. TCSPs are required to apply each of the CDD measures under (a) to (d) below[15]: (a) identification and verification of the client's identity; (b) identification and taking reasonable measures to verify the identity of the beneficial owner and taking reasonable measures to verify the identity of beneficial owner; (c) understanding the purpose and nature of the business relationship; and (d) on-going due diligence on the relationship. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

d) Consideration of the engagement in client relationships: TCSPs are not obliged to avoid risk entirely. Even if the services they provide to their clients are considered vulnerable to the risks of ML/TF based on risk assessment, it does not mean that all TCSPs and all their clients or services pose a higher risk when taking account of the risk mitigating measures that have been put in place.

e) Importance of TCSPs to the overall economy: TCSPs often play significant roles in the legal and economic life of a country. The role of TCSPs in supporting the business registration process, finalising documentation for that and providing professional advice is vital. The risks associated with any type of client group is not static and the expectation is that within a client group, based on a variety of factors, individual clients could also be classified into risk categories, such as low, medium-low, medium high or high risk (see section III below for a detailed description). Measures to mitigate risk should be applied accordingly.

Challenges

38. Implementing a RBA can present a number of challenges for TCSPs in identifying what necessary measures they need to take. A RBA requires resources and expertise, both at a country and institutional level, to gather and interpret information on risks, to develop and maintain effective procedures and systems, and to train personnel. A RBA is also reliant on individuals exercising sound and well-trained judgement when designing and implementing procedures and systems. It will also lead to a diversity in practice, although this can result in innovative solutions to address areas of higher risk. On the other hand, TCSPs may be uncertain as to how to comply with the regulatory framework itself and the TCSP sector may find it difficult to apply a uniform approach.

[15] See R.10

39. TCSPs need to have a good understanding of the risks and should be able to exercise sound judgement. This requires the profession, and the individuals within it, to build expertise through experience and training. If a TCSP attempts to adopt a RBA without sufficient expertise or understanding and knowledge of the risks faced by the sector, they may make flawed judgements. TCSPs may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, and therefore deploy insufficient resources, thereby creating vulnerabilities.

40. TCSPs may find that some staff members are uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. It may also encourage a 'tick-box' approach to risk assessment.

41. Developing sound judgement is reliant on good information and intelligence sharing by designated competent authorities and SRBs. The existence of good practice guidance, training, industry studies and other available information and materials will also assist the TCSPs to make sound risk-based judgements. TCSPs must be able to access this information and guidance easily so that they have the best possible knowledge on which to base their judgements.

42. The services and products TCSPs provide to their clients vary and are not wholly of a financial nature. The FATF Recommendations apply equally to TCSPs when they are engaged in a specified activity, including obligations related to CDD, reporting of suspicious transactions and associated prohibitions on tipping-off, record-keeping, identification and risk management related to politically exposed persons or new technologies, and reliance on other third-party financial institutions and DNFBPs.

Box 1. Particular RBA Challenges for TCSPs

Culture of compliance and adequate resources. Implementing a RBA requires that TCSPs have a sound understanding of the risks and are able to exercise sound judgement. Above all, TCSP and their management should recognise the importance of a culture of compliance across the organisation and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of the organisation. This requires the building of expertise including for example, through training, recruitment, taking professional advice and 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making. The process will benefit from information sharing by relevant competent authorities and SRBs. The provision of good practice guidance by competent authorities and SRBs is also valuable.

S***ignificant variation in services and clients.*** TCSPs may vary substantially in the breadth and nature of services provided and the clients they serve, as well as the size, focus, ownership profile and sophistication of the firm and its employees. In implementing the RBA, TCSPs should make

reasonable judgements for their particular services and activities. This may mean that no two TCSPs are likely to adopt the same detailed practices.

Appropriate mitigation measures will also depend on the nature and risks arising from the service provider's role and involvement. Circumstances may vary considerably between providers who represent clients directly as trustees or directors controlling the affairs of the legal arrangement or legal person to those that are engaged for distinct purposes such as provision of registered office only services and who have to rely on information on the company's activities from external directors.

Transparency of beneficial ownership on legal persons and arrangements. TCSPs are involved in the formation, management, or administration of legal entities and arrangements, though in many countries any legal or natural person also may be able to conduct these activities. Where TCSPs do play this "gatekeeper" role, they may be challenged in obtaining and keeping current and accurate beneficial ownership information depending upon the nature and activities of their clientele. Other challenges may arise when on-boarding new clients with minimal economic activity associated with the legal entity and/or its owners, controlling persons, or beneficial owners, established in another jurisdiction. Finally, whether the source of beneficial ownership information is a public registry, another third party source, or the client, there is always potential risk in the correctness of the information, in particular where the underlying information has been self-reported. Those risks notwithstanding, the start point in determining beneficial ownership should almost always start with questions to the immediate client, having determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the client is a publicly listed company. The information provided by the client should then be appropriately confirmed by reference to public registers and other third party sources where possible. This may require further and clarifying questions to be put to the immediate client. The goal is to ensure that the TCSP is reasonably satisfied about the identity of the beneficial owner. For more practical guidance on beneficial ownership, refer to the guidance in Box 2.

Risk of criminality. TCSPs should be alert to ML/TF risks posed by the services they provide to avoid the possibility that they may commit or become an accessory to the commission of a substantive offence of ML/TF. TCSPs must protect themselves from misuse by criminals and terrorists. This includes the sources and methods used for providing payments for the TCSP's services, which may dictate greater focus on monitoring of clients and their funds for unusual or suspicious activity.

Allocating responsibility under a RBA

43. An effective risk-based regime builds on and reflects a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector and its risk profile. TCSPs should identify and assess their own ML/TF risk taking account of

the NRAs in line with R.1 as well as the national legal and regulatory framework, including any areas of prescribed significant risk and mitigation measures. TCSPs are required to take appropriate steps to identify and assess their ML/TF risks and have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.[16] Where ML/TF risks are higher, TCSPs should always apply enhanced due diligence, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g. varying the degree of enhanced ongoing monitoring).

44. Strategies adopted by TCSPs to mitigate ML/TF risks has to take account of the applicable national legal, regulatory and supervisory frameworks. When determining the extent to which TCSPs can decide how to mitigate risk, countries should consider the ability of the sector to effectively identify and manage ML/TF risks as well as the expertise and resources of their supervisors to adequately supervise how TCSPs manage ML/TF risks and take action to address any failures. Countries may also consider evidence from competent authorities on the level of compliance in the sector, and the sector's approach to dealing with ML/TF risk. Countries whose services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that TCSPs are not fully equipped to effectively identify and manage ML/TF risk. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until understanding and experience of the sector is strengthened.[17]

45. TCSPs should not be exempted from AML/CFT supervision even where their compliance controls are adequate. However, the RBA allows competent authorities to focus more supervisory resource on higher risk entities.

Identifying ML/TF risk

46. Access to accurate, timely and objective information on ML/TF risks is a prerequisite for an effective RBA. INR.1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, SRBs, financial institutions and TCSPs. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share important information on ML/TF risks and threats, or where access to information is restricted by censorship, it will be difficult for TCSPs to correctly identify ML/TF risk.

47. R.34 requires competent authorities, supervisors and SRBs to establish guidelines and provide feedback to financial institutions and DNFBPs. Such guidelines and feedback help institutions and businesses to identify the ML/TF risks and to adjust their risk mitigating programmes accordingly.

Assessing ML/TF risk

48. Assessing ML/TF risk requires countries, competent authorities, including supervisors, SRBs and TCSPs to determine how the ML/TF threats identified will affect them. They should analyse the information obtained to understand the likelihood of these risks occurring, and the impact that these would have, on the individual TCSP, the entire sector and on the national economy. As a starting step,

16 R.1 and INR.1.

17 This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or FSAP.

ML/TF risks are often classified as low, medium-low, medium, medium-high and high. Assessing ML/TF risk therefore goes beyond the mere gathering of quantitative and qualitative information, without its proper analysis; this information forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.[18]

49. Competent authorities, including supervisors and SRBs should employ skilled and trusted personnel, recruited through fit and proper tests, where appropriate. They should be technically equipped commensurate with the complexity of their responsibilities. TCSPs that are required to routinely conduct a high volume of enquiries when on-boarding clients, (e.g. because of the size and geographic footprint of the firm) may also consider engaging skilled and trusted personnel who are appropriately recruited and checked. Such TCSPs are also likely to consider using the various technological options (including artificial intelligence) and software programs that are now available to assist in this regard.

50. TCSPs should develop internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees. TCSPs should also develop an ongoing employee training programme. They should be trained commensurate with the complexity of their responsibilities.

Mitigating and managing ML/TF risk

51. The FATF Recommendations require that, when applying a RBA, DNFBPs, countries, competent authorities and supervisors decide on the most appropriate and effective way to mitigate and manage the ML/TF risks they have identified. They should take enhanced measures to manage and mitigate situations when the ML/TF risk is higher. In lower risk situations, less stringent measures may be applied.[19]

a) Countries may decide not to apply some of the FATF Recommendations requiring TCSPs to take certain actions, provided (i) there is a proven low risk of money laundering and terrorist financing, this occurs in strictly limited and justified circumstances and it relates to a particular type of TCSPs or (ii) a financial activity is carried out by a natural or legal person on an occasional or very limited basis such that there is a low risk of ML/TF, according to the exemptions of INR 1.6 are met.

b) Countries looking to apply simplified measures should conduct an assessment to ascertain the lower risk connected to the category of customers and clients or products targeted, establish the lower level of the risks involved, and define the extent and the intensity of the required AML/CFT measures, provided that the specific conditions required for one of the exemptions of INR 1.6 are met. Specific Recommendations set out in more detail how this general principle applies to particular requirements.[20]

18 FATF (2013a), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

19 Subject to the national legal framework providing for Simplified Due Diligence.

20 For example, R.22 on Customer Due Diligence.

Developing a common understanding of the RBA

52. The effectiveness of a RBA depends on a common understanding by competent authorities and TCSPs of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, TCSPs should deal with the risks they identify. Competent authorities should issue risk-based approach guidance to TCSPs on meeting their legal and regulatory AML/CFT obligations. Supporting ongoing and effective communication between competent authorities and the sector is essential.

53. Competent authorities should acknowledge that in a risk-based regime, not all TCSPs will adopt identical AML/CFT controls. On the other hand, TCSPs should understand that a RBA does not exempt them from applying effective AML/CFT controls with a RBA.

Section III – Guidance for TCSPs

Risk identification and assessment

54. TCSPs should take appropriate steps to identify and assess the risk firm-wide given their particular client base that they could be used for ML/TF. They should document those assessments, keep these assessments up-to-date and have appropriate mechanisms in place to provide risk assessment information to competent authorities and supervisors. The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations.

55. ML/TF risks can be organised into three categories: (a) country/geographic risk; (b) client risk, and (c) transaction/service and associated delivery channel risk. The risks and red flags listed in each category are not exhaustive but provide a starting point for TCSPs to use when designing their RBA.

56. TCSPs should also refer to their country's NRAs and risk assessments performed by the competent authorities and supervisors.

57. When assessing risk, TCSPs should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supra-national risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in TCSP services/sector, risk reports in other jurisdictions where the TCSP based in and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions.

58. TCSPs may well also draw references to FATF Guidance on indicators and risk factors. During the course of a client relationship, procedures for ongoing monitoring and review of the client's risk profiles are also important. Competent authorities should consider how they can best alert TCSPs to the findings of any national risk assessments, the supranational risk assessments and any other information which may be relevant to assess the risk level particular to a TCSP practice in the relevant country.

59. Due to the nature of services that a TCSP generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most TCSPs. The TCSP's knowledge of the client and its business will develop throughout the duration of a longer term and interactive professional relationship. However, although individual TCSPs are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of business relationship. TCSPs will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be low risk (e.g. one-off client relationship). TCSPs should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

60. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow TCSPs to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the TCSP's role and involvement. Circumstances may vary considerably between TCSPs who represent clients on a single transaction and those involved in a long term relationship.

61. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. A TCSP may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB or other credible sources (including a referring TCSP).

62. TCSPs may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling TCSPs, where required, to subject each client to reasonable and proportionate risk assessment.

63. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the TCSP and/or firm. These criteria, however, should be considered holistically and not in isolation. TCSPs, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

64. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller firms and sole practitioners, it is advisable to look at the services they offer (e.g. carrying out company management services may entail greater risk than other services).

65. Criminals deploy a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common mechanisms/techniques have been compiled by FATF in the previous studies, including the 2014 FATF Guidance on Transparency and Beneficial Ownership and the 2018 Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership. TCSPs may refer to the studies for more details on the use of obscuring techniques and relevant case studies.

66. A practical starting point for firms (especially smaller firms) and TCSPs (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

a) **Client acceptance and know your client policies:** identify the client (and its beneficial owners) and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of wealth of the client[21], its owners and the purpose and nature of the transaction.

[21] The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust), while the source of wealth describes the

b) **Engagement acceptance policies:** Understand the nature of the work. TCSPs should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where a TCSP does not have the requisite expertise, the TCSP should not undertake the work.

c) **Understand the commercial or personal rationale for the work:** TCSPs need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. TCSPs however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.

d) **Be attentive to red flag indicators:** exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. These cases would trigger reporting obligations. Documenting the thought process by having an action plan may be a viable option to assist in interpreting/assessing red flags/indicators of suspicion. Then consider what action, if any, needs to be taken.

e) The outcomes of the above action (i.e. the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures (including evidence of source of wealth or funds).

f) TCSPs should adequately document and record steps taken under a) to e).

Country/Geographic risk

67. The provision of services by a TCSP may be higher risk when features of such services are connected to a higher risk country, for example:

a) the origin, or current location of the source of funds in the trust, company or other legal entity;

b) the country of incorporation or establishment of the company or the trusts;

c) the location of the major operations or assets of the trust, company or other legal entity; and

d) the country in which any of the following is a citizen or tax resident: a settlor, beneficiary, protector or other natural person exercising effective control over the trust or any beneficial owner or natural person exercising effective control over the company or other legal entity.

---

activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). While these may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

68. There is no universally agreed definition of a higher risk country or geographic area but TCSPs should pay attention to:

a) Countries/areas identified by credible sources[22] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

b) Countries identified by credible sources as having significant levels of organised crime, corruption, or other criminal activity, including being a major source or a major transit country for illegal drugs, human trafficking and smuggling and illegal gambling.

c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations.

d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.

e) Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.

Client risk

69. In the examples given below, the client of TCSPs may be an individual who is a settlor or beneficiary of a trust, or beneficial owner of a company, or other legal entity that is, for example, trying to obscure the real beneficial owner or natural person exercising effective control of the trust, company or other legal entity. The client may also be a representative of a company's or other legal entity's senior management who are, for example, trying to obscure the ownership structure.

70. The key risk factors that TCSPs should consider are:

a) The TCSP's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.

b) The client include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients (Please refer to the FATF Guidance (2013) on politically-exposed persons for further guidance on how to identify PEPs).

[22] "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

c) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).

d) Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:

   i. Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee or corporate directors, legal persons or legal arrangements splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.

   ii. Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors without any apparent legal or legitimate tax, business, economic or other reason.

   iii. Use of trust structures for tax evasion or to obscure ownership in order to place assets out of reach to avoid future liabilities.

e) Unusual complexity in control or ownership structures without a clear explanation, where there are certain transactions, structures, geographical location, international activities or other factors are not consistent with the TCSP's understanding of the client's business or economic purpose behind the establishment or administration of the trust, company or other legal entity with respect to which the TCSPs are providing services.

f) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.

g) The offer by the person giving instructions to the TCSP to pay extraordinary fees for services, which would not ordinarily warrant such a premium.

h) The relationship between employee numbers/structure is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets compared to similar businesses)

i) Sudden activity from a previously dormant client without a clear explanation.

j) Clients that start or develop an enterprise with unexpected profile or abnormal business cycles or clients that enter into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.

k) Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.

l) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

m) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).

n) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected. Subsequent lack of contact, when this would normally be expected.

o) Inexplicable changes in ownership.

p) Activities of the trust, company or other legal entity are unclear or different from the stated purposes under trust deeds or internal regulations of the company or foundation.

q) The legal structure has been altered frequently and/or without adequate explanation (e.g. name changes, transfer of ownership, change of beneficiaries, change of trustee or protector, change of partners, change of directors or officers).

r) Management of any trustee, company or legal entity appears to be acting according to instructions of unknown or inappropriate person(s).

s) Unreasonable choice of TCSP without a clear explanation, given the size, location or specialisation of the TCSP.

t) Frequent or unexplained change of professional adviser(s) or members of management of the trustee, company or other legal entity.

u) The person giving instructions to the TCSP is reluctant to provide all the relevant information or the TCSP has reasonable grounds to suspect that the provided information is incorrect or insufficient.

v) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for TCSPs to perform a proper risk assessment.

w) Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.

x) Clients with previous convictions for crimes that generated proceeds, who instruct TCSPs (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.

y) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is a lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.

z) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership.

aa) Clients seeking to obtain residents rights or citizenship in the country of establishment of the TCSP in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.

Transaction/service and associated delivery channel risk

71. Services which may be provided by TCSPs and which (in some circumstances) risk being used to assist money launderers may include:

a) Use of pooled client accounts or safe custody of client money or assets or bearer shares, without justification.

b) Situations where advice on the setting up of legal persons or legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or other legal entities, or change of name/corporate seat or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.

c) In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting trustees of such a trust.

d) Services where TCSPs may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.

e) Services that are capable of concealing beneficial ownership from competent authorities.

f) Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants than is normal under the circumstances and in the experience of the TCSP.

g) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.

h) Transactions using unusual means of payment (e.g. precious metals or stones).

i) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

j) Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.

k) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

l) Power of Representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.

m) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations

and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.

n) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner), with no apparent legal, tax, business, economic or other legitimate reason.

o) Commercial, private, or real property transactions or services to be carried out by the trust, company or other legal entity with no apparent legitimate business, economic, tax, family governance, or legal reasons.

p) Products/services that have inherently provided more anonymity or confidentiality without a legitimate purpose.

q) Existence of suspicion of fraudulent transactions, or transactions that are improperly accounted for. These might include:

   i. Over or under invoicing of goods/services.

   ii. Multiple invoicing of the same goods/services.

   iii. Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading).

   iv. Multiple trading of goods/services.

r) Any attempt by the settlor, trustee, company or other legal entity to enter into any fraudulent transaction.

s) Any attempt by the settlor, trustee, company or other legal entity to enter into any arrangement to fraudulently evade tax in any relevant jurisdiction.

Variables that may impact on a RBA and risk

72. While all TCSPs should robust high standards of due diligence in order to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale and expertise amongst TCSPs, as well as the nature of the clients they serve. As a result, consideration should be given to these factors when creating a RBA that also complies with the existing obligations of TCSPs.

73. Consideration should also be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. In such cases, it may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client than it would be for a large firm having a diverse client base with different risk profiles. However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may be regarded by criminals as more of a target for money launderers than large law firms. TCSPs in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice, and

of all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following a RBA.

74. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular TCSP. This factor must always be considered in the context of the practice of TCSP. The RBA methodology of TCSP may thus take into account risk variables specific to a particular client or type of work. Consistent with the RBA and proportionality, the presence of one or more of these variables may cause a TCSP to conclude that either enhanced CDD and monitoring is warranted, or conversely that standard CDD and monitoring can be reduced, modified or simplified. When reducing, modifying or simplifying CDD, TCSPs should always adhere to the minimum requirements as set out in national legislation These variables may increase or decrease the perceived risk posed by a particular client or type of work and may include:

75. Examples of factors that may increase risk are:

a) Unexplained urgency of assistance required.

b) Unusual sophistication of structure, including complexity of control and governance arrangements and use of multiple TCSPs.

c) The irregularity or limited duration of the client relationship. One-off engagements for the establishment of complex trust, company or other arrangements involving legal entities without ongoing involvement may present higher risk.

76. Examples of factors that may decrease risk are:

a) Involvement of financial institutions or other DNFBPs or TCSPs which are regulated in their home jurisdiction and subject to appropriate AML/CFT regulation.

b) Role or oversight of a regulator or multiple regulators (e.g. regulating TCSPs, trustees or any other person exercising effective control).

c) The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact throughout the relationship may present less risk. In addition, a relationship may present less risk where, for example, the TCSP provides an integrated service, including acting as or providing trustees or directors of the trust, company or other legal entity and responsibility for preparation of accounts or maintaining the books and financial records of such trust, company or other legal entity.

d) Trusts, companies or other legal entities that are transparent and well-known in the public domain.

e) Listed entities and other business arrangements, such as pension trusts and employee benefit trusts and other trusts used for commercial purposes.

f) TCSP's familiarity with a particular country, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight.

Documentation of risk assessments

77. TCSPs must always understand their ML/TF risks (for clients, countries or geographic areas, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis and exercise due professional care and use compelling good judgement. However, competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.[23]

78. TCSPs may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time efficient yet comprehensive manner is important.

79. Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment, and dated. In assessing the risk profile of the client at this stage, reference must be made to the relevant targeted financial sanctions lists to confirm neither the client nor the beneficial owner is designated and included in any of them.

80. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties.

81. Where TCSPs are involved in longer term transactions, risk assessments should be undertaken at suitable intervals across the life of the transaction, to ensure no significant risk factors have changed in the intervening period (e.g. new parties to the transaction, new sources of funds etc.).

82. A final risk assessment should be undertaken before a transaction has completed, allowing time for any required suspicious activity report, where required and appropriate, to be filed and any authority to move or transfer assets to be obtained from law enforcement (in countries where this is applicable).

Risk mitigation

83. TCSPs should have policies, controls and procedures that enable them to effectively manage and mitigate the risks that they have identified (or that have been identified by the country). They should monitor the implementation of those controls and enhance or improve them if they find the controls to be weak or ineffective. The policies, controls and procedures should be approved by senior management and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and supervisors. Measures and controls may include:

a) General training on ML/TF methods and risks relevant to TCSPs.

b) Targeted training for increased awareness by the TCSPs providing specified activities to higher risk clients or to TCSPs undertaking higher risk work.

[23] Paragraph 8 of INR.1.

c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain, evidence and record source of wealth and beneficial ownership information if required.

d) Periodic review of the services offered by the TCSP, and the periodic evaluation of the AML/CFT framework applicable to the TCSP and the TCSP's own AML/CFT procedures, to determine whether the ML/TF risk has increased and adequate controls are in place to mitigate those increased risks.

e) Reviewing client relationships on a periodic basis to determine whether the ML/TF risk has increased.

Initial and ongoing CDD (R.10 and 22)

84. TCSPs should design CDD procedures to enable them to form a reasonable certainty that they know the true identity of the relevant beneficial owners of, or natural persons who actually exercise effective control over, the trust, company or other legal entity and, with an appropriate degree of confidence, know the true purpose behind the establishment or use of the trust, company or other legal entity. TCSPs' procedures should include procedures:

a) For identifying the client and verifying that client's identity using reliable, independent source documents, data or information.

b) For identifying the relevant beneficial owners and natural persons who actually exercise control as set out in Annex 1 and taking reasonable measures to verify the identity of such persons (i.e. on a risk-based approach). This is articulated in the following box:

Box 2. Beneficial ownership information obligations
(see R.10, R.22 and INR.10)

R.10 sets out the instances where TCSPs will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF, when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. TCSPs should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk. TCSPs should also have regard to the AML/CFT 2013 Methodology Criteria 10.5 and 10.8-10.12.

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. TCSPs can verify the identity of a client by, for example meeting the client in person and then verifying their identity through

the production of a passport/identity card and documentation confirming his/her address. TCSPs can further verify the identity of a client on the basis of documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the TCSP is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client, and may include conducting public searches as well as by seeking information directly from the client. TCSPs will likely need to obtain the following information for a client that is a legal entity:

a) the name of the company;
b) the company registration number;
c) the registered address and/ or principal place of business (if different);
d) the identity of shareholders and their percentage ownership;
e) names of the board of directors or senior individuals responsible for the company's operations; and
f) the law to which the company is subject and its constitution; and
g) the types of activities and transactions in which the company engages.

To verify the information listed above, TCSPs may use sources such as the following:

a) constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);
b) details from company registers; and
c) shareholder agreements or other agreements between shareholders concerning control of the legal person;
d) filed audited accounts.

TCSPs should adopt a RBA to verify beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to-date or to ask for additional documentation that confirms the beneficial ownership and company structure. The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires reasonable steps to be taken to identify the ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

c) Enabling the TCSP to understand and, as appropriate, obtain information on the purpose and intended purpose of the trust, company or other legal entity.

d) Conducting ongoing due diligence on the business relationship. Ongoing due diligence ensures that the documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of suspicious transaction reports (STRs) to the financial intelligence unit (FIU), or to

respond to requests for information from an FIU and the law enforcement agencies.

85. Where risks are higher, TCSPs should obtain information about the source of funds in the trust, company or other legal entity and source of wealth in relation to the settlor or beneficial owner.

86. TCSPs should design their policies and procedures so that the level of CDD addresses the risk of the trust, company or other legal entity with respect to which services are being provided by the TCSP being used for ML/TF. TCSPs should design a standard level of CDD for normal risk clients and a reduced or simplified CDD process for low risk clients. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply. Enhanced due diligence should be applied to those clients that the TCSP has assessed as high risk. These activities may be carried out in conjunction with the TCSP's normal acceptance procedures, and will take into account any specific jurisdictional requirements for CDD in relation to the trust, company or other legal entity and any trustee, settlor, protector, beneficial owner or other natural person exercising effecting control over the trust, company or other legal entity.

87. In the normal course of their work, TCSPs are likely to learn more about some aspects of the trust, company or other legal entity, and the trustee, settlor, protector, beneficial owners or other natural persons exercising effective control, than other advisors. This information is likely to help the TCSP dynamically assess the ML/TF risk.

88. Identification of, company or other legal entity, any trustee or of any settlor, beneficial owner or natural person exercising effective control should be periodically reviewed. This is to ensure that changes in ownership or control are properly recorded. This may be carried out in conjunction with any professional requirements for client continuation processes.

89. Public information sources may assist with this ongoing review. The procedures that need to be carried out can vary, in accordance with the nature and purpose for which the entity exists, and the extent to which the underlying ownership differs from apparent ownership by the use of nominee shareholders and complex structures.

90. The following box provides a non-exhaustive list of examples of standard, enhanced and simplified CDD:

Box 3. Examples of Standard/Simplified/Enhanced CDD measures (see also INR.10)

Standard CDD

- Identifying the client and verifying that client's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the TCSP is satisfied about the identity of beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required

- Understanding and obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the business and risk profile the client, including, where necessary, the source of wealth and funds

Simplified CDD

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

Enhanced CDD

- Obtaining additional information on the trustee, settlor, beneficial owner or natural person exercising effective control of the trust, company or other legal entity (as described in Annex 1) (e.g. occupation, overall wealth, information available through public databases, internet), and updating more regularly the identification data of such persons and sources which can be regarded as credible
- Obtaining information on the reasons for intended or performed transactions carried out by the trust, company or other legal entity administered by the TCSP
- Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the settlor (as described in Annex 1) and evidencing this through appropriate documentation obtained
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the TCSPs policies should enable it to disregard source documents, data or information which is perceived to be unreliable)
- Considering the source of funds or wealth involved in the transaction or business relationship to seek to ensure they do not constitute the proceeds of crime. This could include obtaining appropriate documentation concerning the source of wealth or funds
- Increasing the frequency and intensity of transaction monitoring
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination

- Where appropriate, requiring the first payment to be carried out through an account in the name of the trust, company or other legal entity with a bank subject to similar CDD standards
- Increasing awareness of higher risk clients and transactions, across all departments with a business relationship with the client, including the possibility of enhanced briefing of engagement teams responsible for the client
- Enhanced CDD may also include lowering the threshold of ownership (e.g. below 25%), to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.

Politically exposed persons (PEP) (R.12)

91. TCSPs should take reasonable measures to identify any trustee, settlor, beneficial owner or natural person exercising effective control (as further described in Annex 1) in relation to a trust, company or other legal persons whether they are a PEP or a family member or close associate of a PEP. If the client or beneficial owner is a PEP or a family member or close associate of a PEP, TCSPs should perform the following additional procedures:

a) obtain senior management approval for establishing (or continuing, for existing structures) such business relationships;

b) take reasonable measures to establish the source of wealth and source of funds in relation to the settlor, beneficiaries who receive distributions, or natural persons exercising effective control over a trust or beneficial owners or natural persons exercising effective control over a legal entity or other arrangement identified as PEPs (as described in Annex 1); and

c) conduct enhanced ongoing monitoring of the business relationship.

92. Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, whether the PEP has access to official funds, the PEP's home country, the type of work the PEP is instructing the TCSP to perform or carry out (i.e. the services that are being asked for), whether the PEP is domestically based or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

93. The nature of the risk should be considered in light of all relevant circumstances, such as:

a) The nature of the relationship between the client and the PEP. If the client is a trust, company or legal entity, even if the PEP is not a natural person exercising effective control or the PEP is merely a discretionary beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.

b) The nature of the client (e.g. where it is a public listed company or regulated entity which is subject to and regulated for a full range of AML/CFT requirements consistent with FATF recommendations, the fact that it is subject to reporting obligations will be a relevant factor, albeit this should not automatically qualify the client for simplified CDD).

c) The nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate consideration.

Ongoing monitoring of clients and specified activities (R.10 and 22)

94. TCSPs are not expected to scrutinise every transaction carried out by a trust, company or other legal entity to whom the TCSP provides services. Some services are provided only on a one-off basis, without a continuing relationship with the trust, company or other legal entity and without the TCSP having access to the books and records of the trust, company or other legal entity and/or bank records. However, many of the professional services provided by TCSPs enable them to identify suspicious activity or transactions carried out using trust, companies or other legal entities. For example, their direct knowledge of, and access, to the records and management processes and operations of such structures as well as through close working relationships with trustees, settlors, managers and beneficial owners may help TCSPs make a determination in this regard. The continued administration and management of the legal persons and arrangements (e.g. account reporting, asset disbursements and corporate filings) would also enable the relevant TCSPs to develop a better understanding of the activities of their clients.

95. TCSPs need to be alert for events or situations which are indicative of a reason to be suspicious of ML/TF, employing their professional experience and judgement in the formulation of suspicions where appropriate. An advantage in carrying out this function is the professional scepticism which is a defining characteristic of many professional TCSPs' functions and relationships.

96. Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that the trustees, settlors, beneficial owners and natural persons exercising effective control (as described in Annex 1) are aware of any changes in the client's identity and risk profile established on acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds and wealth where necessary, to judge consistency with expected behaviour based on CDD information. As discussed below, ongoing monitoring may also give rise to filing a STR.

97. The TCSP should also consider reviewing CDD on an engagement/assignment basis for each trust, company or other legal entity with respect to which the TCSP provides ongoing services. Well-known, reputable, long-standing trustees, settlors, beneficial owners or other natural persons exercising effective control (as described in Annex 1) may suddenly request a new type of service that is not in line with the previous relationship with the TCSP. Such an assignment may suggest a greater level of risk.

98. TCSPs should not conduct investigations into suspected ML/TF on their own but instead file a STR or if the behaviour is egregious they should contact the FIU, law enforcement or supervisors, as appropriate, for guidance. Within the scope of engagement, a TCSP should be mindful of the prohibition on "tipping off" the individual concerned where a suspicion has been formed. Carrying out additional investigations, which are not within the scope of the engagement should also be considered against the risk alerting a money launderer.

99. When deciding whether or not an activity or transaction is suspicious, TCSPs may need to make additional enquiries (within the normal scope of the assignment or business relationship) of the individual or entity concerned or their records – this could typically be done as part of the TCSP's CDD process. Normal commercial enquiries, being made to fulfil duties to the trust, company or other legal entity with respect to which the TCSP provides services, may assist in understanding an activity or transaction to determine whether or not it is suspicious.

Suspicious transaction reporting, tipping-off, internal controls and higher-risk countries (R.23)

100. R.23 sets out obligations for TCSPs on reporting and tipping-off, internal controls and higher-risk countries (R.20, R.21, R.18 and R.19)

Suspicious transaction reporting and tipping-off (R.20, 21 and 23)

101. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must always be made promptly. The requirement to file a STR is not subject to a risk-based approach, but must be made promptly whenever required in the country concerned.

102. TCSPs may be required to report suspicious activities, as well as specific suspicious transactions, and so may make reports on a number of scenarios including suspicious business structures or management profiles which have no legitimate economic rationale. As specified under INR.23, where TCSPs seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

103. However, a RBA is appropriate for identifying a suspicious activity or transaction, by directing additional resources at those areas a TCSP has identified as higher risk. The designated competent authorities or SRBs may provide information to TCSPs, which will be useful to them to inform their approach for identifying suspicious activity or transactions, as part of a RBA. A TCSP should also periodically assess the adequacy of its system for identifying and reporting suspicious activity or transactions.

104. TCSPs should review their existing CDD if they have a suspicion of ML/TF.

Internal controls and compliance (R.18 and 23)

105. In order for TCSPs to have an effective risk-based approach, the risk-based process must be embedded within the internal controls of the firm and they must be appropriate for the size and complexity of the firm.

Internal controls and governance

106. Strong leadership and engagement by senior management and the Board of Directors (or equivalent body) in AML/CFT is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adhere to the firm's policies, procedures and processes designed to limit and control risks.

107. The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being

offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:

a) designating an individual, or individuals, at management level responsible for managing AML/CFT compliance;

b) designing policies and procedures that focus resources on the firm's higher-risk, services, products, clients and geographic locations in which their clients/they operate. These policies and procedures should be implemented across the firm and include:

   - risk-based CDD policies, procedures and processes;
   - ensure that adequate controls are in place before new services are offered; and
   - adequate controls for accepting higher risk clients or providing higher risk services, such as management approval;

c) performing a regular review of the firm's policies and procedures to ensure that they remain fit for purpose;

d) performing a regular compliance review to check that staff are properly implementing the firm's policies and procedures;

e) providing senior management with a regular report of compliance initiatives, identify compliance deficiencies, corrective action taken, and STRs filed;

f) planning for changes in management, staff or firm structure so that there is compliance continuity;

g) focusing on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CFT compliance and providing for timely updates in response to changes in regulations;

h) enabling the timely identification of reportable transactions and ensuring accurate filing of required reports;

i) incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel;

j) providing for appropriate training to be given to all relevant staff;

k) having appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP or a person subject to applicable financial sanctions;

l) providing for adequate controls for higher risk clients and services, as necessary (e.g. additional due diligence, escalation to senior management or additional review and/or consultation);

m) providing increased focus on a TCSP's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse for ML/TF;

n) providing for periodic review of the risk assessment and management processes, taking into account the environment within which the TCSP operates and the services it provides; and

o) providing for an AML/CFT compliance function and review programme, as appropriate, given the scale of the organisation and the nature of the TCSP's practice.

108. TCSPs should review the firm-wide risk assessment that takes into account the size and nature of the practice; the existence of high-risk clients (if any); and the provision of high-risk services (if any). Once completed, the firm-wide risk assessment will assist the firm in designing its policies and procedures and in establishing the level of resources it will require to manage and mitigate the ML/TF risks.

109. TCSPs should consider using proven technology-driven solutions to minimise the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the needs of TCSPs as they continue to develop, this may be particularly important for smaller firms that may be less able to commit significant resources of time to these activities.

110. Depending on the size of the firm, the types of services provided, the risk profile of clients and the overall assessed ML/TF risk, it may be possible to simplify internal procedures. For example, for sole owner/proprietor firms, providing limited services to low risk clients, client acceptance may be reserved to the sole owners/proprietors taking into account their business and client knowledge and experience. The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms serving a diverse client base and providing multiple services across geographical locations, more sophisticated procedures are likely to be necessary.

Internal mechanisms to ensure compliance

111. The TCSP (at the senior management level) should monitor effectiveness of its internal controls. If the TCSP identifies any weaknesses in those internal controls, it should design improved procedures.

112. The most effective tool to monitor the internal controls is a regular independent compliance review. A member of staff that has a good working knowledge of the firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff are properly applying the firm's procedures.

113. If the compliance review identifies areas of weakness and makes recommendations on how to improve the policies and procedures, then senior management should monitor how the firm is acting on those recommendations.

114. The TCSP should consider its firm-wide risk assessment regularly and make sure that the policies and procedures continue to direct effort to those areas where risk of ML/TF is highest.

Vetting and recruitment

115. TCSPs should consider the skills, knowledge and experience of staff both before they are appointed to their role and on an ongoing basis. The level of assessment should be proportionate to their role in the firm and the ML/TF risks they may encounter. Assessment may include criminal records checking and other forms of pre-employment screening such as credit reference checks and background verification (as permitted under national legislation) for key staff positions.

Education, training and awareness

116. R.18 requires that TCSPs provide their staff with AML/CFT training. For TCSPs, and those in smaller firms in particular, such training may also assist with raising awareness of monitoring obligations. A TCSP's commitment to having appropriate controls in place relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant staff with at least general information on AML/CFT laws, regulations and internal policies.

117. Firms should provide targeted training for increased awareness by the TCSPs providing specified activities to higher-risk clients and to TCSPs undertaking higher-risk work. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Training should also be targeted towards the role that the individual performs in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties, or training regarding red flags for those undertaking client/transactional risk assessment.

118. In line with a RBA, particular attention should be given to risk factors or circumstances occurring in TCSP's own practice. In addition, competent authorities, SRBs and representative bodies should work with educational institutions to ensure that the relevant curricula address ML/TF risks. The same training should also be made available for students taking courses to train to become TCSPs.

119. TCSPs must periodically provide their employees with appropriate AML/CFT training. In ensuring compliance with this requirement, TCSPs may take account of any AML/CFT training included in entry requirements and continuing professional development requirements for their professional staff. They must also ensure appropriate training for any relevant staff without a professional qualification, at a level appropriate to the functions being undertaken by those staff, and the likelihood of their encountering suspicious activities.

120. The overall risk-based approach and the various methods available for training and education gives TCSPs flexibility regarding the frequency, delivery mechanisms and focus of such training. TCSPs should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

a) tailored to the relevant staff responsibility (e.g. client contact or administration);

b) at the appropriate level of detail (e.g. considering the nature of services provided by the TCSP);

c) at a frequency suitable to the risk level of the type of work undertaken by the TCSP; and

d) used to test to assess staff knowledge of the information provided.

Higher-risk countries (R.19 and 23)

121. Consistent with R.19, TCSPs should apply effective enhanced due diligence measures (also see paragraph 68), proportionate to the risks, to business relationships and transactions with clients from countries for which this is called for by the FATF.

Section IV – Guidance for supervisors

122. A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resource to areas of higher ML/TF risk. R.28 requires that TCSPs are subject to adequate AML/CFT regulation and supervision. While it is each country's responsibility to ensure there is an adequate national framework in place in relation to regulation and supervision of TCSPs, any relevant supervisors and SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.[24] The RBA to AML/CFT aims to develop prevention or mitigation measures which are commensurate with the ML/TF risks identified. This applies to the way supervisory authorities allocate their resources.

The risk-based approach to supervision

Supervisors and SRBs' role in supervision and monitoring

123. According to R.28, countries must ensure that DNFBPs are subject to effective oversight through the supervision performed by a supervisor or by an appropriate SRB, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF.

124. A SRB is body representing a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), made up of member professionals, which has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and to practise in the profession. A SRB also performs supervisory or monitoring functions (e.g. to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession).

125. Supervisors and SRBs should have adequate powers to perform their supervisory functions (including powers to monitor and to impose effective, proportionate and dissuasive sanctions), and adequate financial, human and technical resources. They should determine the frequency and intensity of their supervisory or monitoring actions on TCSPs on the basis of their understanding of the ML/TF risks, and taking into consideration the characteristics of the TCSPs, in particular their diversity and number.

126. Countries should ensure that supervisors and SRBs are equipped in identifying and sanctioning non-compliance by its members. Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

127. Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives pertaining to the SRB's role in representing their members, while also being obligated to supervise them. If a SRB contains members of the supervised population, or represents those people, the relevant person should not continue to take part in the monitoring/ supervision of their practice/firm to avoid conflicts of interest.

[24] See INR 28.1.

128. Supervisors and SRBs should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas.

Understanding ML/TF risk- the role of countries

129. Countries should ensure, to the extent the national framework allows, that TCSPs apply a RBA that reflects the nature, diversity and maturity of the sector and its risk profile as well the ML/TF risks associated with individual TCSPs.

130. Access to information about ML/TF risks is essential for an effective RBA. Countries are required to take appropriate steps to identify and assess ML/TF risks on an ongoing basis in order to (a) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (b) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (c) make information available for AML/CFT risk assessments conducted by TCSPs and the jurisdiction's national risk assessment. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to competent authorities, SRBs and TCSPs. In situations where some TCSPs have limited capacity to identify ML/TF risks, countries should work with the sector to understand their risks.

131. Supervisors and SRBs should, as applicable, draw on a variety of sources to identify and assess ML/TF risks. These may include, but will not be limited to, the jurisdiction's national risk assessments, supranational risk assessments, domestic or international typologies, supervisory expertise and FIU feedback. The necessary information can also be obtained through appropriate information-sharing and collaboration among AML/CFT supervisors, when there are more than one for different sectors (legal professionals, accountants and TCSPs).

132. These sources can also be helpful in determining the extent to which TCSPs are able to effectively manage ML/TF risks. Information-sharing and collaboration should take place among AML/CFT supervisors across all sectors (legal professionals, accountants and TCSPs). Supervisors and SRBs should issue guidance to the TCSPs on issues of concern. Guidance should be frequently updated.

133. Competent authorities may also consider undertaking a targeted sectoral risk assessment to get a better understanding of the specific environment in which TCSPs operate in the country and the nature of services provided by them.

134. Supervisors and SRBs should understand the level of inherent risk including the nature and complexity of services provided by the TCSP. Supervisors and SRBs should also consider the type of services the TCSP is providing as well as its size and business model, corporate governance arrangements, the compliance culture within the organisation, financial and accounting information, delivery channels, client profiles, geographic location and countries of operation.

135. Supervisors and SRBs should also consider the controls TCSPs have in place (e.g. the quality of the risk management policy, the functioning of the internal oversight functions and the quality of oversight of any outsourcing and subcontracting arrangements). Supervisors and SRBs should require TCSPs to have group wide programmes against ML/TF, including for sharing of information within the group for AML/CFT purposes. Policies and procedures should be consistently applied and supervised across the group.

136. Supervisors and SRBs should seek to ensure their supervised populations are fully aware of, and compliant with, measures to identify and verify a client, the client's source of wealth and funds where required, along with measures designed to ensure transparency of beneficial ownership, as these are cross-cutting issues which affect several aspects of AML/CFT.

137. Supervisors and SRBs should review their assessment of TCSPs' ML/TF risk profiles periodically, including when circumstances change materially or relevant new threats emerge and appropriately communicate this assessment to the profession.

138. Supervisors and SRBs should ensure that they are properly assessing the risks associated with legal persons and legal arrangements. To further understand the vulnerabilities associated with beneficial ownership, with a particular focus on the involvement of professional intermediaries, supervisors should stay abreast of research papers and typologies published by international bodies.[25] Useful reference include the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

Mitigating and managing ML/TF risk

139. Supervisors and SRBs should take proportionate mitigating measures. Supervisors and SRBs should determine the frequency and intensity of these measures based on their understanding of the ML/TF risks. Supervisors and SRBs should consider the characteristics of the TCSPs, particularly his/her role as a professional intermediary, in particular their diversity and number. It is essential to have a clear understanding of the ML/TF risks: (a) present in the country; and (b) associated with the type of TCSP and their clients, products and services.

140. Supervisors and SRBs assessing the adequacy of the internal controls, policies and procedures should properly take account of the risk profile of TCSPs, and the degree of discretion allowed to them under the RBA.

141. Supervisors and SRBs should develop a means of identifying which TCSPs or group of TCSPs are at the greatest risk of being used by criminals. This involves considering the probability and impact of ML/TF risk. Probability means the likelihood of ML/TF taking place as a consequence of the activity undertaken by TCSPs, or a group of TCSPs, and the environment they operate in. The risk can also increase or decrease depending on other factors:

a) service and product risk (the likelihood that services or products can be used for ML/TF);

b) client risk (the likelihood that customers' funds may have criminal origins);

c) the nature of transactions (e.g. frequency, volume, counterparties);

d) geographical risk (whether the TCSP, its clients or other offices trade in riskier locations); and

e) other indicators of risk are based on a combination of objective factors and experience, such as the supervisor's wider work with the TCSP as well as

[25] Such as the FATF, the Organisation for Economic Co-operation and Development (OECD), the World Bank, the IMF and the United Nations Office on Drugs and Crime (UNODC).

information on its compliance history, complaints about the TCSP or about the quality of its internal controls. Other such factors may include information from government/law enforcement sources, whistle-blowers or negative news reports from credible media particularly those related to predicate offences for ML/TF or to financial crimes.

142. In adopting a RBA to supervision, supervisors may consider allocating supervised entities sharing similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of business, type of clients serviced and geographic areas of activities. The setting up of such groupings could allow supervisors to take a comprehensive view of the TCSP sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual firms. If the risk profile of a TCSP within a grouping changes, supervisors may reassess the supervisory approach, which may include removing the TCSP from the grouping.

143. Supervisors or SRBs should also consider the impact, i.e. the potential harm caused if ML/TF is facilitated by TCSPs or group of TCSPs. A small number of TCSPs may cause a high level of harm. This can depend on:

a) size (i.e. turnover), number and type of clients, number of premises, value of transactions etc.), and

b) links or involvement with other businesses (which could affect the susceptibility to being involved in 'layering' activity, e.g. concealing the origin of the transaction with the purpose to legalise the asset).

144. The risk assessment should be updated by supervisors and SRBs on an ongoing basis. The result from the assessment will help determine the resources the supervisor will allocate to the supervision of TCSPs or group of TCSPs.

145. Supervisors or SRBs should consider whether a TCSP meets the ongoing requirements for continued participation in the profession as well as assessments of competence and of fitness and propriety. This will include whether the TCSP meets expectations related to AML/CFT compliance. This will take place both when a supervised entity joins the profession, and on an ongoing basis thereafter.

146. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to differentiate between categories of TCSPs based on various factors such as their client base, countries they deal with and applicable AML/CFT controls etc.

147. Supervisors and SRBs should acknowledge that in a risk-based regime, not all TCSPs will adopt identical AML/CFT controls and that an isolated incident where the TCSP is part of an illegal transaction unwittingly does not necessarily invalidate the integrity of the TCSP's AML/CFT controls. At the same time, TCSPs should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

148. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to TCSPs to enable them to enhance their RBA.

Supervision of the RBA

Licensing or registration

149. R.28 requires TCSPs to be subject to regulatory and supervisory measures to ensure their compliance with AML/CFT requirements.

150. R.28 also requires the supervisor or SRB to take the necessary measures to prevent criminals or their associates from being professionally accredited or holding or being the beneficial owner of a significant or controlling interest or holding a management function in relation to a TCSP. This can be achieved through the evaluation of these persons through a "fit and proper" test.

151. A licensing or registration mechanism is one of the means to identify TCSPs who undertake activities specified in R.22 to whom the regulatory and supervisory measures, including the "fit and proper" test should be applied. It also enables the identification of the number of TCSPs for the purposes of assessing and understanding the ML/TF risks for the country, and the action which should be taken to mitigate them in accordance with R.1.

152. Licensing or registration provides a supervisor or SRB with the means to fulfil a "gate-keeper" role over who can undertake those activities specified in R.22. Licensing or registration should ensure that upon qualification, TCSPs are subject to AML/CFT compliance monitoring.

153. The supervisor or SRB should actively identify individuals and businesses who should be supervised by using intelligence from other competent authorities (e.g. FIUs, company registry, tax authority), information from financial institutions and DNFBPs, complaints by the public and open source information from advertisements and business and commercial registries or any other sources which indicate that there are unsupervised individuals or businesses providing the activities specified in R.22.

154. Licensing or registration frameworks should define the activities which are subject to licensing or registration, prohibit unlicensed or unregistered individuals or businesses providing these activities and set out measures for both refusing licences or registrations and for removing "bad actors".

155. The terms "licensing" or "registration" are not interchangeable. Licensing regimes generally tend to operate over financial institutions and impose mandatory minimum requirements based upon Core Principles on issues such as capital, governance, and resourcing to manage and mitigate prudential conduct as well as ML/TF risks on an on-going basis. Some jurisdictions have adopted similar licensing regimes for TCSPs, generally where TCSPs carry out trust and corporate services, to encompass aspects of prudential and conduct requirements in managing the higher level of ML/TF risks that have been identified in that sector.

156. A jurisdiction may have a registration framework over the entire DNFBP sector, including TCSPs or have a specific registration framework for each constituent of DNFBP. Generally, a supervisor or SRB carries out the registration function.

157. The supervisor or SRB should ensure that requirements for licensing or registration and the process for applying are clear, objective, publicly available and consistently applied. Determination of the licence or registration should be objective and timely. A SRB could be responsible for both supervision and for representing the interests of its members. If so, the SRB should ensure that registration decisions are

taken separately and independently from its activities regarding member representation.

Fit and proper tests

158. A fit and proper test provides a possible mechanism for a supervisor or SRB to take the necessary measures to prevent criminals or their associates from owning, controlling or holding a management function in a TCSP.

159. In accordance with R.28, the supervisor or SRB should establish the integrity of every beneficial owner, controller and individual holding a management function in a TCSP. However, the decisions on an individual's fitness and propriety may also be based upon a range of factors concerning the individual's competency, probity, and judgement as well as their integrity.

160. In some jurisdictions, a fit and proper test forms a fundamental part of determining whether to license or register the TCSP and whether on an ongoing basis the licensee or registrant (including its owners and controllers, where applicable) remains fit and proper to continue in that role. The initial assessment of an individual's fitness and propriety is a combination of obtaining information from the individual and corroborating elements of that information against independent credible sources to determine whether the individual is fit and proper to hold that position.

161. The process for determining fitness and propriety generally requires the applicant to complete a questionnaire. It could gather personal identification information, residential and employment history, and require disclosure by the applicant of any convictions or adverse judgements relating to the applicant, including pending prosecutions and convictions. Elements of this information should be corroborated to establish the bona fides of an individual. Such checks could include enquiries about the individual with law enforcement agencies and other supervisors or screening the individual against independent electronic search databases. The personal data collected should be kept confidential.

162. The supervisor or SRB should also ensure on an ongoing basis that those holding or being the beneficial owner of significant or controlling interest in and individuals holding management functions in a TCSP are fit and proper. A fit and proper test should apply to new owners, controllers and individuals holding a management function in a TCSP. The supervisor or SRB should consider re-assessing the fitness and propriety of these individuals arising from any supervisory findings, receipt of information from other competent authorities; or open source information indicating significant adverse developments.

Guarding against "brass-plate" operations

163. The supervisor or SRB should ensure that its licensing or registration requirements require the TCSP to have a meaningful physical presence in the jurisdiction. This usually means that the TCSP should have its place of business in the jurisdiction. Where the TCSP is a legal person, those individuals who form its mind and management should be actively involved in the business and may also be required to be resident in the jurisdiction (although this may not be a necessity provided that there is an appropriate person resident in the jurisdiction who has a responsibility to

report to the supervisor or SRB). A business with only staff who do not possess the professional qualifications and relevant experience to manage the TCSP should not be licensed or registered.

164. A supervisor or SRB should consider the ownership and control structure of the TCSP to determine that sufficient control over its operation will reside within the business, which it is considering licensing, or registering. Factors to take into account could include consideration of where the beneficial owners and controllers reside, the number and type of management functions the TCSP is proposing to have in the country, such as directors and managers, including compliance managers, and the calibre of the individuals who will be occupying those roles. It should also consider the extent to which the TCSP's activities are outsourced to another jurisdiction.

165. The supervisor or SRB should also consider whether the ownership and control structure of TCSPs unduly hinders its identification of the beneficial owners and controllers or presents obstacles to applying effective supervision.

Monitoring and supervision

166. Supervisors and SRBs should take measures to effectively monitor TCSPs through on-site and off-site supervision. The nature of this monitoring will depend on the risk profiles prepared by the supervisor or SRB and the connected RBA. Supervisors and SRBs may choose to adjust:

a) the level of checks required to perform their licensing/registration function: where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited, and approvals may be made on a review of basic documentation. Where the ML/TF risk associated with the sector is high, supervisors and SRBs may ask for additional information.

b) the type of on-site or off-site AML/CFT supervision: supervisors and SRBs may determine the correct mix of on-site and off-site supervision of TCSPs. Off-site supervision may involve analysis of annual independent audits and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identification of persons responsible for the filing. It may also include undertaking thematic reviews of the sector, making compulsory the periodic information returns from firms. Off-site supervision alone may not be appropriate in higher risk situations. On-site inspections may involve reviewing AML/CFT internal policies, controls and procedures, interviewing members of senior management, compliance officer and other relevant staff, considering gatekeeper's own risk assessments, spot checking CDD documents and supporting evidence, looking at reporting of ML/TF suspicions in relation to clients, and others matters, which may be observed in the course of an onsite visit and where appropriate, sample testing of reporting obligations.

c) the frequency and nature of ongoing AML/CFT supervision: supervisors and SRBs should proactively adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT

supervision as issues emerge (e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from TCSPs' inclusion in thematic review samples).

d) the intensity of AML/CFT supervision: supervisors and SRBs should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of TCSPs' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include; detailed testing of systems and files to verify the implementation and adequacy of the TCSPs' assessment, CDD, reporting and record-keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT assessment in particular lines of business.

167. Supervisors and SRBs should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to TCSPs to enable them to enhance their RBA.

168. Record keeping and quality assurance are important so that supervisors can document and test the reasons for significant decisions relating to AML/CFT supervision. Supervisors should have an appropriate information retention policy and be able to easily retrieve information while complying with the relevant data protection legislation. Record keeping is crucial and fundamental to the supervisors' work. Undertaking adequate quality assurance is also fundamental to the supervisory process to ensure decision-making/sanctioning is consistent across the supervised population.

Enforcement

169. R.28 requires supervisors or SRB to have adequate powers to perform their functions, including powers to monitor compliance by TCSPs. R.35 requires countries to have the power to impose sanctions, whether criminal, civil or administrative, on DNFBPs, to include TCSPs when providing the services outlined in R.22(e). Sanctions should be available for the directors and senior management of the firms when a TCSP fails to comply with requirements.

170. Competent authorities should use proportionate actions, including a range of supervisory interventions and corrective actions to ensure that any identified deficiencies are addressed in a timely manner. Sanctions may range from informal or written warning, reprimand and censure to punitive sanctions (including suspension or cancellation of registration or licence and criminal prosecutions where appropriate) for more egregious non-compliance, as identified weaknesses can have wider consequences. Generally, systemic breakdowns or significantly inadequate controls will result in more severe supervisory response.

171. Enforcement by supervisors and SRBs should be proportionate while having a deterrent effect. Supervisors and SRBs should have (or should delegate to those who have) sufficient resources to investigate and monitor non-compliance. Enforcement should aim to remove the benefits of non-compliance.

Guidance

172. Supervisors and SRBs should communicate their regulatory expectations. This could be done through a consultative process after meaningful engagement with relevant stakeholders. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Guidance issued to TCSPs should also discuss ML/TF risk within their sector and outline ML/TF indicators and methods of risk assessment to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways which are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction.

173. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the TCSP sector, which may cover operational issues, and be more detailed and explanatory in nature. Training events may also provide an effective means to ensure TCSPs are aware of and compliance with AML/CFT responsibilities. Where supervisors cooperate to produce combined guidance across sectors, supervisors should ensure this guidance adequately addresses the diversity of roles that come within the guidance's remit, and that such guidance provides practical direction to all its intended recipients. The private sector guidance should be consistent with national legislation and with any guidelines issued by competent authorities with regard to TCSPs and be consistent with all other legal requirements and obligations.

174. Supervisors should consider communicating with other relevant domestic supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities across sectors (such as legal professionals, accountants and TCSPs). Multiple guidance should not create opportunities for regulatory arbitrage. Relevant supervisory authorities should consider preparing joint guidance in consultation with the relevant sectors, while recognising that in many jurisdictions TCSPs will consider that separate guidance targeted at TCSPs will be the most appropriate form.

175. Information and guidance should be provided by supervisors in an up-to-date and accessible format. It could include sectoral guidance material, findings of thematic reviews, training events, newsletters, internet-based material, oral updates on supervisory visits, meetings and annual reports.

176. An SRB should ensure that advice given by the representative side of the organisation correlates to the rules and guidance set by the supervisory side.

Training

177. Training is important for their supervision staff to understand the TCSP sector and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of a TCSP´s ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of AML/CFT policies, procedures and internal controls. It is recommended that the training has a practical basis/dimension.

178. Training should allow supervisory staff to form sound judgments about the quality of the risk assessments made by TCSPs and the adequacy and proportionality of a TCPS´s AML/CFT controls. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Endorsements

179. Supervisors should avoid mandating the use AML systems, tools or software of any third party commercial providers of to avoid conflicts of interest in the effective supervision of firms.

Information exchange

180. Information exchange between the public and private sector and within private sector (e.g. between financial institutions and TCSPs) is important to combat ML/TF. Information sharing and intelligence sharing arrangements between supervisors and public authorities (such as Financial Intelligence Units and law enforcement) should be robust, secure and subject to compliance with national legal requirements.

181. The type of information that could be shared between the public and private sectors include:

a) ML/TF risk assessments;

b) typologies (i.e. case studies) of how money launderers or terrorist financers have misused TCSPs or trusts, companies or other legal entities or arrangements managed by TCSPs;

c) feedback on STRs and other relevant reports;

d) targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with TCSP's as a class or individually; and

e) countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by R.6.

182. Domestic co-operation and information exchange between FIU and supervisors of the TCSP sector and among competent authorities including law enforcement, intelligence, FIU, tax authorities, and TSCP's supervisors is also important for effective monitoring/supervision of the sector. Such co-operation and co-ordination may help avoid gaps and overlaps in supervision and ensure sharing of good practices and findings. Such intelligence should also inform a supervisor's risk-based approach to supervisory assurance. Intelligence about active misconduct investigations and completed cases between supervisors and law enforcement agencies should also be encouraged. When sharing information, protocols and safeguards should be implemented in order to protect sensitive data.

183. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the TCSP sector, taking account of the multi-jurisdictional reach of many TCSP providers.

Supervision of beneficial ownership requirements and source of funds/wealth requirements

184. TCSPs fulfil a key gatekeeper role to the wider financial community through the activities they undertake in the formation of legal persons and legal arrangements and where they are involved in the management and administration of legal persons and legal arrangements.

185. As DNFBPs, they are required to apply CDD measures to beneficial owners of legal persons and legal arrangements to whom they are providing advice or formation services. In a number of countries a TCSP may be required as part of the process of registering the legal person and will be responsible for providing basic and/or beneficial ownership information to the registry.

186. In their capacity as company directors, trustees, nominees or foundation officials etc. of these legal persons and legal arrangements, TCSPs often represent these legal persons and legal arrangements in their dealings with other financial institutions and DNFBPs that are providing for example banking or audit services to these types of customer.

187. These financial institutions and other DNFBPs may request the CDD information collected and maintained by TCSPs, who because of their role as director, nominee or trustee, will act as the principal point of contact with the legal person or legal arrangement. These financial institutions and other DNFBPs may never meet the beneficial owner/s of the legal person or legal arrangement.

188. Under R.28, countries should ensure that TCSPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which includes identifying the beneficial owner/s and taking reasonable measures to verify them. Additionally R.24 and R.25 regarding transparency of beneficial ownership of legal persons and legal arrangements, require countries to have mechanisms for ensuring that adequate, accurate and up to date information is available on a timely basis on these legal entities. The FATF and Egmont Group also published the Report on Concealment of Beneficial Ownership in July 2018 which identified issues to help address the vulnerabilities associated with the concealment of beneficial ownership.

189. R.24 and R.25 also require countries to have mechanisms to ensure that information provided to registries is accurate and updated on a timely basis and that beneficial ownership information is accurate and current. To determine the adequacy of a system for monitoring and ensuring compliance, countries should have regard to the risk of AML/CFT in given businesses (i.e. if there is a proven higher risk then higher monitoring measures should be taken). TCSPs must, however, be cautious in blindly relying on the information contained in registries. In addition it is important for there to be some form of ongoing monitoring during a relationship to detect unusual and potentially suspicious transactions as a result of a change in beneficial ownership as registries are unlikely to provide such information on a dynamic basis.

190. In accordance with R.28, TCSPs should be subject to risk-based supervision by a supervisor or SRB covering the beneficial ownership and record-keeping requirements of R.10 and R.11. The Supervisor or SRB should have a supervisory framework which can help in ascertaining that accurate and current basic and

beneficial ownership information on legal person and legal arrangements is maintained and will be available on a timely basis to competent authorities.

191. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which TCSPs have established to identify and record the beneficial owner. In addition, they should undertake sample testing of client files on a representative basis to gauge the effectiveness of the application of those measures and the accessibility of accurate beneficial ownership information.

192. As part of the onsite and offsite inspection, supervisors or SRBs should examine the policies, procedures and controls that are in place for on-boarding of new clients to establish what information and documentation is required where the client is a natural person or legal person or trust or other similar legal arrangements. Supervisors or SRBs should verify the adequacy of these procedures and controls to identify beneficial owners in order to understand the ownership and control structure of these legal person or trust or other similar arrangements and to ascertain the business activity.

193. Sample testing of client files will also assist the supervisor or SRB in determining whether controls are effective for the accurate identification of beneficial ownership, accurate disclosure of that information to relevant parties and for establishing if that information is readily available. The extent of testing will be dependent on risk but the files selected should reflect the profile of the client base and include both new and existing clients.

194. Supervisors or SRBs should also consider the measures the TCSP has put in place for monitoring changes in the beneficial ownership of legal person or trust or other similar arrangements to whom they provide services or act to ensure that beneficial ownership information is accurate and current and to determine how timely updated filings are made, where relevant to a registry.

195. During examinations, supervisors or SRBs should consider whether to verify the beneficial ownership information available on the files of the TCSP with that held by the relevant registry, if any.

196. Supervisors or SRBs may also take into account information from other competent authorities such as FIUs public reports and information from other financial institutions or DNFBPs, to verify the efficacy of the TCSP's controls.

197. TCSPs should be subject to risk-based supervision by a supervisor or SRB covering the requirements to identify and evidence the source of funds and source of wealth for higher risk clients to whom they provide services. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current information on sources of funds and wealth is properly evidenced and available on a timely basis to competent authorities. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which TCSPs have established to identify and record sources of wealth in arrangements.

Nominee arrangements

198. A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the beneficial owner. A nominee

shareholder is a natural or legal person who is officially recorded in the Register of Members (shareholders) of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held on trust or through a custodial agreement. This nominee relationship should be disclosed to the company and to any relevant registry.

199. In a number of countries, TCSPs act or arrange for other persons (either individuals or corporate) to act as directors and act or arrange for other persons (either individuals or corporate) to act as a nominee shareholder for another person as part of their professional services. In accordance with R.24, these TCSPs should be subject to licensing/registration and supervision, and where acting as nominee shareholder, their status disclosed.

200. There will be legitimate reasons for a TCSP to act as or provide directors to a legal person or act or provide nominee shareholders. It should be apparent from the records of the legal person that it is the TCSP fulfilling these roles as the identity of the TCSP, or that of its members of staff will be disclosed on the register of directors, register of members for example.

201. There are legitimate reasons for a company to have a nominee shareholder including for the settlement and safekeeping of shares in listed companies where post traded specialists act as nominee shareholders. Company law may impose requirement for a legal person to have more than one member, which may also give rise to nominee arrangements. However, these nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner/s of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of, or from whom, they will take instructions or whom they represent. They are sometimes referred to as “strawmen”.

202. Nominee directors and nominees shareholders can create obstacles to identifying the true beneficial owner/s of a legal person, particularly where their status is not disclosed. This is because it will be the identity of the nominee, which is disclosed in the corporate records of the legal person held by a registry and in the company records at its registered office. Company law in a number of countries does not recognise the status of a nominee director because in law it is the directors of the company who are liable for its activities and the directors have a duty to act in the best interest of the company.

203. Supervisors and SRBs should be alert to the possibility that undisclosed nominee arrangements may exist. They should consider as part of their onsite and offsite inspections and examination of the policies, procedures and controls and client records of the TCSP whether undisclosed nominee arrangements would be identified and addressed as part of the CDD process and ongoing monitoring by the TCSP.

204. An undisclosed nominee arrangement may exists where there are the following (non-exhaustive) indicators:

a) the profile of a trustee, director or shareholder is inconsistent with the activities of the trust, company or other legal entity;

b) the individual holds a number of appointments to unconnected trusts, companies or other legal entities;

c) a nominee's source of wealth is inconsistent with the value and nature of the assets within the trust, company or other legal entities;

d) funds into and out of the trust, company or other legal entity are sent to or received from unidentified third party/ies;

e) the TCSP is accustomed to acting on the instructions of another person who is not the trustee or director or other natural person exercising effective control; and

f) Requests or instructions are subject to little or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the trustee, director/s or other natural person exercising effective control.

Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom a TCSP provides services

1. Taking a RBA, the amount of information that should be obtained by the TCSP will depend on whether the TCSP is establishing or administering the trust, company or other legal entity or is acting as or providing a trustee or director of the trust, company or other legal entity. In these cases, a TCSP will be required to understand the general purpose behind the structure and the source of funds in the structure in addition to being able to identify the beneficial owners and controlling persons. A TCSP which is providing other services (e.g. acting as registered office) to the trust, company or other legal entity will, taking a risk based approach, be required to obtain sufficient information to enable it to be able to identify the beneficial owners and controlling persons of the trust, company or other legal entity.

2. A TCSP that is not acting as trustee may, in appropriate circumstances, rely on a synopsis prepared by another TCSP, a legal professional or accountant providing services to the trust or relevant extracts from the trust deed itself to enable the TCSP to identify who is the settlor, trustees, protector (if any), beneficiaries or natural persons exercising effective control. This is in addition to the requirement, where appropriate, to obtain evidence to verify the identity of such persons as discussed below.

In relation to a trust

3. A TCSP should have policies and procedures in place to identify the following and verify their identity using reliable, independent source documents, data or information (provided that the TCSP's policies should enable it to disregard source documents, data or information which are perceived to be unreliable)

i. the settlor;

ii. the protector;

iii. the trustee(s), where the TCSP is not acting as trustee;

iv. the beneficiaries or class of beneficiaries, and

v. any other natural person actually exercising effective control over the trust.

Settlor

a) A settlor is generally any person (or persons) by whom the trust was made. A person is a settlor if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the settlor must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration).

b) A settlor may or may not be named in the trust deed. TCSPs should have policies and procedures in place to identify and verify the identity of the real economic settlor.

c) A TCSP establishing on behalf of a client or administering a trust, company or other legal entity or otherwise acting as or providing a trustee or director of a

trustee, company or other legal entity should have policies and procedures in place (taking a risk based approach) to identify the source of funds in the trust, company or other legal entity.

d) It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift, letter of wishes etc.

e) Where assets have been transferred to the trust from another trust, it will be necessary to obtain this information for both transferee and transferor trust.

Beneficiaries

a) A TCSP should have policies and procedures in place, adopting a RBA to enable it to form a reasonable belief that it knows the true identity of the beneficiaries of the trust, and taking reasonable measures to verify the identity of the beneficiaries, such that the TCSP is satisfied that it knows who the beneficiaries are. This does not require the TCSP to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the TCSP should at least identify and verify the identity of beneficiaries who have current fixed rights to distributions of income or capital or who actually receive distributions from the trust (e.g. a life tenant).

b) Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), a TCSP should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).

c) Where beneficiaries are identified by reference to a class (e.g. children and issue of a person) or where beneficiaries are minors under the law governing the trust, although a TCSP should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed) the TCSP is not obliged to obtain additional information to verify the identity of the individual beneficiaries referred to in the class unless or until the trustees determine to make a distribution to such beneficiary.

d) In some trusts, named individuals only become beneficiaries on the happening of a particular contingency (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, TCSPs are not required to obtain additional information to verify the identity of such contingent beneficiaries unless or until the contingency is satisfied or until the trustees decide to make a distribution to such a beneficiary.

e) TCSPs who administer the trust or company or other legal entity owned by a trust or otherwise provide or act as trustee or director to the trustee, company or other legal entity should have procedures in place so that there is a requirement to update the information provided if named beneficiaries are added or removed from the class of beneficiaries, or beneficiaries receive distributions or benefits for the first time after the information has been provided, or there are other changes to the class of beneficiaries.

f) TCSPs are not obliged to obtain other information about beneficiaries other than to enable the TCSP to satisfy itself that it knows who the beneficiaries are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust is a PEP.

Natural person exercising effective control

a) A TCSP providing services to the trust should have procedures in place to identify any natural person exercising effective control over the trust.

b) For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:

i. dispose of or invest (other than as an investment manager or adviser) trust property;

ii. direct, make or approve trust distributions;

iii. vary or terminate the trust;

iv. add or remove a person as a beneficiary or to or from a class of beneficiaries and or;

v. appoint or remove trustees.

c) TCSPs who administer the trust or otherwise act as trustee must, in addition, also obtain information to satisfy itself that it knows the identity of any other individual who has power to give another individual “control” over the trust; by conferring on such individual powers as described in paragraph (b) above.

Corporate settlors and beneficiaries

4. These examples are subject to the more general guidance on what information should be obtained by the TCSP to enable it to identify settlors and beneficiaries. It is not intended to suggest that a TCSP must obtain more information about a beneficiary which is an entity where it would not need to obtain such information if the beneficiary is an individual.

a) In certain cases, the settlor, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, the TCSP should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to the entity.

b) In the case of a settlor which is a legal entity, the TCSP should satisfy itself that it has sufficient information to understand the purpose behind the formation of the trust by the entity. For example, a company may establish a trust for the benefit of its employees or a legal entity may act as nominee for an individual settlor or on the instructions of an individual who has provided funds to the legal entity for this purpose. In the case of a legal entity acting as nominee for an individual settlor or on the instructions of an individual, the TCSP should take steps to satisfy itself as to the identity of the economic settlor of the trust (i.e. the person who has provided funds to the legal entity to enable it to settle funds into the trust) and the controlling persons in relation to the legal entity at the time the assets were settled into trust. If the corporate settlor retains powers over the trust (e.g. a power of revocation), the TCSP should satisfy itself that it knows the current beneficial owners and controlling persons of

the corporate settlor and understands the reason for the change in ownership or control.

c) In the case of a beneficiary which is an entity (e.g. a charitable trust or company), the TCSP should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, the TCSP should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate trustee

a) Where a TCSP is not itself acting as trustee, it is necessary for the TCSP to obtain information to enable it to identify and verify the identity of the trustee(s) and, where the trustee is a corporate trustee, identify the corporate, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity.

b) Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the TCSP should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A TCSP can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body which regulates the trustee and of the regulated trustee itself).

c) It is not uncommon for families to set up trust companies to act for trusts for the benefit of that family. These are typically called private trust companies and may have a restricted trust licence which enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, the TCSP should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, the TCSP does not need to obtain detailed information to identify the directors or controlling persons of that entity which acts as shareholder of the private trust company.

Individual and Corporate protector

a) Where a TCSP is not itself acting as a protector and a protector has been appointed, it is necessary for the TCSP to obtain information to enable it to identify and verify the identity of the protector

b) Where the protector is a legal entity, the TCSP should obtain sufficient information that it can satisfy itself who is the controlling person and beneficial owner of the protector, and take reasonable measure to verify their identity.

c) Where the protector is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT

laws, regulations and other measures, the TCSP should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A TCSP can rely on external evidence, such as information in the public domain to satisfy itself as to the beneficial owner of the regulated protector (e.g. the web-site of the body that regulates the protector and of the regulated protector itself).

Annex 2: Glossary of terminology

Beneficial Owner

Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Competent Authorities

Competent authorities refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency and bearer negotiable instruments (BNIs); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.

Designated Non-Financial Businesses and Professions (DNFBPs)

Designated non-financial businesses and professions means:

a) Casinos (which also includes internet and ship based casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the Recommendations, and which as a business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;

- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

Express Trust

Express trust refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).'

FATF Recommendations

Refers to the FATF Forty Recommendations.

Legal Person

Legal person refers to any entities other than natural persons that can establish a permanent client relationship with a legal professional or otherwise own property. This can include bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Legal Professional

In this Guidance, the term *"Legal professional"* refers to lawyers, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Red Flags

Any fact or set of facts or circumstances which, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A "red flag" may be used as a short hand for any indicator of risk which puts an investigating TCSP on notice that further checks or other appropriate safeguarding actions will be required.

Self-regulatory bodies (SRB)

A *SRB* is a body that represents a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or

monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

Supervisors

Supervisors refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("financial supervisors" 90) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

Annex 3: Supervisory practices for implementation of the RBA to TCSPs[26]

The Group of International Finance Sector Supervisors (GIFCS)

Originally known as the Offshore Group of Banking Supervisors, GIFCS was formed in 1980 at the instigation of the Basel Committee on Banking Supervision. Whilst maintaining a close working relationship with the Basel Committee, the group now represents the interests of its member jurisdictions in the supervision of banks, collective investment funds, securities activities and TCSP sectors. GIFCS, which represents supervisory authorities of 20 regional and international finance centres, issued a Standard for the Regulation of TCSPs which sets a minimum benchmark for the effective supervision of the sector, incorporating licensing requirements, together with principles for AML/CFT, prudential and governance supervision of the sector. https://www.groupgifcs.org/letsgo/uploads/gifcsstandardontcsps.pdf

The Standard contains principles for supervision, and specifically includes requirements that the supervisor:

- Assesses at the time of licensing and on an ongoing basis whether a TCSP, its controllers, directors, partners, and Money Laundering Reporting and Compliance Officers are fit and proper,
- Considers the ownership, structure, control and management of the TCSP ensuring that that the ownership structure does not hinder effective supervision or facilitate regulatory arbitrage,
- Requires a TCSP to demonstrate physical presence in the jurisdiction in which it is being regulated which would be demonstrated by requiring its "mind and management" being resident in the jurisdiction and actively involved in the TCSP's governance and having an operational place of business in the jurisdiction,
- Requires that a TCSP embeds a robust corporate governance culture and risk management framework,
- Ensures that a TCSP has ongoing effective management and/or administrative control mechanisms over legal persons and legal arrangements for which its acts, particularly in relation to ultimate beneficial ownership and ensuring that full documentation and information is held on the activity of those vehicles, and
- Ensures that a TCSP has controls to prevent it becoming engaged directly or indirectly with bribery and corruption.

[26] The Hong Kong Institute of Chartered Secretaries (HKICS) has issued an updated guidance to TCSP sector. This is available at: www.hkics.org.hk/media/publication/attachment/PUBLICATION_A_2380_HKICS_AML_CFT_Guideline.pdf. Further, the British Virgin Islands'(BVI's) Anti-Money Laundering and Terrorist Financing (Amendment) (No. 2) Code of Practice, 2018 is available at: www.bvifsc.vg/sites/default/files/anti-money_laundering_and_terrorist_financing_amendment_no._2_code_of_practice_2018.pdf

The Standard also underpins the FATF Recommendations and has a particular focus for supervisors on national and international cooperation and information sharing and ensuring the effective implementation by a TCSP of targeted financial sanctions. All its members are committed to meeting the Standard. A process to evaluate its members' compliance with Standard commenced in 2016.

Guernsey

Guernsey is an international finance centre with a significant TCSP sector which has been subject to prudential and AML/CFT supervision since 2001. The Guernsey Financial Services Commission ("the Commission") is the competent authority in the Bailiwick of Guernsey for licensing and supervising Trust and Corporate Service Providers ("TCSPs).

Under the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000 all licensed TCSPs must at the outset and on an ongoing basis meet a minimum criteria for licensing. This criteria includes a transparent ownership structure, capital adequacy, suitable experience and favourable track record, a suitable risk management framework, sufficient staffing and systems resources, and at least two directors resident in Guernsey who are independent of each over and of appropriate standing and experience to effectively direct and apply "four eyes" control over the business.

Within this criteria, the TCSP and each individual occupying the role of controller (including beneficial owners), partner, director or manager must at the outset and on an ongoing basis meet a fit and proper test covering competence, probity (encompassing their integrity, honesty and reputation), experience, professionalism, soundness of judgement and solvency. Individuals must complete an extensive personal questionnaire recording their employment record, professional qualifications, personal business interests and records regarding any bankruptcy proceedings and any criminal, regulatory or disciplinary sanctions or pending cases.

All licence applications are subject to careful scrutiny. The Commission has statutory powers to impose sanctions against a TCSP or an individual where it considers that the minimum licensing criteria, including the fit and proper criterion, is not or has not been met. Those powers include the power to revoke licences, prohibit individuals from holding a position in the finance sector, impose fines and issue public statements where this criteria is not met. The Commission has published its policy to enforce and use such powers where the failings are sufficiently serious that addressing deficiencies through ordinary or enhanced supervisory processes are not appropriate.

Examples of supervisory action

Example 1 (Refusal of licence application)

An application for a licence was made to establish a TCSP services. Its business model contained a number of significant inherent higher risk factors including proposals to offer "family office" services and yacht administration to high net worth individuals based in jurisdictions identified by credible sources as at a higher risk of bribery and

corruption. It also included jurisdictions which had yet to implement international tax standards on exchange of information.

The application raised the following concerns:

- The applicant proposed having two executive directors. One of the directors would work full time and the other who would give 20% of his normal working week to the business of the applicant but stating that he would increase his hours if necessary. However this director had a large number of other unrelated business interests which could limit the amount of time that he could devote to the applicant's business. The Commission was therefore concerned that there would be lack of effective challenge to the one full time director and limited "four-eyes" control over the applicant's business, a key tenant of the minimum licensing criteria.
- The quality of the application made by the applicant was extremely poor, exhibiting a lack of awareness of the requirements regarding minimum capital and insurance cover for TCSPs together with key information missing on financial forecasts and operating policies and procedures, demonstrating lack of professionalism and skill to provide trust and corporate services. The Commission was not satisfied that the applicant and its directors met the fit and proper test.

The Commission issued a notice that it was "minded to refuse the application" on the grounds that the applicant did not meet the minimum licensing criteria. The application was subsequently withdrawn.

Example 2 (enforcement)

The Commission imposed sanctions against four individuals who were controllers (owners) and directors of a TCSP, and against a fifth individual who was its independent non-executive director, after identifying during an onsite inspection significant failings in the TCSP's anti-money laundering and countering terrorist financing systems and controls. The individuals had failed to ensure that TCSP met the following regulatory requirements of Guernsey AML/CFT regime:-

- To undertake and regularly review relationships risk assessments
- To always take reasonable measures to identify and verify customers and beneficial owners or to obtain information on the purposes and intended nature of each business relationship
- To always undertake enhanced customer due diligence on customers assessed as high risk
- To perform ongoing and effective monitoring of its existing business relationships

- To have appropriate and effective procedures to ensure compliance with legislation for disclosing suspicious activity

The Commission had previously identified similar failings within the TCSP which it had been required to remediate and which had not been appropriately actioned in all instances. As a consequence of these failings the Commission concluded that the individuals had failed to understand the legal and professional obligations upon them as controllers and directors of a TCSP. In failing to remedy previously identified deficiencies the individuals had acted without sound judgement required as part of the fit and proper criterion.

The four executive directors were each fined £50,000 and the non-executive director was fined £10,000. Three of the executive directors were prohibited from acting as a controller, partner, director or money laundering reporting officer within the Bailiwick's finance industry for five years. A public statement was issued identifying the individuals, providing information on the case and the sanctions which were applied.

Example 3 (enforcement)

A TCSP and three of its directors were sanctioned by the Commission for failing to implement appropriate and effective polices, procedure and controls to mitigate ML/TF risks to which the business could be exposed. An onsite inspection identified fundamental failings in the TCSP's anti-money laundering and countering of terrorist financing systems and controls, particularly in respect of business relationships assessed as high risk involving politically exposed persons ("PEPs") linked to higher risk jurisdictions. The failings were referred to the Commission's Enforcement Division to undertake further investigation which carried out a further onsite inspection.

The Commission identified the following failings:

- That the TCSP failed to conduct customer due diligence in accordance with regulatory requirements, and in respect of individuals to whom a Power of Attorney had been granted or were potential beneficiaries of trusts;
- That the TCSP failed to undertake sufficient enhanced customer due diligence, including taking reasonable measures to establish source of wealth and funds of customers who were PEPs and had links to jurisdictions identified by credible sources as having a higher risk of bribery and corruption;
- That the TCSP failed to effectively monitor ongoing customer activity or scrutinise unusual transactions.

The failings were similar to deficiencies identified in two previous inspections to the TCSP and showed that the remedial action that it had been required to undertake had not been appropriately actioned in all instances. The Commission concluded that the TCSP's systems and

controls did not enable it to comply with Guernsey's AML/CFT regulatory requirements and therefore the TCSP had not conducted its business in a prudent manner required by the minimum licensing criteria. The Commission considered that the Directors had demonstrated a lack of probity, competence and soundness of judgement which are factors which are taken into account when considering whether a director is a fit and proper person.

The firm was fined £42,000, one of the directors who served as the compliance director and money laundering reporting officer was fined £18,375 and the two other directors were each fined £10,500. A public statement was issued identifying the parties, providing information on the case and the sanctions which were applied.

Hong Kong, China

Priority is given to and more resources are accorded to higher risk cases for targeted inspection. For higher risk cases, on-site inspections are conducted on a priority basis and the TCSP licensees are subject to more frequent compliance inspections to ensure their continuous compliance with the statutory CDD and record-keeping requirements. Customer and transaction records are checked during the on-site inspections to ensure that effective AML/CFT measures are in place for compliance with the statutory requirements. For higher risk cases, a higher proportion of such records will be selected for checking.

Also, applicants for TCSP licences and licensees are required to complete a supplementary information sheet to provide the relevant information in order to monitor their compliance with the AML/CFT requirements and to assess their ML/TF risks. Off-site supervision consists of analysis of the supplementary information sheets and ongoing monitoring of the compliance of the licensing conditions of the licensees, including compliance with AML/CFT requirements, classifying the risk profiles of individual licensees, identifying risky applicants/licensees, undertaking thematic reviews of the sector and meeting with trade representatives to monitor and assess any changes in the trade practice. Follow-up actions, including prosecution and disciplinary action, will be taken if any non-compliance with statutory CDD and record keeping requirements is identified.

Examples of supervisory action

Example 1

An application for TCSP licence was made by Corporation A. Ms B was the sole director and ultimate owner of Corporation A. She was also named as Corporation A's Compliance Officer and the Money Laundering Reporting Officer. The Companies Registry (CR) conducted on-site inspection on Corporation A to interview Ms B and inspect transaction records of Corporation A. During the inspection, Ms B was unable to produce any record or document and there was no evidence showing that Ms B as the Compliance Officer and the Money Laundering Reporting Officer was normally based in Hong Kong.

Upon consideration of all the circumstances of the case including the non-compliances above, the CR was not satisfied that Ms B was fit and proper to carry on or be associated with a TCSP business. As a result, Corporation A's application for TCSP licence was rejected.

Example 2

A group of five TCSPs operating at the same business premises applied for TCSP licences. They provided company services to a very large number of customers and acted as the company secretaries of over 70 000 companies. A Mr X was the ultimate owner and director of the five TCSPs, and was also the Compliance Officer and Money Laundering Reporting Officer of these TCSPs.

Some of these TCSPs were checked to be the company secretaries of front companies suspected of having business or connection with entities subject to the United Nations Security Council sanctions.

The CR conducted on-site inspection at the business premises and inspected records of the TCSPs' customers and transactions. Mr X was interviewed. All five applicants and Mr X failed to demonstrate that they were fit and proper to carry on or be associated with a TCSP business. They also failed to demonstrate that they had complied with the statutory CDD and record-keeping requirements. Eventually, all the five applicants had withdrawn their applications for TCSP licences before CR proceeded to reject their applications.

Isle of Man

Through the Beneficial Ownership Act 2017 (the "Act"), the Isle of Man established a Beneficial Ownership Register held by the Companies Registry and overseen by the Isle of Man Financial Services Authority. This legislation compliments longstanding requirements upon FIs and DNFBPs to undertake customer due diligence requirements including beneficial owners of their customers.

From 1st July 2017 the Act placed legal obligations on certain types of legal persons, their beneficial owners, intermediate owners, legal owners and nominated officers with regard to beneficial ownership information, namely that beneficial ownership information should be passed through the ownership chain to the legal person's nominated officer. The legal person's nominated officer must retain all beneficial owners' details, and add any beneficial owners holding more than 25% ownership or control to the beneficial ownership database. The Act does not apply to legal persons which are foreign companies, a company listed on a recognised stock exchange or entities wholly owned by a company listed on a recognised stock exchange.

The FSA has powers in order to ascertain whether the obligations and requirements imposed by the Act have been and are being complied with and whether the database is effective and its information accurate. The following case example provides an example of supervisory action:

Members of the FSA's Enforcement Division conducted an inspection in relation to 10 companies which had a common nominated officer. The nominated officer was visited and the information held by them checked against the submissions made to the

beneficial ownership database. Minor errors were identified in relation to two companies whereby the nature of ownership was recorded incorrectly and the trustees of a trust had not been considered as beneficial owners of the underlying Isle of Man company. The Authority issued a report identifying the errors, detailing how the nominated officer should regularise them and a deadline for which the corrections must be made. The database was updated by the nominated officer in the given timescale.

Jersey

Supervising TCSP's business/enterprise risk assessment

The Jersey Financial Services Commission (JFSC) received a response from a regulated TCSP to queries the JFSC raised over its risk assessment. The response provided details of a 'cash register' and cash transactions undertaken on behalf of its customers. Owing to the inherent ML risk relating to these transactions, the TCSP was formally placed under investigation, encompassing a 6-day onsite examination with Enforcement and Supervision reviewing corporate governance, the compliance function and conduct of business, with particular focus to those customers identified on the cash register. Following the on-site examination the JFSC made the following observations:

The regulated TCSP appeared to have committed significant breaches of the TCSP Code of Practice;

Contrary to legal and regulatory requirements, the TCSP had carried out cash transactions where it did not hold adequate CDD, Source of Funds or rationale for services being carried out.

The TCB was informed that the JFSC was concerned that it may have facilitated money laundering on an extensive scale, for which suspicious activity reports were submitted. Directions were issued to each principal person restricting their involvement in Jersey's finance industry, along with the issuance of a public statement in respect of the TCSP and the Principals

Examples of supervisory actions

Example 1

The JFSC undertook an onsite examination to a TCSP and identified deficiencies related to corporate governance, effectiveness of compliance function and AML/CFT issues, which included ineffective procedures, transaction monitoring deficiencies, lack of CDD/Source of Funds (including on PEPs), lack of AML/CFT awareness/training and deficient record keeping. As a result of these deficiencies, the JFSC issued a Notice requiring the appointment of a reporting professional to review a larger sample of client files. The reporting professional's findings replicated to a large extent the JFSC's findings.

Whilst the Reporting Professional's review was being undertaken, the JFSC became aware of a Notice on a foreign regulator's website regarding an action that was being taken in relation to a company that had a connection to a company that the Reporting Professional was reviewing. Contact was made with the foreign regulator and a meeting was held. Assistance was also provided to law enforcement authority from the foreign jurisdiction concerned regarding a fraud perpetrated there but where the proceeds of the fraud were received by the TCSP. Perpetrators of the fraud were jailed in the UK. The business was sold to another TCSP and the JFSC issued a public statement and placed restrictions on the Principal Persons by directions.

Example 2

The JFSC conducted a supervisory on-site examination of a regulated TCSP, which identified a number of significant concerns over corporate governance and its provision of services to structures under administration. An internal remediation process was undertaken and a regulatory consulting firm was engaged to perform an independent review of the corporate governance and customer files in respect of the trust company business. The regulated TCSP also promptly implemented initial steps in relation to training and revised policies and procedures to remediate issues identified.

Following the on-site examination, the JFSC required co-signatories to be appointed to review and pre-approve certain transactions. The co-signatories were required to provide a report of any issues identified during the course of their engagement. Two individuals responsible for approx. 70% of the trust and corporate business clients voluntarily took a leave of absence and subsequently left.

The on-site examination, co-signatories report and consultants report identified a lack of effective governance and lack of appropriate compliance oversight in relation to the trust company business. This resulted in the two individuals receiving banning directions and a public statement being issued in respect of the regulated TCSP and both individuals. Following the conclusion of the investigation, the regulated TCSP underwent intense remediation, monitored by the JFSC.

Example 3

During an on-site examination serious concerns were noted in relation to the conduct of the TCSP and its principal persons in the provision of services to a customer structure. The matter was referred to the Enforcement Division and an investigation was commenced, which identified a number of failings on behalf of the TCSP and its principal and key persons in relation to the customer structure. In order to assess whether the failings were inherent across the wider business, the JFSC required the TCSP to appoint an independent reporting professional to

conduct a wider review of customer structures. The investigation and the reporting professional's report both identified a lack of effective governance surrounding, and inadequate systems and controls in respect of the TCSP's obligations under the AML/CFT regime on issues related to obtaining sufficient CDD; applying correct customer risk ratings; understanding and documenting customer rationale, fully understanding source of wealth/source of funds; exercising control and understanding the complexity of risks; implementing a robust annual review process; considering and acting upon adverse information; poor record keeping and failing to consider obligations under the AML/CFT legislation to with regards to suspicious activity reporting

The JFSC issued directions requiring remediation and to the principal and key persons requiring further AML/CFT training.

Example 4

The JFSC was notified of a number of regulatory breaches namely four breaches of Section 8.3.1 of the AML/CFT Handbook, the late notification and internal reporting to the MLRO of suspicion relating to customers. As a result of the late notification of the breaches, the TCB was issued with Civil Penalty warning. Given the nature of the breaches, the matter was referred to Enforcement for consideration, who made the Jersey FIS aware of concerns over failing to report and late submission of SARs.

In agreement with the JFSC, the TCSP appointed a reporting professional voluntarily to conduct a review of its remediation of issues and compliance function.

The report produced alleviated much of the JFSC's concerns concerning the current compliance environment however there was still some remediation required. The matter was passed back to Supervision for monitoring of the remediation and to test at a later stage. The TCSP was notified that the JFSC would consider a Band 2 Civil Penalty should the issues not be remediated satisfactorily.

Example 5

As a result of an on-site examination, concerns were highlighted over the competency of the MLRO in AML/CFT at a TCSP. Specifically it appeared that the MLRO had failed to externalise a number of internal SARs in circumstances where he noted suspicion of criminality.

Following a referral from Supervision, Enforcement conducted an investigation in respect of the MLRO's fitness and propriety. The investigation concluded that the MLRO lacked competency in AML/CFT matters but did not lack integrity.

A without prejudice settlement was entered into with the MLRO, restricting him from acting in any Key Person role until such time he

completed further AML/CFT training. As a result of the Enforcement action, the TCB appointed a new MLRO.

Malaysia

A. Fit and Proper Requirements

Trust service providers in Malaysia consist of trust companies registered under the Trust Companies Act 1949 or incorporated under the Public Trust Corporation Act 1995. Company service providers are made up of members of professional bodies or individuals licensed by the Companies Commission of Malaysia. All TCSPs are subject to appropriate market entry controls under the respective legislation and professional obligations governing them, by which they are required to fulfil certain fit and proper requirements.

B. AML/CFT Risk-based Supervision – Bank Negara Malaysia (BNM)

Under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), BNM is the designated competent authority for the AML/CFT supervision of the DNFBPs, including TCSPs. BNM adopts a risk-based approach supervision on TCSPs, in which the differentiation is guided by the outcome of the National Risk Assessment (NRA) and the application of Risk-Based Supervisory Framework (D'SuRF), as follows:

i. National Risk Assessment (NRA) 2017

Malaysia's third iteration of the NRA in 2017 comprising assessment of ML/TF inherent risk and overall control effectiveness stipulated the TCSPs' net ML and TF risks as **"MEDIUM HIGH"** and **"MEDIUM"** level, respectively, as exacerbated by the sector's marginal control, as follows:

ML		TF	
Inherent Risk	Medium	Inherent Risk	Low
Control	Marginal	Control	Marginal
Net Risk	Medium High	Net Risk	Medium

i. Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF)

D'SuRF encapsulates end-to-end governance and supervisory process, risk-based application of supervisory tools. In line with the ML/TF rating of the sector and the application of D'SuRF, the frequency and intensity of monitoring on TCSPs are guided accordingly to include a range of supervisory tools, which include the following:

- **On-site Examination**

Firms are selected based on a robust selection process under the D'SuRF, which is in line with the risk profile of the reporting institutions (RIs). The on-site examination is in-depth, with assessments covering the RIs' inherent risk and quality of risk management. In applying RBA, BNM imposes post-onsite follow-up measures for RIs with heightened risks. This includes requiring the RI to submit proposals to BNM on planned measures to rectify any supervisory issues and progress report until full rectification. The D'SuRF sets the deadline for both submissions. The follow-up measures have been imposed on a number of TCSPs selected for on-site examination.

- **Off-site Monitoring and Supervisory Outreach Activities**

In addition, BNM employs a range of off-site monitoring and supervisory outreach activities, aimed to elevate awareness and guide the implementation of the AMLA requirements by the TCSPs. These off-site tools are also deployed according to the RBA, whereby the intensity and frequency for the TCSPs is relatively higher compared to other sectors. Among the off-site monitoring, includes the submission of data and compliance Report, internal audit reports, and statistical data. BNM and the relevant SRBs also conduct periodic nationwide AML/CFT outreach and awareness programmes.

Monaco

Monaco completed its first NRA (National Risk Assessment) in 2017 and the CSPs were included in the scope (see public NRA report in www.siccfin.mc/en/The-National-Risk-Assessment-NRA).

The assessed risk regarding CSPs was rated MH (moderate high) so the CSP are included in the priority professionals to be inspected on-site. There are about 40 CSPs in Monaco so ten to twelve inspections are planned every year. In addition, the CSPs are subject to a compulsory annual questionnaire which they have to send to SICCFIN by February 28, which helps the supervisor in detecting anomalies in their activities. The RBA is not yet fully formalized, but the selection of CSPs to be added to the inspection planning is performed as follows:

- The date of the previous inspection
- The conclusions of the previous inspection and how the CSP responded to it (improvements implemented)
- The evolution of the CSP as detected through the annual questionnaire
- Information transmitted by the FIU (which is within SICCFIN as well as the supervision of professional submitted to AML act) regarding the quality of SARs and other related topics.

Other criteria are planned to be added in the near future.

Singapore

Singapore's Registered Filing Agents and Registered Qualified Individuals Regulatory Regime

Since 2015, firms and companies which intend to incorporate legal entities on behalf of another person or provide corporate services (e.g. acting or arranging for someone to act as director, secretary, shareholders or providing registered office addresses) in the course of their business, must register with the Accounting and Corporate Authority (ACRA) as a Registered Filing Agent (RFA). These firms have to act through at least one Registered Qualified Individual (RQI) with ACRA. Lawyers and accountants are supervised by their respective regulators/regulatory bodies, but if the accountancy or law firm also provides corporate services, it also needs to be registered with ACRA as a RFA and will be subjected to ACRA's AML/CFT requirements in their role as a RFA.

These firms will not be permitted to register as a RFA if any of the firm's beneficial owners, directors, partners or managers have been convicted of criminal offences or if they are undischarged bankrupts. An individual will not be permitted to be registered as a RQI if he/she has been convicted of a criminal offence (especially those related to fraud or dishonesty) or if he is an undischarged bankrupt.

Since 15 Nov 2018, ACRA has enhanced the RFA's registration requirements to mandate anyone seeking registration or renewal as a RFA, to complete a prescribed AML/CFT training programme and also pass a proficiency test once every two years as a pre-condition to their registration or renewal. This seeks to ensure that RFAs can adequately comply with AML/CFT obligations through continuous education.

Annex 4: Members of the RBA Drafting Group

FATF members and observers	Office	Country/Institution
Sarah Wheeler (Co-chair)	Office for Professional Body AML Supervision (OPBAS), FCA	UK
Sandra Garcia (Co-chair)	Department of Treasury	USA
Erik Kiefel	FinCen	
Helena Landstedt and Josefin Lind	County Administrative Board for Stockholm	Sweden
Charlene Davidson	Department of Finance	Canada
Viviana Garza Salazar	Central Bank of Mexico	Mexico
Fiona Crocker	Guernsey Financial Services Commission	Group of International Finance Centre Supervisors(GIFCS)
Ms Janice Tan	Accounting and Regulatory Authority	Singapore
Adi Comeriner Peled	Ministry of Justice	Israel
Richard Walker	Financial Crime and Regulatory Policy, Policy & Resources Committee	Guernsey
Selda van Goor	Central Bank of Netherlands	Netherlands
Natalie Limbasan	Legal Department	OECD
	Accountants	
Member	Office	Institution
Michelle Giddings (Co-chair)	Professional Standards	Institute of Chartered Accountants of England & Wales
Amir Ghandar	Public Policy & Regulation	International Federation of Accountants
Legal professionals and Notaries		
Member	Office	Institution
Stephen Revell (Co-chair)	Freshfields Bruckhaus Deringer	International Bar Association
Keily Blair	Economic Crime, Regulatory Disputes department	PWC, UK
Mahmood Lone	Regulatory issues and complex cross-border disputes	Allen & Overy LLP, UK
Amy Bell	Law Society's Task Force on ML	Law Society, UK
William Clark	ABA's Task Force on Gatekeeper Regulation and the Profession	American Bar Association (ABA)
Didier de Montmollin	Founder	DGE Avocats, Switzerland
Ignacio Gomá Lanzón Alexander Winkler	CNUE's Anti-Money Laundering working group	Council of the Notariats of the European Union (CNUE)
	Notary office	Austria
Rupert Manhart	Anti-money laundering Committee	Council of Bars and Law Societies of Europe
Silvina Capello	UINL External consultant for AML/CFT issues	International Union of Notariats (UINL)

	TCSPs	
Member	Office	Institution
John Riches (Co-chair) Samantha Morgan	RMW Law LLP	Society of Trust and Estate Practitioners (STEP)
Emily Deane	Technical Counsel	
Paul Hodgson	Butterfield Trust (Guernsey) Ltd	The Guernsey Association of Trustees
Michael Betley	Trust Corporation International	
Paula Reid	A&L Goodbody	A&L Goodbody, Ireland

FATF

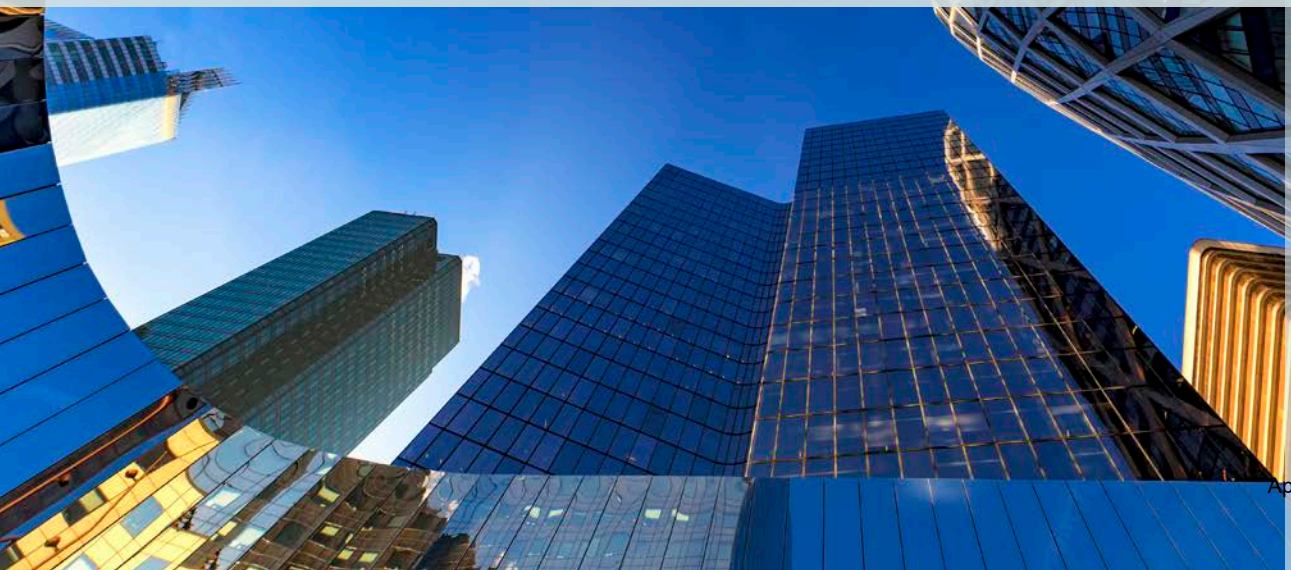
GUIDANCE FOR A RISK-BASED APPROACH
TRUST AND COMPANY SERVICE PROVIDERS

The risk-based approach (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012.

This guidance highlights the need for a sound assessment of the money laundering and terrorist financing risks that trust and company service providers face so that the policies, procedures and initial and ongoing client due diligence measures can mitigate these risks.

The FATF developed this non-binding guidance with significant input from the TCSP sector, to ensure that it reflects their practical expertise and good practices.

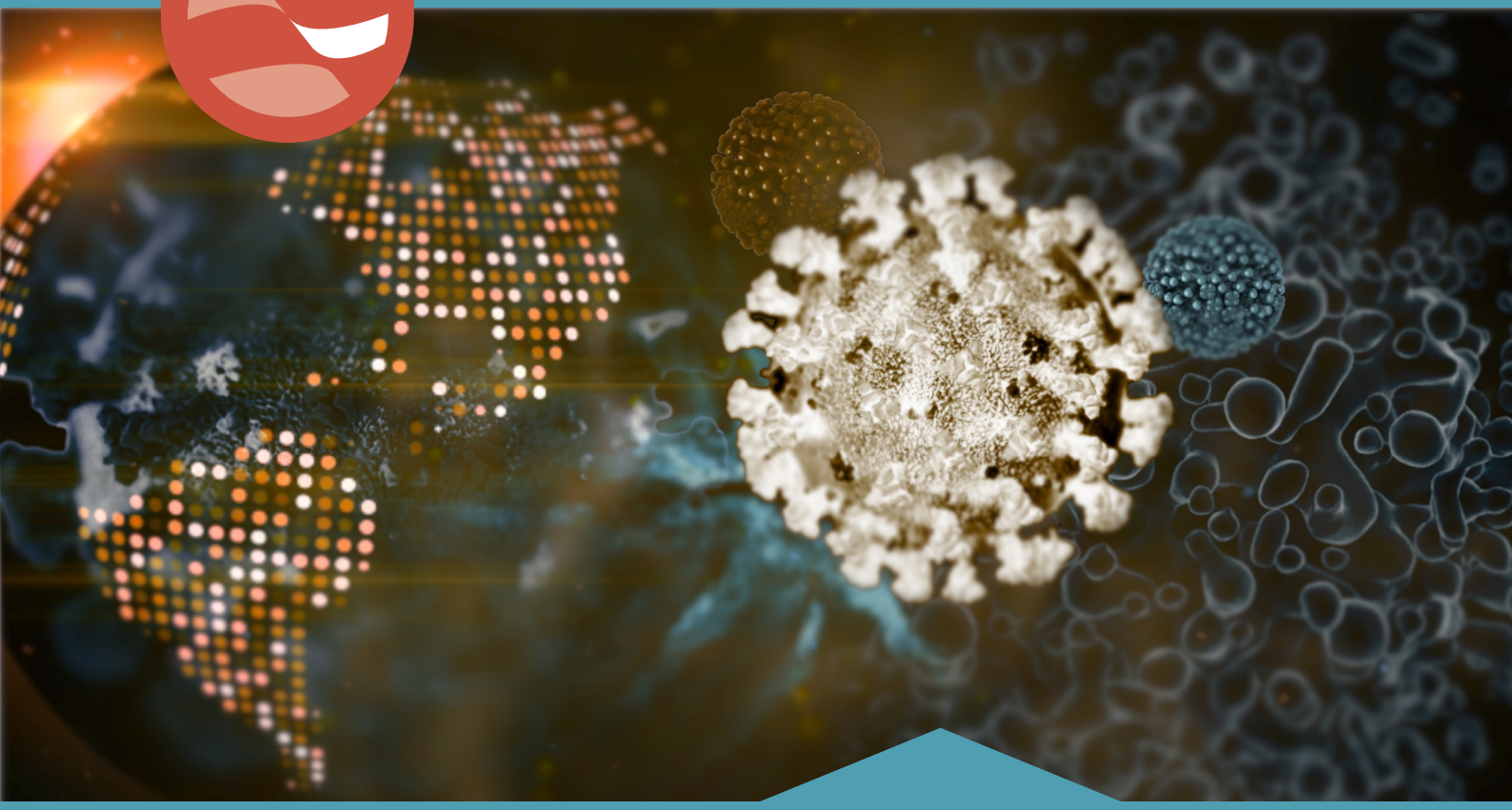
www.fatf-gafi.org | June 2019



Appendix RR:

COVID-19-related Money Laundering and Terrorist Financing: Risks and Policy Responses (Paris: FATF, 2020)

FATF



COVID-19-related Money Laundering and Terrorist Financing

Risks and Policy Responses

May 2020

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2020), *COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses,* FATF, Paris, France,
www.fatf-gafi.org/publications/methodandtrends/documents/covid-19-ML-TF.html

COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses

Foreword

The COVID-19 pandemic has led to unprecedented global challenges, human suffering and economic disruption. This paper identifies challenges, good practices and policy responses to new money laundering and terrorist financing threats and vulnerabilities arising from the COVID-19 crisis.

It is based on papers shared on 7 and 23 April with the FATF Global Network of FATF Members and FATF-Style Regional Bodies (FSRBs), together making up more than 200 jurisdictions. The authors thank the FATF members, observers, the FSRB Secretariats and their members for their contribution to the report. This report was written by Kristen Alma, Shana Krishnan, Colby Mangels and Mei-Lin Wang from the FATF Secretariat.

This paper is for information and does not constitute the official view of the FATF. It does not imply or constitute any changes to the FATF Standards. The measures cited, and taken by some FATF members' authorities, have not been reviewed or considered by the FATF membership as a whole.

Table of contents

Key findings

- The increase in COVID-19-related crimes, such as fraud, cybercrime, misdirection or exploitation of government funds or international financial assistance, is creating new sources of proceeds for illicit actors.
- Measures to contain COVID-19 are impacting on the criminal economy and changing criminal behaviour so that profit-driven criminals may move to other forms of illegal conduct.
- The COVID-19 pandemic is also impacting government and private sectors' abilities to implement anti-money laundering and counter terrorist financing (AML/CFT) obligations from supervision, regulation and policy reform to suspicious transaction reporting and international cooperation.
- These threats and vulnerabilities represent emerging money laundering (ML) and terrorist financing (TF) risks. Such risks could result in:
    - Criminals finding ways to bypass customer due diligence measures;
    - Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
    - Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds;
    - Increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds;
    - Misuse and misappropriation of domestic and international financial aid and emergency funding;
    - Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries.
- AML/CFT policy responses can help support the swift and effective implementation of measures to respond to COVID-19, while managing new risks and vulnerabilities. These include:
    - Domestic coordination to assess the impact of COVID-19 on AML/CFT risks and systems;
    - Strengthened communication with the private sector;
    - Encouraging the full use of a risk-based approach to customer due diligence;
    - Supporting electronic and digital payment options.

1. Introduction

This paper is part of a coordinated and timely response to the impact of the COVID-19 crisis on global anti-money laundering (AML) and counter terrorist financing (CFT) efforts and the application of the FATF Standards in this context. This response also includes a Statement from the FATF President, issued on 1 April, on how the risk-based approach of the FATF Standards provides for emerging threats and vulnerabilities to be managed effectively and in support of COVID-19 aid and containment efforts (see Annex A).

A list of statements and guidance issued by authorities in response to COVID-19 is included in Annex B, for reference.

This paper was developed in response to the unprecedented and rapidly evolving COVID-19 public health crisis. The findings contained within are likely to evolve as this crisis further develops.

This paper is informed by open-source research, and information received from member countries of the FATF and FATF-style regional bodies (FSRBs) and observer organisations such as the International Monetary Fund (IMF), World Bank and United Nations.

The focus of this paper relates to three broad themes:

- New threats and vulnerabilities stemming from COVID-19-related crime and impacts on ML and TF risks;
- Current impact on AML/CFT efforts by governments and the private sector due to COVID-19;
- Suggested AML/CFT policy responses to support the swift and effective implementation of measures to respond to COVID-19, while managing new risks and vulnerabilities identified, including: charitable activity and economic and fiscal stimulus and financial rescue packages for firms and individuals.

2. Evolving ML/TF risk picture

2.1. Increased ML Threats

The COVID-19 pandemic has generated various government responses, ranging from social assistance and tax relief initiatives, to enforced confinement measures and travel restrictions. While unintended, these measures may provide new opportunities for criminals and terrorists to generate and launder illicit proceeds.

While the precise situation and public health responses in each country varies according to the impact of COVID-19, the evolving risk picture detailed in this section is based on the following general assumptions:

- Governments, businesses and individuals are increasingly turning to online systems to enable remote work. Individuals under "lockdown" (or other movement restriction measures) are also increasingly turning to online platforms for social interaction.
- Businesses that are classified as non-essential have physically closed. Both essential and non-essential business are seeing increased online sales.

- The COVID-19 pandemic has driven significant demand for medical supplies, such as personal protective equipment, ventilators and medicines and there is a global shortage of such goods due to the overwhelming demand.
- Banks and financial institutions remain in operation with some offering more limited services and restricting in-person banking.
- The closure of many businesses due to "lockdown" measures and other restrictions on trade and travel has led to mass unemployment or the furloughing of workers, loss of government revenue and a general economic recession that will impact the financial and social behaviour of businesses and individuals.
- Government resources have been reprioritised towards responding to COVID-19, taking resources away from other areas of work.
- With global trade volumes in decline and individual travel at a near standstill, conventional transnational organised crime schemes that take advantage of global supply chains and the traditional illicit revenue schemes of organised crime groups are impacted by COVID-19.

Increased Fraud

Reporting from FATF members, observers, and open sources indicates that criminals have attempted to profit from the COVID-19 pandemic through increased fraudulent activities. At the time of writing, the primary fraudulent activities include:

- **Impersonation of officials**: In such cases, criminals contact individuals (in person, email or telephone) and impersonate government officials with the intent of obtaining personal banking information or physical cash. In some cases, criminals impersonate hospital officials who claim a relative is sick and require payment for treatment (Interpol, 2020[1]), or government officials requesting personal banking information for tax relief purposes (US Treasury, 2020[2]). Cases involving government impersonation are likely to increase as governments around the world disburse grants and tax relief payments to their citizens, with criminals attempting to profit from these payments.
- **Counterfeiting, including of essential goods (such as medical supplies and medicines)**: Given the high demand, there is a significant increase in online scams involving certain medical supplies, personal protective equipment and pharmaceutical products. In such cases, the suspects claim to be employees of businesses, charities, and international organisations offering masks, testing kits and other products, and request credit card information for payment or a shipping fee but never deliver the goods. (US FDA, 2020[3]) In some scenarios, victims were asked to make payment in advance via bank transfers and then directed to collect goods from various locations, but were then subsequently informed that there were no such arrangements. (Singapore Police Force, 2020[4]) In similar scams, the goods are delivered to the consumer but are counterfeit or ineffective.[1] Such scams target both individual consumers and businesses. FATF members are also seeing an increase in false and misleading COVID-19 treatment claims and vendors selling illegal products marketed as "miracle" cures.[2]
- **Fundraising for fake charities**: FATF members highlight an increase in fundraising scams. In such cases, criminals posing as international organisations or charities circulate emails requesting donations for COVID-19-related

[1] (European Commission, 2020[28]) (Cellule de Renseignement Financier Luxembourg, 2020[6]) (Interpol, 2020[7]) (Europol, 2020[8])

[2] (US Justice Department, 2020[9]) (US ICE, 2020[10])

fundraising campaigns (purportedly for research, victims and/or products). Recipients of these emails are then directed to provide credit card information or make payments through the suspect's secure digital wallet.

- **Fraudulent investment scams**: The economic crisis resulting from COVID-19 has led to an increase in investment scams, such as promotions falsely claiming that products or services of publicly traded companies can prevent, detect or cure COVID-19. (Europol, 2020[5]) Reporting by FATF members highlighted that microcap stocks, typically issued by the smallest companies, may be particularly vulnerable to fraudulent investment schemes as they are low-priced stocks with often limited publicly-available information. This facilitates the spread of false information about the company. (US Securities and Exchange Commission, 2020[6])

Cyber Crime

There has been a sharp rise in social engineering attacks, specifically phishing email and mobile messages through spam campaigns. These attacks use links to fraudulent websites or malicious attachments to obtain personal payment information.

- **Email and SMS phishing attacks**: Criminals are exploiting concerns about COVID-19 to insert malware on personal computers or mobile devices. In one example, cybercriminals posed as the World Health Organization (WHO) and sent email and mobile messages to lure individuals into clicking malicious links or opening attachments, which subsequently reveal the individual's user name and password. (WHO, 2020[7]) Various versions of these phishing attacks are currently being reported. Other examples include government impersonation via SMS to lure individuals to fraudulent government websites to obtain personal account information and/or sensitive usernames and passwords. (CISA, 2020[8])
- **Business email compromise scams**: Amid a sharp rise in global remote-working, cybercriminals are also exploiting weaknesses in businesses' network security to gain access to customer contact and transaction information. This information is then used in targeted phishing emails whereby the criminals pose as the compromised business and request payment for legitimate goods and/or services but instead direct this payment into their illicit accounts. (FBI, 2020[9]) In another example, a company received spoofed emails similar to those sent by their business partner to redirect payment transfers to scammers' controlled bank accounts, under the pretext of paying for large supplies of surgical masks and hand sanitiser.
- **Ransomware attacks**: Reports also indicate that cybercriminals are using different methods to insert ransomware on personal computers and mobile devices. For example, some FATF members report that cybercriminals are using malicious websites and mobile applications that appear to share COVID-19-related information to gain and lock access to victims' devices until payment is received. Organisations at the forefront of the COVID-19 response can be heightened targets for cybercriminals. Specifically, hospitals and other medical institutions have increasingly become targets of cybercriminals for ransomware attacks. (Interpol, 2020[10])

Impact on Other Predicate Crimes

- **Human Trafficking[3] and Exploitation of Workers**: Criminals may take advantage of the pandemic to exploit vulnerable groups. This may lead to an increase in the exploitation of workers and human trafficking. (Council of Europe, 2020[11]) The suspension or reduced activity of government agencies regularly engaged in detecting human trafficking cases and identifying victims of trafficking (including workplace inspectors and social and health care workers) means that cases may go undetected. (WEF, 2020[12]) The shutdown of workplaces, slowdown in the economy, rising unemployment, and financial insecurity are factors that could result in an increase in human exploitation. One FATF member has advised reporting entities to be increasingly alert to the exploitation of workers and trafficking in vulnerable persons. (Austrac, 2020[13])
- **Online Child Exploitation**: There are reports from some members of a rise in the production and distribution of online child exploitation material, often for profit. With the closure of schools, children are increasingly using the internet during "lockdown" periods, which could lead to an increase in online child exploitation. (FBI, 2020[14]) There are also reports that "lockdowns" and travel bans are increasing demand for this material. (Austrac, 2020[13])
- **Organised Property Crime**: With many properties currently uninhabited due to COVID-19, there are reports of an increase in organised property crime/theft. (Europol, 2020[15])

2.2. Other Contextual Factors and ML Vulnerabilities

Changing Financial Behaviours

Reporting indicates significant changes in financial behaviours and patterns in light of COVID-19. Many bank offices and branches are closed due to public health and "lockdown" measures. Customers are therefore carrying out more transactions remotely. Over the medium to long-term, an economic downturn could further alter financial activities and result in individuals seeking financing outside the formal economy.

- **Increased remote transactions**: FATF and FSRB members report that some banks have closed their physical branches, reduced opening hours or restricted the services available in-person. Members also report increased online banking activities, including customer on-boarding and identity verification. Some supervisors have clarified that, in line with a risk-based approach, banks can postpone certain elements of customer identity verification during confinement periods. However, FATF and FSRB members note that some financial institutions may not be equipped to verify customers' identity remotely.
- **Unfamiliarity with online platforms**: Certain population segments (e.g., the elderly, low-income groups, and remote or indigenous communities) may be less familiar with using online banking platforms, and therefore more susceptible to fraud. Reports indicate that online bank fraud targeting financial or account

[3] Human trafficking is defined in the *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime* as: the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

information is on the rise. (Cellule de Renseignement Financier Luxembourg, 2020[16])

- **Unregulated financial services**: Citing correlations with past economic downturns, both FATF and FSRB members note that, in a prolonged economic recession, those with financing needs may seek out non-traditional or unlicensed lenders, which may include criminal groups. Members also indicate that traditional financial gatekeepers may become pre-occupied with business continuity issues while still having to cope with monitoring suspicious transactions.

Misdirection of Government Funds or International Financial Assistance and Increased Risks of Corruption

Many governments are providing stimulus funds to mitigate the economic impact related to COVID-19. FATF and FSRB members report that criminals may try to fraudulently claim or misdirect such funds. Corruption in procurement or aid delivery channels could also impact international financial assistance.

- **Exploiting stimulus measures**: FATF and FSRB members report that a small proportion of economic support directed to businesses and individuals may present potential fraud risks, and consequent ML. In particular, criminals can falsely claim to provide access to stimulus funds to obtain personal financial information. (US IRS, 2020[17]) FATF members report that criminals may use legal persons to make fraudulent claims on government stimulus funds by posing as legitimate businesses seeking assistance. Some FATF members reported taking steps to reduce risks, such as disbursing aid to people and businesses via existing government accounts for receiving social benefits. (Australian Ministers for the Department of Social Services, 2020[18]) Stimulus measures that involve loan schemes may also be abused by criminals to launder funds.
- **International financial assistance and increased risks of corruption**: Many countries have an immediate need for emergency financial assistance to respond to COVID-19. However, international financial institutions report that there is a risk that emergency financial aid provided to countries can be misappropriated by corrupt officials, particularly in countries where the rule of law is weak and there are poor transparency and accountability measures. FSRB members also report that government contracts to purchase large amounts of COVID-19-related medical supplies provide opportunities for corruption and the misappropriation of public funds. This activity may become more prevalent if there is a perception of decreased financial oversight on government procurement and spending. FSRB members also indicate that individuals could use corruption or informal channels to obtain lucrative government contracts outside standard procurement procedures.

Increased Financial Volatility

Recent financial and economic volatility reflects uncertainties associated with COVID-19. In this context, opportunistic criminals may shift their activities to exploit new vulnerabilities.

- **Economic downturn**: In an economic downturn, criminals may seek to invest in real estate or troubled businesses to generate cash and mask illicit proceeds. Criminal groups can also introduce illicit proceeds into the financial system by restructuring existing loans and lines of credit. In addition, corporate insolvency proceedings can free up illicit cash contained in businesses whilst masking the

funds' origins. FATF members highlight that tax evasion and related crimes may increase as individuals and companies facing economic difficulties look to reduce their fiscal burdens. A prolonged economic downturn could result in private sector entities having fewer resources to combat ML/TF, thereby increasing their risks. Finally, increases in financial hardship due to an economic slowdown could lead to a rise in certain types of subsistence crimes in developing countries (e.g., burglary, theft and wildlife poaching).

- **Increased physical cash transactions**: FATF members report that recent swings in securities values are resulting in individuals liquidating their portfolios and transferring large amounts of funds electronically. FATF and FSRB members reported an overall increase in banknote withdrawals, with some FATF members raising cash withdrawal limits. FATF and FSRB members highlight that increased use of banknotes can mask ML/TF activities in the following ways:
    - When financial markets stabilise, large movements to re-deposit funds could provide cover to efforts at laundering illicit funds, including banknotes;
    - Banknotes can be used to purchase safe haven assets (e.g., gold), which are less easily traceable;
    - An increased risk of cash-out schemes, where criminals obtain access to an individual's bank account and withdraw funds in banknotes from an ATM; and
    - Customers involved in suspicious banknote withdrawals or transactions reference "COVID-19" as the transaction purpose, thereby masking potential illicit activities.
- **Virtual assets**: FATF and FSRB members highlighted the continuing ML/TF risks associated with virtual assets. In one recent case, an individual used virtual assets to launder proceeds earned from selling fraudulent COVID-19 medicine. (US Justice Department, 2020[19])
- **Insider trading**: Reporting indicates an increase in investor fraud due to increasingly volatile financial markets. Wholesale financial service providers are transferring or liquidating assets in securities markets in response to COVID-19-related uncertainties. These large value shifts in markets can potentially increase the risk of illicit financial market activities, such as insider trading that seeks to profit from large value swings. FATF members also report individuals using securities offerings to raise capital on fake products or medicines.

2.3. Financing of Terrorism

The United Nations has warned that threats related to terrorism remain and that terrorist groups may see opportunities for increased terrorist and terrorist financing activity while government attention is focused on COVID-19. (UN, 2020[20]) This is a particular concern in the Sahel region. One FSRB Secretariat and one FSRB member raised concerns about terrorist groups using the COVID-19 crisis to raise and move funds and increase existing illicit activity to finance their operations. As international humanitarian and aid responses to COVID-19 increase, governments should emphasise the importance of implementing the risk-based approach when mitigating the risk of funds being diverted to support terrorists and terrorist groups. (US Treasury, 2020[21])

2.4. Summary of Potential ML/TF Risks

Given the relatively early stages of the health and economic crisis, the majority of risks currently reported relate to proceeds generating predicate offences. ML/TF-specific trends or typologies emerging from COVID-19 are still in the early stages of identification. Nevertheless, some national authorities have indicated that their FIUs have begun issuing COVID-19-related typologies and indicators to their private sector.

At the time of writing, ML typologies relate to misuse of virtual assets to launder illicit proceeds and misuse of the formal banking system. No specific TF typologies related to COVID-19 have been reported by FATF or FSRB members.

In summary, and as outlined in the key findings, the potential ML/TF risks emerging from the aforementioned threats and vulnerabilities could be:

- Criminals finding ways to bypass CDD measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds;
- Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
- Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds;
- As individuals move money out of the banking system due to financial instability, this may lead to an increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds;
- Misuse and misappropriation of domestic and international financial aid and emergency funding by avoiding standard procurement procedures, resulting in increased corruption and consequent ML risks;
- Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries, both for the laundering of proceeds as well as to fund their operations, as well as fraudulently claiming to be charities to raise funds online.

3. Current COVID-19 impact on AML/CFT regimes

Open source research, as well as feedback received from members and FSRB Secretariats indicate that the COVID-19 pandemic is impacting government and private sectors' abilities to implement AML/CFT obligations. This is primarily due to confinement and social distancing measures introduced to contain the COVID-19 virus. Many AML/CFT government and private sector employees are now working remotely, have been redeployed to COVID-19 responses, or are not working at all. To some extent, especially for countries with more limited resources and less advanced business continuity planning, re-prioritisation efforts by governments are likely to result in a reallocation of resources away from AML/CFT activities to other areas, such as financial stability, and humanitarian and economic recovery efforts. There have been indications that some countries with less resilient AML/CFT regimes or resources may be unable to maintain AML/CFT operations while they prioritise responding to COVID-19.

The COVID-19 crisis appears to affect the following key areas, depending on the magnitude of a country's COVID-19 outbreak at the time of writing.

Supervision: The majority of FATF members indicate that their AML/CFT onsite inspections have been postponed or substituted with desk-based inspections (including the use of video conferencing). In some instances, onsite inspections are only conducted for high-risk sectors or entities. Respondents indicated that banks, financial institutions and other reporting entities continue to implement their AML/CFT requirements and provide requested information to their supervisors. Some supervisory authorities have indicated that they have provided risk-based flexibility on the filing of annual reports, and have delayed issuing new licenses, particularly for some sectors that may have been shut down, such as casinos (excluding online casinos). Regarding sanctions and other remedial actions, a number of countries have introduced suspensions on decisions, including imposing monetary penalties for AML/CFT violations. Registering new companies in registries is also delayed.

Regulation and policy reform: Many national, supranational and international policy departments have activated business continuity plans, with most or all staff working remotely or redeployed to respond to COVID-19. This has, in some jurisdictions, resulted in a significant pause in new AML/CFT policy and legislatives initiatives. This is further compounded by the suspension of meetings of some legislative decision-making bodies, or their prioritisation and focus on COVID-19 emergency matters.

Suspicious transaction reports (STRs): Banks and other reporting entities continue to file STRs. Some members indicated that financial institutions have not encountered delays or difficulties to analyse and file STRs. Other members are providing reporting entities extensions to submit STRs (except in the case of high-risk areas, such as TF) and threshold-based reports. In many cases, authorities have instructed reporting entities to expeditiously notify supervisors and/or financial intelligence units (FIU) if they encounter any delays or barriers to reporting. Jurisdictions that still rely on paper-based reporting systems, or that have inadequate database software, may face delays in receiving and processing reports.

FIU analysis: FIUs of FATF members, and FSRB members who responded are operational, even in those countries severely affected by COVID-19 at present. FIU staff are working remotely to the extent that information technology systems and security allow. There are some anecdotal reports that some FIUs in lower capacity countries are significantly reducing their operations or even shutting down completely.

International cooperation: There are mixed reports about the impact on operational cooperation due to the COVID-19 crisis. Some delegations expressed concern that delays in cooperation could be exacerbated over time due to remote working of FIU staff, and potential re-prioritisation efforts of law enforcement and supervisory authorities and within the private sector. Formal cooperation, such as mutual legal assistance and extradition are already impacted by the crisis due to the limitation or suspension of court operations, and the delayed execution of extradition orders caused by travel restrictions. Some delegations have reported that the provision of AML/CFT technical assistance has also been reduced or suspended.

Law Enforcement Authorities (LEAs): Limited feedback indicates that LEAs in FATF member countries continue to prioritise AML/CFT efforts, with a heightened focus on emerging COVID-19 predicate offences. Some prosecutions may be postponed or delayed due to the suspension of trials, hearings, and other in-person proceedings. There are some reports that the diversion of law enforcement and security resources to COVID-19 responses in high-risk, poorly resourced countries, may embolden terrorists and terrorist financiers in their activities.

Private Sector: Respondents noted that financial institutions have initiated business continuity plans in response to the crisis. Some banks are closing branches, facing

challenges at outsourcing centres, limiting their services and redeploying staff. There are reports from a few less affected countries that their banks are indirectly impacted and raised concerns about accessing information to conduct due diligence on foreign customers and foreign business relationships. Some members have flagged that there is increased activity in non-banking sectors like online gambling, the insurance sector, dealers in precious metals and stones and securities, while there is decreased activity in other sectors like casinos and real estate. The money value transfer service sector faces particular disruption as migrant workers have been affected by confinement measures and company shutdowns, and much of their business is done face-to-face. Should the current economic situation further deteriorate, there is a risk that financial institutions may re-prioritise their AML/CFT efforts and focus on broader prudential and stability measures.

4. Potential AML/CFT Responses for consideration

This section sets out a range of actions that jurisdictions are taking or could consider taking in response to these challenges, from dealing with new risks and/or reduced operational capacity to facilitating charitable activity, economic and fiscal stimulus and financial relief packages. It provides practical examples of responses taken by authorities.

Coordinate domestically to assess the impact of COVID-19 on AML/CFT risks and systems, to develop responses and engage with the private sector.

- Response teams are working with stakeholders to assess private and public sector resilience on a continuing basis (e.g., weekly situation reports).
- Supervisors, FIUs and LEAs are working together to identify, monitor and communicate the changing risk landscape (see Section 3) and provide guidance to the private sector.
- AML/CFT supervisors are engaging with prudential supervisors to ensure the appropriate prioritisation of AML/CFT measures to address potential illicit activity related to COVID-19 and its impact.

Strengthen communication with the private sector by proactively engaging on the application of their AML/CFT measures and working constructively with them to minimise potential impact.

- Supervisors and/or FIUs are providing regulated entities with a contact point where they face serious difficulties in meeting regulatory requirements and requiring them to keep relevant records and develop a plan to clear the backlog as the situation improves.
- Importantly, some countries are communicating beyond the financial sector, to designated non-financial businesses and professions, other trusted partners and industry associations, to address sectors that may have lower resilience.
- There are examples of some countries engaging proactively with the non-profit organisations (NPO) sector. Countries and financial institutions should apply a risk-based approach to ensure that legitimate NPO activity is not unnecessarily delayed, disrupted or discouraged. (FATF, 2015[22]) In one jurisdiction, the government has designated channels for COVID-19 donations.

Encourage full-use of a risk-based approach to CDD and address practical issues.

- Some supervisors are communicating with reporting entities about the importance of continuing to provide essential financial services while also

mitigating ML/TF risks by using the full range of tools at their disposal. In relation to CDD, supervisors have put in place some of the following measures:

- Applying simplified due diligence measures where lower risks are identified, for example, accounts created specifically to facilitate government payments to individuals or businesses and offering access to digital/contactless payment solutions.[4] See below section on economic relief packages.
- Providing guidance that there may be legitimate reasons for customers not providing information for ongoing due diligence or 'know-your-customer (KYC) refreshers' (e.g., if they are confined, under quarantine or ill) and that the usual processes for dealing with these situations (including exiting the customer relationship) may not be appropriate at this time.[5]
- Allowing reporting entities to accept recently expired government-issued identification until further notice in order to verify the identity of an individual (although still required to determine the authenticity of the identification).
- Considering the application of delayed verification provisions for new business relationships in line with the FATF Standards (e.g., by implementing transaction limits). Reporting entities can accept digital copies of documents as an interim measure, with the originals to be sighted in due course.

- Encouraging the use of responsible digital identity and other responsible innovative solutions for identifying customers at onboarding and while conducting transactions. See the recent FATF Digital ID Guidance (FATF, 2020[23]) that highlights that non-face-to-face onboarding and transactions conducted using trustworthy digital ID are not necessarily high-risk and can be standard or even lower-risk.

Support electronic and digital payment options.

- More broadly, supervisors are encouraging the full use of electronic and digital channels to continue payment services while maintaining social distancing. Some examples include increasing contactless limits, increasing point of sale purchase limits, raising maximum limits for e-wallets and reducing charges for domestic money transfers between banks to encourage the use of contactless payment methods in order to reduce the spread of the virus.

Undertake pragmatic, risk-based AML/CFT supervision.

- All supervisors have continued AML/CFT supervisory activities, although practices are adapted to be more pragmatic in the current situation (see Section 4).
- Supervisors continue to monitor the business continuity plans put in place and operationalised by financial institutions in order to ensure their sound operations, including implementation of AML/CFT measures. Some supervisors are adjusting their focus as relevant. For example, they are putting greater focus on online casinos and gambling platforms considering regular casinos and gambling arcades are closed, and more focus on dealers in precious metals and stones with greater investment in gold.

[4]FATF Interpretative Note to R.10 notes that "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes" are an example of a lower risk scenario.

[5]More information on how such measures can be implemented is set out in the 2017 FATF guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence.

- Conversely, there is potentially less focus on lower risk areas such as cash-intensive businesses that have halted trading. All supervisors should consider reviewing their supervisory priorities and plans and adjust these to emerging risks, as necessary.

Understand new risks and adapt operational responses.

- Authorities are working with relevant partners, domestically and internationally, to understand and monitor the evolving risk environment (see Section 3). This requires liaising with a broad range of stakeholders. Countries with existing public/private partnerships are harnessing these forums to obtain the latest information.
- A number of countries have introduced special taskforces or other operational coordination measures to deal with COVID-19-related crime, particularly in relation to fraud.
- In some countries, authorities have issued advice to relevant agencies on the prioritisation of investigations and prosecutions.
- Some FIUs have asked regulated entities to use a keyword in their reports to triage and prioritise incoming STRs. FIUs are developing strategic analysis based on review of available bulk data and adapting STR prioritisation and analysis.
- Agencies are considering pooling available resources, including repurposing assets confiscated or forfeited from criminals to assist in COVID-19 responses (e.g., using confiscated properties as temporary/emergency hospital facilities).

Clarify AML/CFT requirements in the context of economic relief measures.

- Authorities are providing clarity on how to apply AML/CFT requirements in the context of economic relief packages for individuals and businesses.
- To facilitate the smooth processing of applications, some supervisors have approved simplified due diligence measures (including for customer verification) for transactions under government assistance programs where they are assessed to present lower risks. They include obligations for regulated entities to put in place mitigation measures, such as ongoing due diligence and to review CDD if other risks are later detected.
- One country has implemented measures to identify risk indicators, and implemented processes and controls to prevent the misuse of the aforementioned assistance packages for ML/TF purposes. These measures will likely vary depending on the scope and delivery of the relief package and contextual factors, including corruption issues.
- Countries receiving economic stimulus by international organisations such as the IMF may receive additional guidance to implement targeted AML/CFT measures to ensure those funds are not diverted for other purposes (such as corruption or ML).
- All countries should guide regulated entities to remain vigilant to detect suspicious financial transactions, particularly in the context of cross-border flows from countries that are receiving emergency COVID-19-related funding from international organisations and other donors.

Continue cooperating across borders.

- FIUs should keep the Egmont Group Secretariat appraised of any developments, including any operational disruptions that could impact international cooperation responses and provide a key contact point.
- Increased communication may be required, particularly on group-wide supervision.

Monitor the impact of COVID-19 on the private sector.

- FIUs and supervisors should continue to monitor the impact on reporting entities, as the COVID-19 situation continues.
- Prolonged economic disruption may force some regulated entities to close down. Disorderly shutdowns may leave significant ML/TF vulnerabilities.

Annex A. Statement by the FATF President

COVID-19 and measures to combat illicit financing[6]

Paris, 1 April 2020 - The members of the FATF, both domestically and multilaterally, are applying every available resource to combat the COVID-19 pandemic. As the global standard-setter for combating money laundering (ML) and the financing of terrorism (TF) and proliferation, the FATF encourages governments to work with financial institutions and other businesses to use the flexibility built into the FATF's risk-based approach to address the challenges posed by COVID-19 whilst remaining alert to new and emerging illicit finance risks. The FATF encourages the fullest use of responsible digital customer onboarding and delivery of digital financial services in light of social distancing measures. At a time when critical relief is needed in-country and beyond, effective implementation of the FATF Standards fosters greater transparency in financial transactions, which gives donors greater confidence that their support is reaching their intended beneficiaries. The continued implementation of the FATF Standards facilitates integrity and security of the global payments system during and after the pandemic through legitimate and transparent channels with appropriate levels of risk-based due diligence.

Addressing COVID-19-related financial crime risks by remaining vigilant

Criminals are taking advantage of the COVID-19 pandemic to carry out financial fraud and exploitation scams, including advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, and engaging in phishing schemes that prey on virus-related fears. Malicious or fraudulent cybercrimes, fundraising for fake charities, and various medical scams targeting innocent victims are likely to increase, with criminals attempting to profit from the pandemic by exploiting people in urgent need of care and the goodwill of the general public and spreading misinformation about COVID-19. National authorities and international bodies are alerting citizens and businesses of these scams, which include impostor, investment and product scams, as well as insider trading in relation to COVID-19. Like criminals, terrorists may also exploit these opportunities to raise funds.

Supervisors, financial intelligence units and law enforcement agencies should continue to share information with the private sector to prioritise and address key ML risks, particularly those related to fraud, and TF risks linked to COVID-19. Additionally, criminals and terrorists may seek to exploit gaps and weaknesses in national anti-money laundering/counter-financing of terrorism (AML/CFT) systems while they assume resources are focused elsewhere, making risk-based supervision and enforcement activity more critical than ever. Financial institutions and other businesses should remain vigilant to emerging ML and TF risks and ensure that they continue to effectively mitigate these risks and are able to detect and report suspicious activity.

Digital onboarding and simplified due diligence

With people around the world facing confinement or strict social distancing measures, in-person banking and access to other financial services is difficult, and unnecessarily exposes people to the risk of infection. Use of digital/contactless payments and digital onboarding reduce the risk of spreading the virus. As such, the use of financial technology (Fintech) provides significant opportunities to manage some of the issues presented by COVID-19. In line with the FATF Standards, the FATF encourages the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible. The FATF recently

[6] www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html

released Guidance on Digital ID, which highlights the benefits of trustworthy digital identity for improving the security, privacy and convenience of identifying people remotely for both onboarding and conducting transactions while also mitigating ML/TF risks. The FATF calls on countries to explore using digital identity, as appropriate, to aid financial transactions while managing ML/TF risks during this crisis.

When financial institutions or other businesses identify lower ML/TF risks, the FATF Standards allow them to take simplified due diligence measures, which may help them adapt to the current situation. The FATF encourages countries and financial service providers to explore the appropriate use of simplified measures to facilitate the delivery of government benefits in response to the pandemic.

Delivery of aid through non-profit organisations

This global public health emergency has highlighted the vital work of charities and NPOs to combat COVID-19 and its effects. The FATF has long recognised the vital importance of NPOs in providing crucial charitable services around the world, as well as the difficulties in providing that assistance to those in need. The FATF has worked closely with NPOs over the years to refine the FATF Standards to provide flexibility to ensure that charitable donations and activity can proceed expeditiously through legitimate and transparent channels and without disruption. It is important to recognise that FATF Standards do not require that all NPOs be considered high-risk and that most NPOs carry little or no TF risk. The aim of the FATF Standards is not to prevent all financial transactions with jurisdictions where there may be high ML/TF risks, but rather to ensure these are done through legitimate and transparent channels and money reaches its legitimate intended recipient. National authorities and financial institutions should apply a risk-based approach to ensure that legitimate NPO activity is not unnecessarily delayed, disrupted or discouraged. FATF encourages countries to work with relevant NPOs to ensure that much needed aid is getting to its intended recipients in a transparent manner.[7]

Ongoing outreach and advice

Regulators, supervisors, financial intelligence units, law enforcement authorities and other relevant agencies can provide support, guidance and assistance for the private sector on how national AML/CFT laws and regulations will be applied during the current crisis. Such guidance can give financial institutions and other businesses reassurance that the authorities share their understanding of challenges and risks involved in the current situation, and of the appropriate actions to take. Authorities in some countries have already taken swift action and provided this type of advice. Mechanisms by which victims, financial institutions, and other businesses can report COVID-19 related fraud may be especially useful.

At the international level, the FATF is working with the Committee on Payment and Market Infrastructures and the World Bank to help ensure coordinated policy responses for the continued provision of critical payment services against the backdrop of the COVID-19 crisis. The FATF, International Monetary Fund, World Bank, and United Nations are working with their membership to mitigate the impacts of the COVID-19 crisis, including through the use of AML/CFT measures, where relevant. In addition, the FATF is working with its members and the FATF-Style Regional Bodies to identify and share good practices in response to common issues faced in many affected countries.

FATF's commitment to support efforts to address COVID-19 issues

The FATF stands ready to provide further AML/CFT guidance to support the current global efforts to tackle the COVID-19 crisis and its effects, and welcomes feedback.

[7] See 2015 Best Practices Paper on Combating the Abuse of Non-Profit Organisations

Annex B. Statement or guidance issued by authorities in response to COVID-19

Below are statements and guidance issued by FATF and FSRB members in response to COVID-19. The measures cited, and taken by FATF members' authorities, have not been reviewed or considered by the FATF membership as a whole, and therefore do not constitute the official view of the FATF.

- **Anguilla** –The FIU has issued a public release to the reporting entities as well as the general public on the risk of potential scams/fraud.
- **Australia** – AUSTRAC updates to reporting entities on COVID-19 including advice and guidance on: working with reporting entities during COVID-19 pandemic, extension on annual compliance reporting, advice on rule changes for early access to superannuation funds, suspicious matter reporting and advice on meeting KYC requirements:

  https://www.austrac.gov.au/covid-19-updates.
- **Bolivia** – The UIF (FIU Bolivia) issued an official communication addressed to reporting entities on COVID-19 pandemic risk on ML/TF to advise them on how to better comply with their AML/CTF obligations.

  http://www.uif.gob.bo/.
- **Brazil** – COAF has replicated the FATF and GAFILAT communiqués in Portuguese and published in its web-site. Furthermore, it addressed these statements together with red flags to all reporting entities, supervisors and other competent authorities.

  https://www.fazenda.gov.br/orgaos/coaf/publicacoes/comunicado-do-presidente-do-gafi-sobre-covid-19-e-medidas-de-combate-ao-financiamento-ilicito
- **Canada** – FINTRAC message to all reporting entities in light of COVID-19:

  https://www.fintrac-canafe.gc.ca/covid19/covid19-eng
- **Cayman Islands** –The FRA (FIU) has published and circulated notices regarding the physical closure of the office and guidance on how reporting entities should submit reports during the physical closure of the office.
- **Chile** – UAF has issued several communiqués and press release addressed to the reporting entities in order to inform and guide them to better comply with the AML/CTF obligations during this COVID-19 pandemic situation. This agency also issue communiqués addressed to all relevant authorities, and a social media campaign to raise awareness on the ML/TF risk associated to the pandemic was also launched (https://twitter.com/UAF_Chile).

  https://www.uaf.cl/ArchivoEstatico/carta_so_covid.pdf

  https://www.uaf.cl/prensa/archivo_det.aspx?id=576

  https://www.uaf.cl/prensa/archivo_det.aspx?id=574

  https://www.uaf.cl/prensa/archivo_det.aspx?id=573
- **People's Republic of China** – The Peoples Bank of China (PBC) has issued Notices on AML/CFT requirements in responding to the COVID-19 pandemic to all its branches on 5th Feb 2020. All branches of PBC should continue more pragmatic

AML/CFT supervisory activities adapted to local situation and provide necessary guidance to local regulated entities when they face difficulties in meeting regulatory requirements;

PBC has also issued Guidance on how to meet the AML/CFT requirements in responding to the COVID-19 pandemic to regulated entities on 5th Feb 2020. All regulated entities are encouraged to develop contingency program meeting the AML/CFT requirements by using the full range of tools at their disposal. To support charitable activity and medical aid, simplified due diligence measures are allowed but the STR of TF and the other high-risk areas should be maintained overall.

- **Colombia** – UIAF issued a press release sent to all compliance officers and published it on its website, requesting greater rigor in CDD measures, in the context of the health emergency caused by COVID-19 pandemic. UIAF has also replicated the GAFILAT communiqué in its web-site and carried out a social media campaign to boost all the stakeholders to continue to rigorously implement AML / CFT risk management systems (https://twitter.com/UIAFColombia #YoNoBajoLaGuardia**)**.

  https://www.uiaf.gov.co/caracterizacion_usuario/slide_home/_30420

  https://www.uiaf.gov.co/sala_prensa/noticias_comunicados/la_actual_coyuntura_exige_se_sigan_30457

  https://www.uiaf.gov.co/sala_prensa/noticias_comunicados/comunicado_gafilat_covid_19_sus_30438

- **Costa Rica** – The FIU/ICD issued a statement to all relevant authorities and the reporting entities to guide them on the ML/TF risk associated with COVID-19 and to advise them on possible good practices:

  http://www.icd.go.cr/portalicd/images/docs/uif/ALACFT/Comunicado_a_la_Red_Global_ALACFT.pdf.

- **Cuba** – The Central Bank of Cuba has issued communiqués in line with the FATF's and GAFILAT's statement on COVID-19 and its associated ML and FT risks to raise awareness of the reporting entities and the public sector on this matter.

- **Denmark, Kingdom of** – FSA Fighting money laundering and terrorist financing must continue during the Covid-19 crisis: https://www.dfsa.dk/News/Press-releases/2020/Fighting_money_laundering_covid19.

- **Dominican Republic** – To prevent citizens from being scammed during the Covid-19 emergency, information campaigns are carried out in order to inform the population about the channels and mechanisms to receive financial aid programs. In the official websites of the relevant organizations, specific sections have been created for said programs, which are reported by press and social media.

  https://www.hacienda.gob.do/ministerio-de-hacienda-informa-cambio-para-aplicar-al-fase/

  https://www.quedateencasa.gob.do

  http://vicepresidencia.puntosolidario.gob.do/

- **EGMONT Group** - The ECOFEL eLearning platform - accessed by FIUs and other competent authorities from all over the world - now hosts a large quantity of

reports and other content related to ML/TF threats and vulnerabilities arising from COVID-19 outbreak, including the online course "COVID-19 emerging risks".

Furthermore, the ECOFEL will soon start organizing round-table discussions that will bring together the FIUs from jurisdictions that are experiencing different stages of COVID-19 outbreak, in order to share their experiences and lessons learned as to how to tackle the relevant managerial and operational issues they face and prepare the FIUs to efficiently return to a normal operational routine once the lockdown decisions by governments are lifted.

- **Egypt** – Guidance issued by the Central Bank of Egypt on bank operations during COVID-19 on 20 March 2020.
- **European Banking Authority** – Statement on actions to mitigate financial crime risks in the COVID-19 pandemic:

  https://eba.europa.eu/eba-provides-additional-clarity-on-measures-mitigate-impact-covid-19-eu-banking-sector.
- **Europol** – press release and report on pandemic profiteering: how criminals exploit the COVID-19 crisis:

  https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic.
- **Finland** – FIU-FI disseminated an alert to reporting entities concerning the possible typologies related to COVID -19 on 26 March 2020.
- **France** – Joint communiqué by financial supervisor (ACPR-AMF) on the scam financial risks related to Covid-19 (in French):

  https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/lamf-et-lacpr-mettent-en-garde-le-public-contre-les-risques-darnaques-dans-le-contexte-de-lepidemie.

  Statement of ACPR (France's main financial supervisor) as regards the continuity of its mission and adaptation during the crisis (in French):

  https://acpr.banque-france.fr/communique-de-presse/lautorite-de-controle-prudentiel-et-de-resolution-assure-la-continuite-de-ses-missions-durant-la.

  Confirmation that asset freezing obligations and STR reporting cannot be granted any exceptions during the crisis (bill) (in French):

  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041800899&categorieLien=id.

  Statements issued on extension of deadlines for reporting AML-CFT obligations for:

  Banking sector (in French):

  https://acpr.banque-france.fr/communique-de-presse/lautorite-de-controle-prudentiel-et-de-resolution-annonce-un-assouplissement-des-modalites-de-remise;

  Insurance sector (in French):

  https://acpr.banque-france.fr/communique-de-presse/lautorite-de-controle-prudentiel-et-de-resolution-annonce-un-assouplissement-des-dates-de-remise-des;

  Portfolios management sector (in French):

https://www.amf-france.org/fr/actualites-publications/actualites/continuite-des-activites-de-gestion-en-periode-de-coronavirus.

- **GAFILAT**– The heads of delegations, together with the Presidency and the Executive Secretariat of GAFILAT, approved an official statement on COVID-19 and its associated ML and FT risks. The document was developed with the inputs received from the member countries and in accordance with the measures reported by FATF. This statement attempts, on the one hand, to alert the authorities of the member countries and the private sector about possible emerging risks and, on the other hand, to share good practices and mitigating measures identified in response to the common problems faced by the GAFILAT's member countries and the international community.

  https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/3823-gafilat-covid19-en-gafilat/file

- **Germany** – BaFin information on new developments and key points on the COVID-19 situation (in English and German):

  https://www.bafin.de/EN/Aufsicht/CoronaVirus/CoronaVirus_node_en.html;

  https://www.bafin.de/DE/Aufsicht/CoronaVirus/CoronaVirus_node.html.

- **Guatemala** – SIB, (FI's regulator) issued statements related to financial supervision on AML/CTF and to the use of cash in order to prevent and mitigate the possible ML/TF risk emerging from the CODIV-19 pandemic situation.

  https://www.sib.gob.gt/c/document_library/view_online_get_file?folderId=6762386&name=DLFE-35734.pdf

  https://www.sib.gob.gt/c/document_library/view_online_get_file?folderId=6762638&name=DLFE-35740.pdf

- **Guernsey** - The Guernsey Financial Services Commission has issued press releases emphasizing to the financial services and DNFBP community the importance of operational resilience in the face of increased fraud risk (including cybercrime) arising from Covid-19 measures being taken domestically and worldwide, and on encouraging regulated firms to move to electronic customer verification measures. Consumers have also been alerted to various types of potential Covid-19 scams.

  https://www.gfsc.gg/news/article/commission-warns-licensees-increased-risk-fraud-arising-covid-19

  https://www.gfsc.gg/news/article/coronavirus-update-2-–-commission-support-financial-services-industry

- **Honduras** – UIF, has published on its website, the statement issued by GAFILAT in this regard, as well as the document issued by the United Nations Office on Drugs and Crime (UNODC) on Cybercrime and COVID-19. These documents were shared with the compliance officers of the reporting entities, so that they can use them as a tool to identify possible risks.

  http://pplaft.cnbs.gob.hn/blog/2020/04/30/el-covid-19-problemas-actuales-y-futuros/

  http://pplaft.cnbs.gob.hn/

- **Hong Kong, China** – Hong Kong Monetary Authority guidelines for financial institutions:

https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200407e1.pdf;

https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200407e2.pdf.

- **Isle of Man** - The regulators and the financial intelligence unit in the Isle of Man have published statements providing guidance to the regulated sector on potential risks, and also setting out expectations of the regulators, during COVID-19:

  https://www.iomfsa.im/covid-19/

  https://www.gov.im/categories/business-and-industries/gambling-and-e-gaming/

  https://www.fiu.im/fiu-covid-19-response/

- **Israel** - The Israeli National Police, IMPA (the Israeli FIU), the Bank of Israel (Banking Supervision Division), the Israel Securities Authority and the Israeli Capital Markets, Insurance and Savings Authority have published notices to reporting entities and the public, concerning specific risks arising in connection with the COVID-19 crisis.

- **Italy** – At the outset of the lockdown, Unità di Informazione Finanziaria per l'Italia – UIF provided obliged entities in all relevant sectors with indications on how to maintain appropriate contacts for any communications, disclosures or requests and for facilitating compliance: https://uif.bancaditalia.it/pubblicazioni/comunicati/documenti/Contatti_lavoro_a_distanza.pdf.

  With a second Communiqué UIF indicated the need to leverage IT tools to identify suspicions through remote screening. Also, based on an assessment of the impacts of the emergency, the terms for the filing of certain data related to threshold-based disclosures have been prolonged: https://uif.bancaditalia.it/pubblicazioni/comunicati/documenti/Comunicato_UIF_Covid19.pdf.

  Furthermore, UIF has set out to monitor developing trends and identify emerging threats and vulnerabilities, with a view to highlighting areas of risk and providing obliged entities with indicators for the detection of suspicious transactions in the context of the emergency. In the wake of initiatives undertaken by the FATF and European bodies and of similar measures adopted by counterparts in other jurisdictions, UIF issued on 16 April a Communiqué drawing the attention of AML/CFT obliged entities and their staff to the new threats and risks to which they may be exposed and to the need to promptly detect suspicions related to the Covid-19 emergency and report them: https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione-UIF-16.04.2020.pdf.

  On April 10, 2020 Banca d'Italia issued a communication to banks and financial intermediaries drawing the attention on the central role of the financial system to transmit the effects of governmental measures, and to avoid detrimental impacts on clients. In this framework, Banca d'Italia also issued recommendations on the implementation of anti money laundering safeguards, recalling to calibrate AML obligations according to the emerging ML/TF risks associated with COVID-19. In this respect, specific attention is requested in order to prevent misuse of financial public aid to individuals and corporations:

https://www.bancaditalia.it/compiti/vigilanza/normativa/orientamenti-vigilanza/Comunicazione-intermediari-aprile.pdf

- **Japan** – Consumer Affairs Agency & National Police Agency advice public to be aware of COVID-19 related frauds (in Japanese):

  https://www.npa.go.jp/bureau/soumu/corona/index_corona_special.html;

  https://www.caa.go.jp/policies/policy/consumer_policy/information/notice_200227.html.

- **Jersey** - The Jersey FSC has issued guidance and launched a series of webinars about working in the pandemic, including a specific webinar on the subject of customers due diligence.

  https://www.jerseyfsc.org/news-and-events/webinar-covid-19-implications-on-customer-due-diligence/

  https://player.vimeo.com/video/411514721?autoplay=0&loop=1

- **Republic of Korea** – KoFIU has issued guidance for reporting entities on STR reporting requirements during the crisis.

- **Luxembourg** – the FIU (CRF) has published a COVID-19 typologies report: https://justice.public.lu/dam-assets/fr/organisation-justice/crf/2020-04-02-COVID19-EN.pdf (in English);

  https://justice.public.lu/dam-assets/fr/organisation-justice/crf/note-covid19-1.pdf (in French).

- **Mexico** – FIU and the National Banking and Securities Commission (CNBV) Joint statement to regulated entities; CNBV statement on prudential and AML/CFT requirements; FIU and Tax and Customs Authority joint statement for DNFBPs (all public documents and in Spanish). In addition, the FIU and the CNBV shared with the financial entities a non-public document about the ML and TF Risks related to COVID-19:

  https://uif.gob.mx/work/models/uif/imp/AVISO_UIFMARZO.pdf;

  https://www.dof.gob.mx/nota_detalle.php?codigo=5590567&fecha=26/03/2020;

  https://uif.gob.mx/work/models/uif/imp/ComunicadoCOVID19.pdf.

- **Morocco** – Bank Al-Maghrib has issued a press release on measures taken during COVID-19 on 29 March 2020.

- **Namibia** – FIU public statement on COVID-19 lockdown and public alert on COVID-19 scams:

  https://www.fic.na/uploads/Public_Awareness/General_Publications/COVID-19%20%E2%80%93%20National%20Lockdown.pdf;

  https://www.fic.na/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=321&cntnt01showall=&cntnt01pagelimit=25&cntnt01returnid=76.

- **Netherlands, Kingdom of** – The FIU has issued an information leaflet to all reporting entities, informing them on how they can identify specific financial COVID-benefits paid by the Dutch government, on possible misuse situations and on possible red flags related to COVID-19 fraud cases. These red flags have been developed in cooperation with the several public authorities (Anti Money Laundering Centre, Inspectorate SZW (Social Affairs and Employment) and Public

Prosecutors Office). An interview with more details on the information leaflet can be found here: https://www.moneylaundering.com/news/dutch-fiu-chief-warns-of-covid-19-fraud-and-money-laundering/?type=free.

DNB (the central bank) and AFM (the Dutch Financial Markets Authority) have issued several notifications:

https://www.dnb.nl/consumenten/corona/dnb388001.jsp (DNB, overview page)

https://www.dnb.nl/en/news/dnb-nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-april-2020/index.jsp (DNB, April 6, 2020)

https://www.afm.nl/nl-nl/nieuws/2020/april/eba-witwassen (AFM, April 1, 2020).

Dutch National Police has issued a warning on cybercriminals taking advantage of corona-related measures:

https://www.politie.nl/nieuws/2020/maart/17/cybercriminelen-misbruiken-maatregelen-rondom-corona.html.

- **New Zealand** – Joint guidance by three supervisory agencies:

  https://www.dia.govt.nz/diawebsite.nsf/Files/AML-CFT-2020/$file/aml-cft-supervisor-guidance-covid-19-alert-26-march-2020.pdf.

- **Nicaragua** – The AML/CTF/PF National Committee has replicated the public documents that the FATF / GAFILAT have published on COVID-19 and its risks associated with ML/TF in order to analyze and evaluate the emerging risks that may result in this context.

- **Palestinian Authority** – Palestine Monetary Authority issued Circulate No. (84/2020) for Specialized Lending Institutions Operating in Palestine; Circulate No. (85/2020) for Banks Operating in Palestine; Circulate No. (86/2020) for Money Exchangers Operating in Palestine on 26 March 2020.

- **Paraguay** – SEPRELAD issued a press release and guidance addressed to the relevant private and public sector in order to alert them on ML/TF related emerging risks.

  http://www.seprelad.gov.py/gafilat-informa-sobre-el-covid-19-y-sus-riesgos-asociados-de-lavado-de-activos-y-financiamiento-del-terrorismo-n108

- **Peru** – The SBS published several communiqués and press release addressed to reporting entities and the public, concerning specific risks arising connected with the COVID-19 pandemic.

  https://www.sbs.gob.pe/prevencion-de-lavado-activos/Noticias-Comunicados-SBS/noticia/gafilat-difunde-comunicado-sobre-covid19--y-sus-riesgos-asociados-de-lavado-de-activos-y-financiamiento-del-terrorismo/id/1607

  https://www.sbs.gob.pe/prevencion-de-lavado-activos/boletines-informativos

  https://www.sbs.gob.pe/Portals/5/jer/BOLETIN-INFORMATIVOS/2020/Boletin_covid19.pdf

- **Portugal** – Statements by supervisors:

  https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/bo3_2020_s.pdf;

https://www.bportugal.pt/comunicado/comunicado-sobre-os-documentos-emitidos-pela-eba-e-pelo-gafi-no-contexto-da-pandemia;

https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/bo_4_2020s.pdf;

https://www.cmvm.pt/en/Comunicados/communiques/Pages/20200320mc3.aspx?v=;

https://www.cmvm.pt/pt/Legislacao/Legislacaonacional/Circulares/Documents/Circular_PAI_covid_20200330.pdf;

https://www.cmvm.pt/pt/Legislacao/Legislacaonacional/Recomendacoes/Pages/rec_auditoria_2020.aspx?v=;

https://www.asf.com.pt/NR/exeres/DCEA4D59-33B9-4149-91A3-384160BDC805.htm;

https://www.asf.com.pt/NR/rdonlyres/58DAE1BA-D274-4C2D-87C5-ED043E9A0784/0/CartaCircularnr42020.pdf.

- **Saudi Arabia** – SAMA provided guidance to regulated entities.
- **Seychelles** – Advisory from the FIU and Financial Services Authority statement on COVID-19 to reporting entities:

  https://www.seychellesfiu.sc/FIU/?p=1109;

  https://www.fsaseychelles.sc/wp-content/uploads/2020/03/Communique-COVID19.pdf.

- **Singapore** – The Singapore Police Force (SPF) and AML/CFT authorities (e.g. Monetary Authority of Singapore) have provided guidance and advisories to regulated entities and the public respectively. SPF has issued an advisory warning of a new type of e-commerce scam involving sale of face masks:

  https://www.police.gov.sg/media-room/news/20200222_others_new_type_of_ecommerce_scams_involving_the_sale_of_face_masks.

  SPF also regularly shares news on types of scams, including those relating to COVID-19, via www.scamalert.sg/news.[8]

  The Ministry of Law has issued a statement to all Registered Dealers, describing government-wide measures taken in response to Covid-19:

  https://acd.mlaw.gov.sg/news/notices/remain-vigilant-during-covid-19.

  The Monetary Authority of Singapore has been providing guidance to financial institutions on risks and expectations of regulators and supervisors during COVID-19:

  https://www.mas.gov.sg/news/media-releases/2020/mas-takes-regulatory-and-supervisory-measures-to-help-fis-focus-on-supporting-customers.

- **Spain** – SEPBLAC public message:

  https://www.sepblac.es/en/2020/03/18/covid-19/.

[8] Recent advisories on scams include one where Singapore Prime Minister Lee Hsien Loong warns of fake COVID-19 emails purportedly sent by him asking for "contributions" and the Ministry of Health's warning of scammers impersonating its COVID-19 contact tracing personnel to request for personal information and financial details.

Bank of Spain public releases on COVID 19:

https://www.bde.es/bde/en/Home/Noticias/covid-19/

CNMV public releases on COVID 19:

http://www.cnmv.es/portal/gpage.aspx?id=COVID19

- **Sweden** – Police advice to general public:

  https://polisen.se/aktuellt/nyheter/2020/mars/forandrade-brottsmonster-till-foljd-av-coronaviruset/.

- **Trinidad and Tobago** – Guidance has been issued to reporting entities on filing STRs using online secure reporting solutions and on CDD for on-boarding customers using digital identification (online at: www.fiu.gov.tt) and (issued notifications on COVID-19 scams (online at: https://www.fiu.gov.tt/wp-content/uploads/COVID19-SCAM.pdf).

- **United Kingdom** –

  Law Enforcement Agencies have produced threat assessment and published advice on the risk of Covid-19 fraud:

  https://nationalcrimeagency.gov.uk/news/fraud-scams-covid19.

  The Financial Conduct Authority (FCA) CEO has written to the CEOs of firms providing services to retail investors with advice and detail of the FCA's response to Covid-19:

  https://fca.org.uk/publication/correspondence/dear-ceo-letter-coronavirus-update-firms-providing-services-retail-investors.pdf.

  The Institute for Chartered Accountants of England and Wales (ICAEW) has published advice for its firms on how they can continue to meet their AML/CTF obligations:

  https://www.icaew.com/-/media/corporate/files/technical/legal-and-regulatory/money-laundering/coronavirus-guide-aml-responsibilities.ashx.

- **United Nations Office on Drugs and Crime** –

  Money Laundering and Covid-19: Profit and Loss:

  https://www.unodc.org/documents/Advocacy-Section/UNODC_-_MONEY_LAUNDERING_AND_COVID19_-_Profit_and_Loss_v1.1_-_14-04-2020_-_CMLS-COVID19-GPML1_-_UNCLASSIFIED_-_BRANDED.pdf

- **United States** –

  FBI's coronavirus reference site urging diligence (continually updated): https://www.fbi.gov/coronavirus

  FinCEN press release, FinCEN Encourages Financial Institutions to Communicate Concerns Related to COVID-19 and to Remain Alert to Related Illicit Financial Activity:

  https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions;

  https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial.

  US Department of Justice memorandum and press release:

https://www.justice.gov/ag/page/file/1258676/download;

https://www.justice.gov/opa/pr/attorney-general-william-p-barr-urges-american-public-report-covid-19-fraud.

FDIC Chairman's Statement, FDIC Chairman Addresses FSOC; Underscores Banks and Deposits Remain Safe; FDIC Frequently Asked Questions, For Financial Institutions and Consumers Affected by the Coronavirus:

https://www.fdic.gov/news/news/press/2020/pr20040.html;

https://www.fdic.gov/news/news/financial/2020/fil20018.pdf.

Federal Reserve Board Press Releases: Federal Reserve Statement on Supervisory Activities, Federal Reserve provides additional information to financial institutions on how its supervisory approach is adjusting in light of the coronavirus:

https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200324a1.pdf;

https://www.federalreserve.gov/newsevents/pressreleases/bcreg20200324a.htm

Office of the Comptroller of the Currency Bulletin 2020-34: Bank Secrecy Act/Anti-Money Laundering, OCC Supports FinCEN's Regulatory Relief and Risk-Based Approach for Financial Institution Compliance in Response to COVID-19:

https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-34.html.

US Department of the Treasury, press release, Treasury Underscores Commitment to Global Flow of Humanitarian Flow of Humanitarian Aid in Face of COVID-19 Pandemic:

https://home.treasury.gov/news/press-releases/sm969

U.S. Department of the Treasury, Fact Sheet, Provision of Humanitarian Assistance and Trade to Combat COVID-19:

https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20200416.aspx

U.S. Department of the Treasury, Statement, Office of Foreign Assets Control (OFAC) Encourages Persons to Communicate OFAC Compliance Concerns Related to the Coronavirus Disease 2019 (COVID-19): https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20200420.aspx

U.S. Department of the Treasury, Information and FAQs for lenders of relief packages:

https://home.treasury.gov/policy-issues/cares/assistance-for-small-businesses

- **Uruguay** – SENACLAFT has published the GAFILAT statements on the ML/TF risks emerging from the COVID-19 pandemic and the possible measures to mitigate them.

  https://www.gub.uy/secretaria-nacional-lucha-contra-lavado-activos-financiamiento-terrorismo/comunicacion/noticias/comunicado-del-gafilat-sobre-covid-19-riesgos-asociados-lavado-activos

- **Zimbabwe** – FIU notice to banks on business continuity arrangements during the national 'lockdown'.

References

Austrac (2020), *Fighting Financial Crime Together – SMRs during the COVID-19 Pandemic*, https://www.austrac.gov.au/smrs-during-covid-19. [13]

Australian Ministers for the Department of Social Services (2020), *Economic Stimulus Scammers Will Be Caught*, https://ministers.dss.gov.au/media-releases/5636. [18]

Cellule de Renseignement Financier Luxembourg (2020), *Typologies COVID-19.*, https://justice.public.lu/dam-assets/fr/organisation-justice/crf/2020-04-02-COVID19-EN.pdf. [16]

CISA (2020), *COVID-19 Exploited By Malicious Cyber Actors*, http://www.us-cert.gov/ncas/alerts/aa20-099a. [8]

Council of Europe (2020), *In Time of Emergency the Rights and Safety of Trafficking Victims Must be Respected and Protected*, https://rm.coe.int/greta-statement-covid19-en. [11]

European Commission (2020), *Launches Enquiry into Fake COVID-19 Related Products*, https://ec.europa.eu/anti-fraud/media-corner/news/20-03-2020/olaf-olaf-launches-enquiry-fake-covid-19-related-products_en. [28]

Europol (2020), *Catching the Virus: Cybercrime, Disinformation and the COVID-19 Pandemic.*, https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf. [25]

Europol (2020), *COVID-19: Fraud*, http://www.europol.europa.eu/covid-19/covid-19-fraud. [5]

Europol (2020), *How Criminals Profit From The COVID-19 Pandemic.*, https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic. [15]

FATF (2020), *Guidance on Digital ID*, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html. [23]

FATF (2015), *Combating the Abuse of Non-Profit Organisation (Recommendation 18)*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html. [22]

FBI (2020), *FBI Anticipates Rise In Business Email Compromise Schemes Related To The COVID-19 Pandemic*, http://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic. [9]

FBI (2020), *School Closings Due to COVID-19 Present Potential For Increased Risk of Child Exploitation*, https://www.fbi.gov/news/pressrel/press-releases/school-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation. [14]

Interpol (2020), *Global Operation Sees a Rise in Fake Medical Products Related to COVID-19*, https://www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19. [24]

Interpol (2020), *Cybercriminals Targeting Critical Healthcare Institutions with Ransomware.*, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware [10]

Interpol (2020), *INTERPOL Warns of Financial Fraud Linked to COVID-19. [online]*, http://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19. [1]

Interpol (2020), *Unmasked – International Covid-19 fraud exposed*. [online] Available at: https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed.

Singapore Police Force (2020), *New type of e-commerce scams involving the sale of face masks,*, http://www.police.gov.sg/media-room/news/20200222_others_new_type_of_ecommerce_scams_involving_the_sale_of_face_masks . [4]

UN (2020), *Secretary-General's Remarks to the Security Council on the COVID_19 Pandemic*, https://www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-the-security-council-the-covid-19-pandemic-delivered. [20]

U.S. Cybersecurity and Infrastructure Security Agency (2020), *COVID-19 Exploited By Malicious Cyber Actors | CISA*, www.us-cert.gov/ncas/alerts/aa20-099a.

US FDA (2020), *There Are No FDA-Approved Drugs Or Vaccines To Treat COVID-19*, http://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments. [3]

US ICE (2020), *ICE HSI arrests Georgia resident for selling illegal pesticide, claiming it protects against coronavirus*, https://www.ice.gov/news/releases/ice-hsi-arrests-georgia-resident-selling-illegal-pesticide-claiming-it-protects. [27]

US IRS (2020), *IRS issues warning about Coronavirus-related scams; watch out for schemes tied to economic impact payments.*, https://www.irs.gov/newsroom/irs-issues-warning-about-coronavirus-related-scams-watch-out-for-schemes-tied-to-economic-impact-payments. [17]

US Justice Department (2020), *Darknet Vendor Arrested on Distribution and Money Laundering Charges*, https://www.justice.gov/usao-edva/pr/darknet-vendor-arrested-distribution-and-money-laundering-charges. [19]

US Justice Department (2020), *Justice Department Seeks to End Illegal Online Sale of Industrial Bleach Marketed as "Miracle" Treatment for COVID-19*, https://www.justice.gov/opa/pr/justice-department-seeks-end-illegal-online-sale-industrial-bleach-marketed-miracle-treatment. [26]

US Securities and Exchange Commission (2020), *Look Out For Coronavirus-Related Investment Scams - Investor Alert. [online] Available at:*, http://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus. [6]

US Treasury (2020), *COVID-19 Scams*, https://home.treasury.gov/services/report-fraud-waste-and-abuse/covid-19-scams. [2]

US Treasury (2020), *Treasury Underscores Commitment to Global Flow of Humanitarian Aid in Face of COVID-19 Pandemic*, https://home.treasury.gov/news/press-releases/sm969. [21]

WEF (2020), *This is the Impact of COVID-19 on Modern Slavery*, https://www.weforum.org/agenda/2020/04/covid19-modern-slavery/. [12]

WHO (2020), *Cybersecurity. [online] Available at:*, http://www.who.int/about/communications/cyber-security. [7]

FATF

www.fatf-gafi.org

May 2020

Appendix SS:

FATF, *FATF Report: Illicit Tobacco Trade* (Paris: FATF, 2012)

FATF

FATF REPORT

Illicit Tobacco Trade

June 2012

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

1. The Financial Action Task Force (FATF) Plenary met in Mexico City, during June 2011. It was at said Plenary where a proposal to conduct typology research work into money laundering and terror financing to be associated with the Illicit Trade in Tobacco (ITT) was accepted.

2. March of 2011 also saw the OECD launch the "Oslo Dialogue" with the aim of promoting a whole of government approach to the tackling of financial crimes and illicit flows. This has been augmented by the G20 calling for strengthened inter-agency cooperation to fight illicit activities as well as the FATF adding tax crimes to the list of predicate offences.

3. The proponents of the typology stated that the illicit tobacco trade was prone to money laundering. Trade was considered to be cash intensive and profitable whilst being accompanied by low levels of risk posed to the criminal groupings (in terms of detection, seizures, penalties, criminal procedure) contributing towards the manifestation of the related illicit activities. Key areas of concern included:

a) Loss of revenue to the fiscal authorities.

b) The use of the illicitly generated proceeds (*i.e.,* to fund other crimes or the financing of terror).

c) The ability to distinguish between illicit activities as undertaken by licit and illicit players in the tobacco sector.

d) To identify the extent that governments enforcement agencies prioritise the addressing of illicit trade in tobacco when compared to other crimes.

4. It was furthermore mentioned that the project was to augment work already conducted by the FATF, which included *Trade Based Money Laundering* (June 2006), *Laundering the Proceeds of VAT Carousel Fraud* (February 2007), *ML Vulnerabilities in Free Trade Zones* (February 2010) as well as the then recently published *Global ML/TF Threat Assessment* (June 2010).

5. The identified key objectives were:

a) To determine the extent of the Money Laundering and Terror Financing (ML/TF) vulnerabilities associated with illicit trade in tobacco at a global, regional and domestic level.

b) To identify relevant case studies and determine trends and patterns from a global, regional and domestic perspective.

c) To identify possible indicators which may assist financial and non financial institutions in developing mechanisms to identify, report and counter smuggling activities and the misuse of trade practices.

d) To assist jurisdictions and FATF-Style Regional Bodies (FSRBs) in knowledge building and the identification of harms, drivers and measures associated with the illicit trade in tobacco.

e) To enhance the efforts aimed at curbing ML and TF associated with the illicit trade in tobacco.

6. This document provides a synopsis of the nature and extent of the ML/TF risks currently associated with the illicit trade in tobacco. It contains an overview of the problem statement and the data provided, as well as an analysis of the predicate offences, extent of associated money laundering and terror financing activities coupled lastly to the various jurisdictional enforcement responses to the curbing of this specific phenomenon.

7. The typology also attempts to highlight the primary reasons for the prevalence of ITT and should by no means be regarded as an exhaustive reflection of the subject. It must be borne in mind that jurisdictional approaches will differ in accordance to whether their territories can be characterised as a country of origin, transit or destination for illicitly traded tobacco as well as the related laundered proceeds thereof. This to a large extent is also characterised by jurisdictions health and related taxation policies as well as the differing approaches to the criminalisation of the predicate offences and the resulting money laundering, which ultimately impacts on organised crime groups (OCGs) responses thereto.

8. It can be stated that the international nature of ITT requires a global response. This once again, as with other typologies underscores the importance of international cooperation and the sharing of information. This should be done through (and not be limited to) active participation within and across a multitude of international forums such as the OECD, the FATF, the WCO, Interpol as well as amongst taxation authorities. Efforts should furthermore also be undertaken to incorporate inputs from organs of civil society.

9. Nationally, governments could guide reporting institutions on how to identify funds emanating from ITT. This can naturally emanate predominantly from within the law enforcement and customs environments. The setting up of centralised databases can also assist in identifying transnational organised crime groupings, their primary role players, their financiers and beneficiaries.

10. The purpose of this document is to therefore highlight the vulnerabilities that the ITT and related ranging predicate offences pose to the manifestation of money laundering and financing of terror. It highlights the nature of the predicate offence, the resulting money laundering as well as the propensity or appetite to investigate lastly mentioned. The typology also indicated the approaches as followed amongst enforcement agencies with special emphasis placed on customs authorities, law enforcement, financial intelligence units (FIUs) and lastly taxation authorities.

2. MONEY LAUNDERING, TERROR FINANCING AND THE ILLICIT TRADE IN TOBACCO

11. Various studies concur that that the illicit trade in tobacco accounts for a significant percentage of the global cigarette market. The revenues generated by this are estimated to amount to tens of billions of dollars. These revenues are usually hidden from taxation regimes and may also be used to fund other forms of crime and terror. The illicit trade in tobacco (ITT) therefore generates significant amounts of criminal proceeds, arising from both the trade itself and associated customs and tax offences.

12. A corollary affect is the increase in tobacco related illnesses and deaths because of the availability of cheap or counterfeit cigarettes. This has serious implications for the provision of appropriate health and welfare services to support an increase in consumption, of which the financial issues are exacerbated with a linked fall in tax revenues.

A. THE NEED FOR THE TYPOLOGY

13. Various FATF members are exposed to the risks posed by the illicit trade in tobacco. These risks manifest along the value chain, from the growing of raw tobacco, to national and international distribution, through to the final point of sale, whether it be in the formal or informal sectors. Extensive market penetration, coupled with cash intensive trade highlights the need for a typology evaluating the risk from ITT, especially in understanding how and where the criminal proceeds are laundered. Key areas of concern include:

a) The percentage of lost government revenues due to evaded taxes and customs duties.

b) Identifying the nature and extent of the risks posed by illicit tobacco trade in comparison to enforcement actions taken to curb the phenomenon.

c) The final destination and purpose of aggregated illicit funds.

d) The methodologies used to launder these illicit funds and the potential to uncover new mechanisms specific to ITT, and

e) A need to better understand the totality of ITT criminal finances, including opportunities for disruptive activity targeting perceived or identified financial pinch points (such as during the laundering of street cash following sales of illicit tobacco products).

B. SCOPE

14. The FATF Working Group on Typologies (WGTYP) is mandated to identify new threats and vulnerabilities as well as to conduct research into money laundering and terrorist financing techniques, with an emphasis on differentiating between the predicate offence and associated money laundering. The report aims to:

a) Define the illicit trade in tobacco, including the supply chain associated with the different types of smuggling.

b) Determine and assess the extent of the money laundering and terror financing (ML/TF) vulnerabilities associated with the illicit trade in tobacco and illustrate this via case studies provided by key contributors.

c) Identifying possible indicators to assist financial and non-financial institutions in uncovering, reporting and countering smuggling activities, the misuse of trade practices and money laundering or terrorist finance techniques.

15. In line with guidance given in the FATF Global ML/TF Threat Assessment, this will inform and assist jurisdictions and FATF Style Regional Bodies (FSRBs) in knowledge building as well as the identification of the harms, drivers and measures associated with the illicit tobacco trade.

C. METHODOLOGY

16. The research methodology included the development of a questionnaire sent to FATF member countries as well as FSRBs. The development of the typology was limited to evaluating the following research propositions:

a) Illicit trade in tobacco is a significant predicate offence to money laundering.

b) The proceeds of illicit trade in tobacco are used to fund terror.

c) Law Enforcement regards the effect of the illicit trade in tobacco as insignificant when compared to trade in other forms of contraband.

d) FIU suspicious transaction reports (STRs) will be insignificant in terms of identifying illicit trade in tobacco as predicate to ML or TF.

e) Despite the threat of civil or criminal investigations and disruption, ITT represents a good opportunity for Organised Crime Groups and / or Terror Groups to generate large sums of criminal profit.

f) The proceeds of illicit trade in tobacco is either laundered or used to fund other crimes or terror.

g) The use of trade in tobacco is significant within the trade based money laundering typology.

h) High taxes on tobacco stimulate illicit trade in tobacco.

17. A typologies workshop was also held with inputs received from various participants. These inputs are incorporated into the typology. It must however be noted that the primary theme to emerge from the workshop focused primarily on the predicate offence with information sourced from the returned questionnaires providing the bulk in terms of addressing money laundering and or terror financing to be associated with the phenomenon. Other sources of information used were accepted academic studies as well as pieces of information from various other accepted open sources.

3. AN OVERVIEW OF THE ILLICIT TRADE IN TOBACCO

DEFINITION OF THE ILLICIT TRADE IN TOBACCO AND THE HIGH-LEVEL RISKS ASSOCIATED WITH IT:

18. The illicit trading of tobacco products is the supply, distribution and sale of smuggled genuine, counterfeit[1] or cheap white[2] tobacco products. In generic non-commodity specific terms, it works on the following principle – there is a financial incentive to source a product in a lower-priced market and transport, distribute and sell it in a higher-priced market. This can include international movements or within countries that allow for intra-community price differentials. Illicit trade in tobacco is made up of various activities. Smuggling is conducted for one or both of the following reasons: to avoid excise taxes, and to evade rules prohibiting the sale of such goods. Merriman defines smuggling as the evasion of excise taxes on goods by circumvention of border controls.[3]

19. The sophistication and complexity of the smuggling depends upon the size and ambition of the groups involved and the nature of the commodity. For example, some Organised Crime Groups (OCGs) will manage all aspects of the production process, from sourcing raw tobacco product, through to developing specific tobacco packaging that will generate suitable market interest and / or appear legitimate if counterfeit product. Others will rely on the work of key facilitators, often based overseas, who engage with smaller legitimate tobacco manufacturers in sourcing the tobacco goods and associated packaging. The OCG then agrees a distribution route with the facilitator and agrees risk mitigation mechanisms to ensure successful delivery. Certain groups simply exploit lower cross-border[4] prices of genuine tobacco products and smuggle them to their chosen destination for sale.

20. Whatever the size and scale of the smuggling operation, the illicit trade in tobacco has crosscutting implications for governments, private businesses, law enforcement agencies, healthcare providers and the public, both smokers and non-smokers alike. The most tangible of these implications, financial or otherwise, are:

a) Deprivation of tax revenues, which can mean increases in other tax instruments to support a shortfall and / or the cutting of other public expenditure to ensure budgets, are managed within available funding profiles.

---

1 A product which is an identical copy of a branded product and packaging that is manufactured by parties that do not have the relevant intellectual property rights authorising them to manufacture such branded products. These products are illicit at the point of production because they have been manufactured without the authorisation of the legal brand owner.

2 Cheap whites are factory made cigarettes produced with the approval of a licensing authority in that jurisdiction. These are sometimes known as illicit whites but this is an incorrect term as they are produced legally.

3 Merriman, D (n.d.).

4 While there is a legitimate market for cross border trade, it is exploited by organised crime groups or individuals when the volumes exceed agreed personal allowance limits and / or the volume would be considered for commercial use.

b) If the perceived threat from smuggling is large enough, pressure on law enforcement to focus a percentage of available resources to interdict contraband, which can have implications for deployments against other border priorities and / or criminal activities.

c) A disproportionate impact on health services, such as reducing the provision of health care to treat other non-tobacco related / causal conditions, further exacerbated if the country also suffers a reduction in tax revenues.

d) Legitimate manufacturers who produce licensed tobacco products struggle to compete in an economy suffering an influx of cheap or counterfeit tobacco products. This has consequences for those frameworks aimed at regulating legitimate manufacturers (such as a reduction in tax receipts) and the overall attractiveness of a jurisdiction to associated trade.

21. Tobacco smuggling is attractive to criminals (or opportunists), for several reasons, including the generation of large sums of money for criminal reinvestment or funding lavish lifestyles, and the perception of lesser punitive sanctions or penalties if caught smuggling. The subsequent sections explore the different types of smuggling methodologies, including an assessment of the supply chains of each method.

DEFINING THE SUPPLY CHAIN AND SMUGGLING METHODOLOGIES:

22. A supply chain means the transformation of raw materials and components into a finished product, including any subsequent transportation and storage before distribution to the end customer. Although tobacco smuggling is an illicit activity, much of its supply chain is predicated on legitimate commodity movements, including people, technology, information and resources involved in moving and storing the products from the supplier (complicit or not) to the customer. Each methodology will include different supply chain requirements, which are further differentiated depending on the size, scale and sophistication of the smuggling activity. Organised Crime Groups (OCGs) or opportunist smugglers will add in their own variations depending on a number of factors. These factors include:

a) Mitigating the risk of detection at source, in transit or at point of sale, as this affects criminal profit margins. For example, monies set aside to pay off corrupt officials or the purchase of counter-surveillance equipment at storage or distribution points. Smaller groups or individuals will have a different attitude towards risk of detection and adapt their supply chain mechanisms accordingly.

b) The volume and type of the commodity they intend to smuggle. For example, packaged cigarettes require different logistical mechanisms than raw product or hand-rolling tobacco (HRT), while larger quantities of packaged cigarettes will place a different emphasis again on distribution and storage supply chain requirements.

c) The relative maturity of the individuals or groups involved in the smuggling. Experience may determine the level of sophistication they employ to smuggle goods into the identified jurisdiction. Less well established groups or individuals might sacrifice volume smuggled in an effort to mitigate risk of detection, while still making a

profit for reinvestment. As they become established, they may move from one particular distribution methodology for reasons of cost, increased volume or risk mitigation.

23. The supply chain of the illicit trade in tobacco, shows similarities with legitimate commodity importation. Each element of the supply chain (manufacturers, warehouse storage, transport, sale to the public) will carry a particular risk (financial or otherwise), which the smugglers evaluate and determine the best methodology to suit their needs.

BOOTLEGGING:

24. This involves the purchase of cigarettes or other tobacco products in relatively smaller quantities than would be associated with OCGs, but would still exceed limits set by customs regulations. Typically, bootleggers operate individually or in small groups whose membership is known and tightly managed. Compared to large-scale smuggling, bootleggers' methodologies are often less sophisticated, determined by whether it is opportunistic or market driven.

25. The smugglers purchase products either in low-tax jurisdictions or at duty-free or similar outlets (*i.e.,* cross-border ferry crossings or hypermarkets etc). The smuggler will transport the goods into the high-tax jurisdiction and sell them on an ad-hoc basis (opportunist) or deliver to an agreed customer, such as a wholesaler or other tobacco retail outlet. Typically, those involved in bootlegging use specially modified delivery vans or trucks, which include compartments to store the goods and evade customs detection. If foot passengers, they may also rely on the volume of passenger traffic to evade detection, storing the tobacco goods in their luggage[5].

26. This will also affect the frequency of smuggling activity, with those involved in bootlegging controlling much of the acquisition, transportation and distribution of the product. To avoid attracting the attention of law enforcement or justify travelling modes, bootleggers often manufacture elaborate and seemingly legitimate travel patterns to acquire the goods.

27. The relative maturity of bootleggers will also influence their attitude to supply chain risk and mitigation tactics, and by extension, their resilience to interdiction. That said, compared with large-scale smuggling, it is unlikely that bootleggers could absorb constant interdiction by enforcement agencies. Instead, they will often rely on the seemingly smaller scale of their smuggling activities to avoid detection.

LARGE-SCALE SMUGGLING:

28. Large-scale smuggling involves the acquisition and transportation of commercially sized consignments of tobacco products. Depending on the nature of the smuggling, one group or series of interconnected groups will take responsibility for the subsequent inland distribution and sale of the products; otherwise, distinct individuals (with relationships based on provision of service) manage elements of the supply chain demands. Large-scale organised smuggling likely accounts for the vast majority of cigarettes smuggled globally.

5 Joossens, *et al.* (2000).

29. While the greatest scope for profit generation is in jurisdictions with high taxation rates, this is not the only determinant. The smugglers will operate wherever there is scope to undercut a legitimate market and generate a suitable profit against their initial outlay. There is also anecdotal evidence to suggest OCGs involved in large-scale smuggling are territorial and will sell tobacco product(s) in their own jurisdiction.

30. While there are regional and market-level differences, several characteristics are common in large-scale smuggling operations:

a) Historically, prior to the control of genuine product supply chains, large-scale smuggling involved international brands, produced by the large multinational tobacco companies, because of the familiarity of the products and the ease in selling them.[6] However, recent operational activity has shown an increase in the smuggling of cheap whites, counterfeit goods and even counterfeit cheap white tobacco products due to the relative success of supply chain controls.

b) Secondly, large-scale smuggling takes advantage of the 'in transit' system developed to facilitate international trade. This system allows for the temporary suspension of customs duties, excise taxes, and VAT payable on goods originating from and / or destined for a third country, while in transit across the territory of a defined customs area. For example, cigarettes exported from the United States that are destined for North Africa will enter Belgium while en-route. Once in Belgium, the smugglers transported the cigarettes via the European road network to Spain, and then shipped to North Africa. As long as confirmation is given of re-exporting the goods, no tax liability is generated while the cigarettes are in transit.

c) Thirdly, large-scale cigarette smuggling can involve multiple individuals or gangs who will facilitate the transportation of the goods. Depending on the type of goods and the method of transport, these transactions can happen over a short period with the value of the product increasing as it nears the final point of distribution or sale. The likelihood or risk of detection also affects the price of the goods.

d) Finally, large-scale smuggling requires a good local distribution network, which can involve middle market distributors who may supply their own customers with the product and made available at an agreed distribution point or similar (sometimes referred to as a slaughter point). Otherwise, the importing OCG is involved in widespread street selling, allowing for the quick and effective sale of the smuggled cigarettes.[7]

31. Naturally, the supply chain for large-scale smuggling is longer and more sophisticated than that associated with bootlegging or opportunist smuggling, although this means a commensurate rise in the risk of infiltration from law enforcement or rival crime gangs. Whereas the bootlegger or opportunist smuggler is inclined to retain complete control over their product, OCGs tend to relinquish this responsibility to others; due to the significant volumes of goods smuggled, and

6 Barford, M.F. (1993).

7 Joosens, *et al*. (2000).

complexity of transportation and warehousing methods employed. Therefore, operating methods mitigate liabilities over safe delivery and accountability for any financial losses in the event of product seizure before reaching its final destination.

32. Those engaged in large-scale smuggling tend to use storage facilities in locales close to the point of importation or within the final jurisdiction. Not only does this allow the OCG control over access to these sites, it also builds resilience into their smuggling models as they can stock pile goods to offset the risk of detection, counter attacks from rival OCGs, and develop a more flexible response to evade frontier enforcement capabilities. While OCGs loathe losing loads to interdiction, unlike bootleggers or opportunistic smugglers, their business models will build in an acceptable level of loss.

33. Large-scale smuggling usually involves the transportation of volumes in excess of one million cigarettes per consignment, rather than an aggregated figure. Large-scale smugglers purchase master cases, which contains 10 000 cigarettes broken down into 50 cartons, which are 10 packets of 20 cigarettes. Buying in such large volume allows for the negotiation of purchase price for the initial importer and the middle market receiver.

34. Although smugglers will have an end destination for their tobacco product(s), some OCGs are willing to realise part of their consignment en-route or will 'sell' complete loads to other crime groups close to or around the point of final importation. Thus, the secondary OCG takes responsibility (and accountability) for transporting the goods into the final destination. The original owners will then re-purchase the goods at a higher price but still within suitable tolerances for them to generate a significant profit in country.

THE ECONOMICS OF TOBACCO SMUGGLING

PRODUCT PRICE:

35. As mentioned above, a variety of jurisdictions, produce cheap whites, with a large concentration of manufacturers in the United Arab Emirates free trade zones, but also in Malaysia, South Africa and Eastern Europe. Manufacturers in the UAE will sell a master case of cheap white cigarettes (10 000 cigarettes) for as little as 35 USD.

36. Counterfeit products operate under a different pricing structure because of the additional distance the goods have to travel, the illegal nature of the goods and the fact they sell for close to the recommended retail price in an effort to 'prove' they are genuine. On average, a master case of counterfeited cigarettes can cost between 140 and 150 USD, and a 50g pouch of counterfeited HRT costs between 7 and 8 USD at the point of production.

37. The price of genuine tobacco products is dependent on the retail price in the country of purchase, or if the smuggler abuses lower duty or duty free markets, such as cross-border ferry crossings. The product price rises as it is nears the final point of sale, reflecting an increase in risk of detection and associated costs of transportation and storage. The following is just one example of a smuggling methodology used by an OCG and involves the importation of cheap whites into the UK.

Box 1: **Case study – Pricing model of large scale smuggled tobacco**

Pricing Model

A UK-based OCG, via its overseas purchaser, arranges to buy 1 000 master cases from an independent tobacco manufacturer for 35 USD each. This appears legitimate to any law enforcement agencies based in the country of production. The overseas purchaser will arrange to sell the 1 000 master cases to a key EU-based transport facilitator for 65 USD a master case. At this stage any relevant customs documentation may correctly list the goods as cigarettes. Although the financial responsibility for safe transportation of the goods reverts to the EU facilitator, the OCG retains 'ownership' of the goods.

Once safely deposited into a near-continent based warehouse controlled by the UK-based OCG (who now takes formal ownership of the goods and any associated risks), the EU facilitator will receive, on average, 600 EUR per master case, a percentage of which represents the risk the facilitator took in delivering the product. Any related customs documentation is altered so the goods are listed as a less suspicious commodity.

Upon successfully importing the goods into the UK, the OCG will sell them to their UK middle market suppliers for 700 EUR to 1 100 EUR a master case, depending on the quantity ordered and the brand requested. The OCG retains accountability for any losses until the goods reach the agreed distribution point. At the point of sale, the cigarettes will sell for anything between three and four GBP, which appears to be an 'acceptable' price to the consumer for buying illicit cigarettes.

If the middle market distributor purchased a mastercase for 700 EUR (approx 560 GBP) and sells all 500 packets of 20 cigarettes for 3 GBP, they will make a profit of just under 1 000 GBP when subtracting the cost of purchase. However, this doesn't take into account any other associated costs which can affect the profit margin.

Source: United Kingdom

38. Putting the illicit tobacco trade into context, Table 1 shows the price and tax burden of a pack of 20 cigarettes in eight of the 27 EU Members states, representing the four most and least expensive jurisdictions. As the table indicates, bootleggers or organised smugglers can make significant profit (and by extension a tax loss experienced by the government) from purchasing genuine duty-paid cigarettes in Estonia, transporting them to any of the four most expensive jurisdictions and sell them for a discounted price.

Table 1: **The price and tax burden of 20 cigarettes in the premium cigarette price category in eight of the 27 EU Member States.**

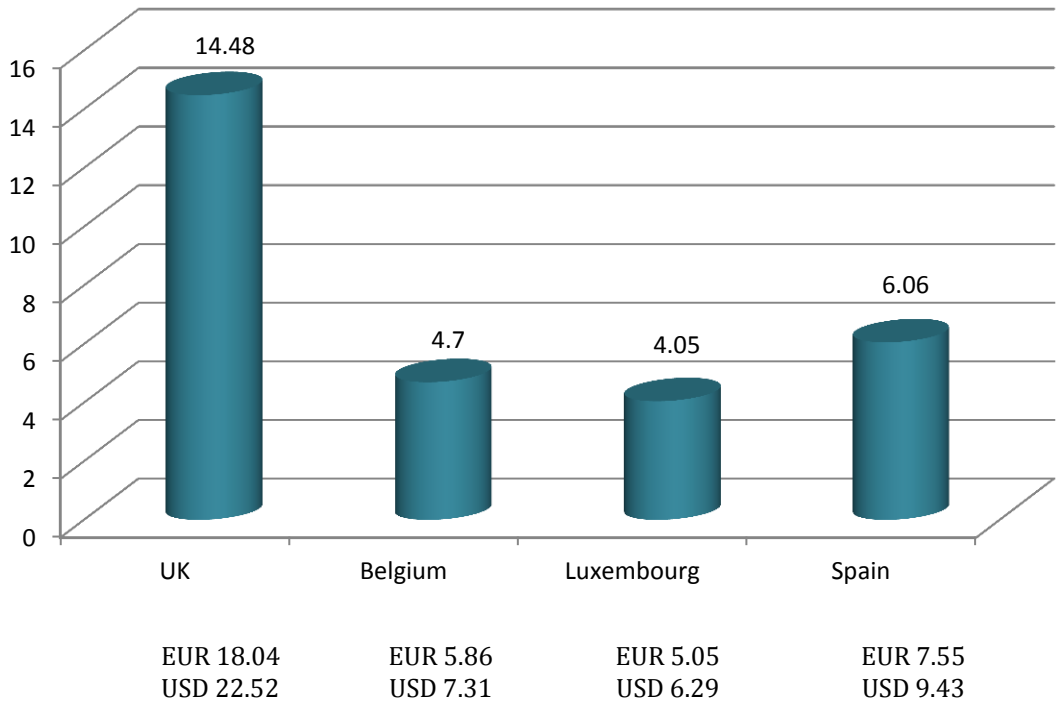
	RRP per 20 cigarettes			Tax burden per 20 cigarettes			Tax Incidence
Country	GBP	EUR	USD	GBP	EUR	USD	
Ireland	7.41	9.27	11.62	5.82	7.28	9.13	79%
UK	6.95	8.69	10.89	5.40	6.75	8.47	78%
Sweden	5.71	7.14	8.95	3.95	4.94	6.19	69%
France	5.12	6.40	8.03	4.09	5.12	6.41	80%
Bulgaria	2.65	3.31	4.15	2.08	2.60	3.26	79%
Lithuania	2.41	3.01	3.77	1.78	2.23	2.79	74%
Hungary	2.40	3.00	3.76	1.88	2.35	2.95	78%
Estonia	2.38	2.97	3.73	1.85	2.31	2.90	78%

Source: The Tobacco Manufacturers' Association website

39. Figure 1 shows selected EU price differentials for 50g hand-rolling tobacco pouches, reinforcing the UK's position as an attractive jurisdiction for the smuggling of genuine and smuggled HRT product.

40. The price of the smuggled goods is dependent on several issues, including the brand, *i.e.,* whether it is a cheap white or a counterfeited genuine product, the evaluation of law enforcement capability and the existence of a reliable internal distribution market. Smugglers will test different brands and prices to find a balance that maximises market penetration and profit generation. As a rule of thumb, the distributors sell the products for between 50% and 75% of the recommended retail price of genuine tobacco products. However, as mentioned above, wherever there is scope for a smuggler to undercut an existing market, they will transport goods into the jurisdiction and determine a suitable price based on their experience in gaining market penetration and the cost of legitimate products.

Figure 1: **Hand-rolling tobacco price differentials of selected EU countries April 2011 (in GBP)**



TRANSPORTATION & STORAGE COSTS:

41. This is dependent on the nature of the product smuggled and the money available. Large-scale smuggling requires more money set aside to cover transport and storage costs than required by opportunist smuggling or bootlegging. The main methodologies for all types of smuggling are:

a) Via container shipped from point of production either directly to point of consolidation for in-country wholesale or retail distribution or via other ports to disguise their origin and / or secondary distribution. Containers can hold up to 10 million cigarettes in total, but OCGs can reduce the overall volume by smuggling the products within legitimate cover loads.

b) Roll on / Roll off (Ro-Ro) freight traffic, sometimes used in collaboration with sea-shipped containers. A twenty-foot trailer can hold 475 master cases, which is approximately 4.75 million cigarettes. OCGs may operate haulage companies directly or financially incentivise otherwise legitimate haulage companies to transport shipments to the final point of sale. The costs associated with the use of these businesses, including payments paid to the drivers are not well known. For example, in two separate UK investigations involving Ro-Ro, one driver received GBP 1 500 per successful crossing, while another OCG was paying its drivers up to GBP 10 000 to ensure successful transportation.

c) Fast parcel / airfreight of smuggled goods and transport packaging material associated with tobacco products, such as HRT pouches and even the raw tobacco product itself.

As with the other methodologies, smugglers incorrectly describe loads to frustrate law enforcement intervention.

d) The abuse of cross-border shopping by vehicle or foot traffic, which can mean the overall volume is less than large-scale smuggling, but with a still noticeable impact on a country's tax receipts from the importation of non-duty paid genuine product. However, certain OCGs realise the potential from infiltrating the bootlegging market and exploit these cross-border opportunities. For example, coach loads of seemingly legitimate holidaymakers working on behalf of a crime group will travel to a jurisdiction where the price of genuine product is low and bulk buy. This gives the OCGs a stock of genuine product to sell, with the monies generated covering the costs of the method but still delivering a healthy profit.

42. It is likely large-scale smugglers will employ a combination of methods to spread the risk of detection. By having a flexible transportation model, it allows them to manage more effectively spikes in demand from customers as well as maintain a strong grip on costs.

43. Not all smuggling methodologies lend themselves to the acquisition of warehousing or storage facilities, but when used; they provide the OCGs with resilience in the face of a possible increase in the efforts of investigating agencies. When transporting illicit cigarettes to the UK, several OCGs own and manage 'super warehouses' in various near continent jurisdictions such as France, Belgium and the Netherlands. This allows them to stockpile goods in the event of an increase in enforcement authority at border locations or seizures of commodity inland.

ILLICIT DISTRIBUTION POINTS & CASH COLLATION

44. Many OCGs transport larger consignments to distribution points only known to them and their customers. Here the load is split down and sold to middle market suppliers. These distribution points change on a regular basis, with the location determined as close to importation date as possible to frustrate law enforcement intervention opportunities. There is no fixed typology for the type of location favoured. It can be a rented plot on an industrial estate, housed within a self-storage facility or if a smaller load, kept in a lock-up or garage.

45. Depending on the reliability of middle market buyers, the smugglers can generate at these illicit distribution points, which is either collated offsite before the OCGs launder the proceeds or is immediately returned overseas, often via a cash courier or using concealments in a vehicle. Again, there is no fixed typology to identify cash remittance methodologies but it represents a tangible risk to the smugglers until used to a) pay for any future loads or b) the criminal profit is laundered.

THE IMPACT OF THE ILLICIT TRADE IN TOBACCO

46. The illicit trade in tobacco affects governments, private business, labour and society. The most visible of said consequences are:

a) Governments deprived of tax revenue, which necessitates increases in other tax instruments to deliver mandated public expenditure programmes. A general decrease in tax compliance and expected revenues undermines the tax system as a whole.

b) The potential promotion of criminality and corruption within government, which can coincide with an increase in tolerance of criminality, which in turn encourages and attracts national and international organised crime groups or opportunistic smugglers.

c) The severe affect on consumer health and healthcare provision, especially where tobacco products do not comply with minimum health requirements.

d) Difficulties for legal tobacco manufacturers to compete openly and fairly, which undermines regulatory regimes aimed at governing the legitimate industry.

47. Joossens, *et al.* (2000) sight the following as consequences of unabated illicit trading in tobacco.

a) Smuggled cigarettes compete with legal cigarettes. The two implications are an increase in cigarette consumption and an artificial impact on cigarette pricing. This can be lowered to secure the legitimate market but is affected by government commitments to tackle cigarette consumption. Moreover, the presence of smuggled cigarettes can put legitimate retailers at a competitive disadvantage, leading some to be less compliant with tobacco-control laws than they would be in the absence of competition from a black market.

b) A black market in cigarettes can undermine efforts to limit youth access to tobacco products and other approaches to reducing overall availability of these products. While tobacco retailers may comply with national or local policies prohibiting the sale of tobacco products to underage persons and otherwise limit availability, it is much less likely that vendors of smuggled cigarettes will comply with these policies.

c) The potential profits associated with large-scale cigarette smuggling create incentives for organised crime networks to develop, bringing with them a number of problems. Cigarette smuggling can be a relatively low-risk source of revenues for these networks, and then used to support more high-risk activities. In addition, the growth of these networks can increase the general level of corruption in a country, both among its citizens who purchase cigarettes in the black market and among public officials who facilitate black market activities.

48. The aforementioned is very difficult to measure, both for the illicit economy as a whole but also in the case of measuring the effect of illicit trading in one commodity. This has consequences for developing suitable metrics to quantify the associated money laundering.

APPROACHES TO THE DEVELOPMENT OF A MEASUREMENT TOOL

49. It is not the purpose of this document to provide a measurement tool to test the prevalence of the illicit trade in tobacco. A short synopsis of a tool as designed by Merriman is provided to indicate that approaches do exist and that further study may identify the prevalence of money laundering associated with quantified illicitly traded tobacco.

50. Reliable quantitative measures of tobacco smuggling can enhance tobacco control policy. Baseline measurements of tobacco use and tax avoidance and evasion can develop, upon which policies are then established. Further measurements can provide appropriate benchmarks to ensure

the implementation, review, and improvement of such policies. In addition, sound measurements of the association between changes in tobacco control policies and changes in smuggling can prove the success of these policies.

51. Estimating the true nature of smuggling is challenging because it is an illegal and hidden activity. A number of useful and reliable methods to measure smuggling are available, but each method has limitations. When time and resources permit, it is best to use several different methods in order to cross-validate estimates minimizing any methodological objections.

52. This tool offers five methods to measure tobacco smuggling. The methods are ranked, with the first requiring the least technical and statistical sophistication and the last requiring the greatest level of technical complexity and statistical inference:

a) Observe the producers and ask the experts for smuggling data.

b) Observe smokers directly and ask them about their methods of obtaining tobacco.

c) Monitor and analyze data on the export and import of tobacco.

d) Compare the sale of tobacco with estimated consumption of tobacco by using household surveys.

e) Compare the sale of tobacco with estimated consumption of tobacco by using a mathematical formula and economic inference.

53. Following the development of indicative figures quantifying the illicit trade in tobacco, domestic and international agencies can work together to determine the volume and value of associated money laundering. This type of complementary statistical analysis can support a step-change in investigative response, moving agencies away for a solely commodity seizure based response to a more holistic position of targeting both the commodity and the associated business model, including efforts at laundering criminal cash. The next section evaluates existing investigative responses in more detail.

THE OPPORTUNITIES FOR AN IMPROVED INVESTIGATIVE RESPONSE

54. According to the foreword to the World Customs Organisation's 2010 Customs and Tobacco report, the WCO had "witnessed an unparalleled growth in the illicit trade of tobacco products over recent years" recognising a need for countries to step up their efforts to tackle this problem. The report also stated "that where goods are highly taxed, easily portable and penalties remain relatively light for smuggling, trans-national criminal organisations will take advantage of any weaknesses in customs, revenue or other border controls to amass profits".[8]

55. With such a commodity intensive crime type, the default setting is to seize as much of the product before it reaches the middle market suppliers / point of sale, supported by a criminal investigation aimed at tackling the smugglers. Depending on the capability of the investigating agency, it establishes a parallel financial investigation seeking to recover assets bought or associated with the criminal proceeds.

8 WCO (2011).

56. For relatively inexperienced or low-volume smugglers, such an approach can seriously undermine their ability to establish a foothold in the market. They do not have time to build up additional stock in the event of product seizures, nor will they have the ability to change their smuggling methodology. It is likely they have invested their own start up capital and are reliant on the sale of several smuggled loads before they can realistically absorb the financial losses associated with a seizure. They may also use relatively simple mechanisms to launder the proceeds of their crime and the acquisition of property and other assets takes place in their home jurisdiction. As such, asset denial or recovery can have a serious impact on their ability to continue smuggling and disrupt their seemingly legitimate life.

57. As assessed above, those involved in large-scale smuggling will adopt risk mitigation strategies to offset any potential financial and commodity losses via law enforcement interdiction. This includes 'losing' loads to investigating agencies to frustrate anti smuggling / investigation capability in the knowledge that they have subsequent loads en-route or passing through the point of entry at the same time. Law enforcement authorities may also use upstream interdiction tactics, though from a financial perspective tobacco products will not have acquired the value that generates substantial criminal profit. Given the propensity of OCGs to purchase assets overseas or use complex mechanisms to launder the profits from their criminality, it can be extremely difficult to dismantle the more sophisticated crime groups without international cooperation.

58. What is required is an improved understanding of the business models underpinning tobacco smuggling. Whilst each jurisdiction may have discrete ITT methodologies, mapping economic models against generic supply chain models will enhance enforcement opportunities and impact on the ITT using concurrent financial, frontier and inland intervention activities.

59. The growing threat from the ITT requires greater sharing of acquired knowledge and understanding of criminal activity and financial business models to improve enforcement impact at domestic and international levels. The international nature of the ITT demands a global response that includes tackling the financial dimensions of the trade and recovering illicitly derived assets.

4. THE JURISDICTIONAL APPROACH TOWARDS THE ILLICIT TRADE IN TOBACCO

60. The purpose of this chapter is to provide an overview of the various jurisdictional approaches towards the criminalisation of the illicit trade in tobacco. The body of information was obtained from the jurisdictions via responses to a questionnaire. (Refer to the list of respondents in Chapter 5, Table 2.) The focus of the questionnaire was to place emphasis on the criminalisation of ITT as well as other types of offences which may be associated with ITT. Consideration was also lastly given to possible penalties or remedies at the disposal of the said jurisdictions.

A. THE CRIMINALISATION OF THE ILLICIT TRADE IN TOBACCO (ITT) AND POSSIBLE ALTERNATIVE OFFENCES

61. The vast majority of respondents indicated that the ITT is a criminal offence. An aspect that was however clear is that the definitions of what would constitute the ITT differed between jurisdictions. The penalties associated with these acts were in some cases also dependant on the volume and or value of illicitly traded tobacco.

62. Jurisdictions therefore stated that ITT was a criminal offence but then also indicated that transgressions could be found within the criminal, customs, tax crimes and trademark modalities. The core themes being smuggling, evasion of customs duties and tax, tax fraud and the violation of monopoly law. Respondent 5 indicated that the illicit production of tobacco for instance was also an offence. Respondent 6 also made reference to the trading of counterfeit goods.

63. Respondent 15 however indicated that ITT is not a criminal offence and that charges related to it would be importation offences under customs legislation or legal proceedings derived from trademark infringements.

64. **Conclusions:** The following is therefore of importance:

a) Most Jurisdictions do see the ITT as a criminal offence. This does not however imply that they would see it as a predicate offence to ML.

b) Other associated offences include tax crimes and transgressions within the trademark environment.

c) The ITT can therefore be associated with tax offences which have then also been accepted as a predicate offence to Money Laundering.

B. PENALTIES TO BE ASSOCIATED WITH CONVICTIONS REGARDING ITT

65. The following significant responses are provided:

a) Respondent 3: "There are various instruments for recourse that are provided by the country's legislation for contraventions related to the illicit trade in tobacco products. These include, but are not limited to the Customs and Excise Act, 91 of 1964, the Tobacco Products Control Act, 83 of 1993 and the Financial Intelligence Centre Act, 38

of 2001, as well as the Value Added Tax Act, 89 of 1991 and Criminal Procedure Act, 51 of 1997. The identified contravention determines the legal instrument that will be applicable. Fines and sentences differ from case to case. Some of the suspects were apprehended on more than one occasion with the equivalent of a USD 2 500 fine and or 3 years imprisonment, suspended for five years (In this case 13800 sticks were being traded). The revenue service has also raised schedules on manufacturers and distributors for the diversion of cigarettes. Non-compliance with section 3 and (3) A of the Counterfeit Goods Act (Act 37 of 1997) as amended constitutes a criminal offence in accordance with section 7(3) of the act and any person found guilty of such an offence shall on conviction be liable to a fine not exceeding the equivalent of USD 120 000. With respect to the Customs and Excise Act (as amended) the omission of the stamp is regarded as an offence in terms of section 80(1) and any person found guilty shall be liable on conviction of a fine not exceeding the equivalent of USD 2500 or treble the value of the goods.

b) Respondent 4 indicated:

   i) For smuggling: from two to eight years or four to eight years of imprisonment depending on the circumstances and;

   ii) For evasion (tax fraud): from two to six years or three years and six months to nine years of imprisonment.

   iii) For counterfeit transgressions: one to six years of imprisonment (when official stamps are involved); or three months to two years of imprisonment (when trademarks are involved).

c) Respondent 5 indicated that penalties are up to the twofold of the evaded duties. In case of commercial perpetration up to the threefold of the evaded duties, as well as in criminal and in administrative procedures. In addition criminal courts can apply imprisonment of up to two years (in case of commercial perpetration up to three years). In cases of qualified tax fraud, imprisonment of up to ten years is applicable. Administrative panels can apply additional imprisonment up to three months. All illicit traded tobacco has to be confiscated. If confiscation is not possible (*i.e.,* it has been consummated), perpetrators are then also charged with a compensation penalty.

d) Respondent 8 indicated that a penalty of up to five years imprisonment or a monetary fine can be imposed for tax evasion. In particularly serious cases, a penalty of between six months and ten years imprisonment shall be imposed. A case shall generally be deemed to be particularly serious where the perpetrator deliberately understates taxes on a large scale or derives unwarranted tax advantages, abuses his authority or position as a public official, solicits the assistance of a public official who abuses his authority or position, repeatedly understates taxes or derives unwarranted tax advantages by using falsified or forged documents, or as a member of a group formed for the purpose of repeatedly committing acts, understates turnover taxes or excise duties or derives unwarranted turnover tax or excise duty advantages. Whoever evades import or export duties on a commercial basis or who illegally imports, exports or transports goods on a commercial basis in contravention of monopoly regulations

shall be subject to imprisonment from six months up to ten years. In less serious cases, the penalty shall be imprisonment for up to five years or a monetary fine.

e) Respondent 9 interestingly states that tobacco smuggling is considered a crime when the amount of product dealt is more than ten Kilos. It is normally punished by imprisonment (from two to five years) and a financial sanction of 5 EUR per grams. The punishment increases (from three to seven years) in relation to particular conditions. Heavier penalties are provided when the offence is committed by criminal organisations (imprisonment that can go from a minimum of three years to a maximum of eight years).

f) Respondent 13 states in a similar vein that no person shall sell, offer for sale or have in their possession a tobacco product unless it is stamped (duties/taxes paid) Dual offence: Indictment: min fine to the max fine or max of five years in jail or both (fine & jail) Summary conviction: min fine to a max of USD 500 000 or up to 18 months in jail or both (fine & jail) Min fine: USD 0.17 x number of cigarettes Max fine: USD 0.255 x number of cigarettes.

66. **Conclusions:** It is therefore clear that a wide array of penalties is at the disposal of law enforcement entities. These penalties range from transgressions in terms of tax evasion and fraud, customs duty/excise evasion and fraud, smuggling etc. The nature of penalties imposed range from varying periods of incarceration and fines dependant on other factors such as relations to organised crime as well as the volume and or weight of the illicitly traded product. Of importance however was to then determine whether money laundering charges and convictions could be associated with the aforementioned.

C. MONEY LAUNDERING INDICTMENTS TO BE ASSOCIATED WITH CHARGES RELATING TO THE ILLICIT TRADE IN TOBACCO

67. Of the 18 responses received only 6 respondents indicated that they could relate money laundering cases to the illicit trade in tobacco. A total of three successfully prosecuted cases were claimed by three separate jurisdictions with one jurisdiction stating that "Of the 157 tobacco cases adopted for criminal investigation during 2010 – 2011, 22 also included ML as a secondary regime. These operations are still live and no charging decisions have yet been finalised".

68. **Conclusions:** It is therefore clear that authorities are convicting perpetrators of ITT on varying offences but that ML is very seldomly included in the charge sheet. The question that then remained was what the relation would be between terror financing and the ITT.

D. INDICTMENTS ASSOCIATED WITH THE ILLICIT TRADE IN TOBACCO CAN BE LINKED TO TERRORIST ORGANISATIONS

69. Only one possible indictment related to ITT and terror financing could be sighted out of the possible 18 respondents.

E. OTHER CRIMINAL ACTIVITY TO BE LINKED/ASSOCIATED WITH THE ILLICIT TRADE IN TOBACCO

70. In essence an array of other crimes could also be associated with ITT. These once again included the normal tax and customs offences which were then also indicative of the illicit trade in other commodities or contraband.

71. Respondent 11 for instance indicated that intelligence suggested that there continues to be some crossover between tobacco fraud and the following:

a) MTIC (Missing Trader Intra-Community) fraud by criminals known to the said jurisdictions customs and revenue service.

b) Secondly, alcohol excise fraud was also prevalent with intelligence indicating that some Organised Crime Groups involved in tobacco fraud are also involved in illicit alcohol shipments. Furthermore some hauliers used by Organised Crime Groups for tobacco smuggling are also used for alcohol smuggling.

c) Oils excise fraud – "we have seen intelligence indicating that some Organised Crime Groups involved in tobacco fraud associated with illicit oils movements".

d) Drugs – we have seen intelligence indicating that some Organised Crime Groups involved in tobacco fraud are involved in drug smuggling.

e) Money Laundering – criminally complicit haulage companies have been known to act as cash couriers on behalf of the Organised Crime Groups, aiding their efforts to launder / transfer the proceeds.

f) There is also strong evidence and intelligence linking criminally complicit MSBs (including hawaladars) with the laundering of monies generated by tobacco smuggling.

F. CONCLUSIONS

72. The primary focus to be determined from this specific section of the questionnaire was to obtain a broad view on how jurisdictions approach ITT. The primary trend to emerge was that jurisdictions tended to investigate and prosecute on the predicate offence with little to suggest an emphasis on pursuing money laundering and or terror financing cases to be associated with the illicit trade in tobacco. It is possible that this might occur where perpetrators are known to be involved in organised crime. The tax and customs offences are also sighted to be investigated in isolation. A more detailed overview is however supplied in the following chapters.

5. THE MODUS OPERANDI PERTAINING TO THE PREDICATE OFFENCE

73. The purpose of this chapter is to provide an overview of how various jurisdictions view the Illicit Trade in Tobacco as a predicate offence. It is important for contextual purposes to provide a description of the respondents. The differentiating factors are:

- Status in terms of FATF membership.
- Member of observer organisations to the FATF.
- Geographic location.

74. The aforementioned can therefore be displayed as follows:

Table 2: **Respondent List**

Serial No	Country	Membership of FATF and other	Observer organisations to FATF	Location
1.	Japan	FATF APG MONEYVAL[1] EAG[1]	AfDB, AsDB, Egmont Group, EBRD, IADB, IAIS, IMF, Interpol, IOSCO, OAS[1], OECD, UN, World Bank, WCO	Asia
2.	Hong Kong	FATF APG	AsDB, Egmont Group, IAIS, IMF, IOSCO, OGBS, WCO	Asia
3.	South Africa	FATF ESAAMLG	AfDB, Egmont Group, Commonwealth Secretariat, IAIS, IMF, IOSCO, Interpol, UN, World Bank, WCO	Africa
4.	Argentina	FATF GAFISUD	AfDB, Egmont Group, IADB, IAIS, IOSCO, IMF, Interpol, OAS, UN, World Bank, WCO	South America
5.	Austria	FATF	AfDB, AsDB, Egmont Group, EBRD, ECB, Europol, IADB, IAIS, IMF, IOSCO, Interpol, OECD, UN, Word Bank, WCO	Europe
6.	Belgium	FATF	AfDB, AsDB, Egmont Group, EBRD, Europol, ECB, IADB, IAIS, IMF, IOSCO, Interpol, OAS[1], OECD, UN, World Bank, WCO	Europe
7.	France	FATF APG[1] CFATF[2] EAG[1] GAFISUD[1]	AfDB, AsDB, EBRD, Egmont Group, Europol, ECB, IADB, IAIS, IMF, IOSCO, Interpol, OAS[1,] OECD, UN, World Bank, WCO	Europe
8.	Germany	FATF EAG[1]	AfDB, AsDB, EBRD, Egmont Group, Europol, ECB, IADB, IAIS, IMF, IOSCO, Interpol, OAS[1], OECD, UN, World Bank, WCO	Europe
9.	Italy	FATF EAG[1]	AfDB, AsDB, EBRD, Egmont Group, Europol, ECB, IADB, IAIS, IMF, IOSCO, Interpol, OAS[1], OECD, UN, World Bank, WCO	Europe
10.	Switzerland	FATF	AfDB, AsDB, EBRD, IADB, IOSCO, Egmont Group, IAIS, IMF, Interpol, OAS[1], OECD, UN, World Bank, WCO	Europe

Table 2: **Respondent List**

Serial No	Country	Membership of FATF and other	Observer organisations to FATF	Location
11.	United Kingdom	FATF APG[1] CFATF[2] EAG[1] ESAAMLG[2]	AfDB, AsDB, EBRD, Egmont Group, Commonwealth Secretariat, Europol, ECB, IADB, IAIS, IMF, Interpol, IOSCO, OAS[1], OECD, UN, World Bank, WCO	Europe
12.	United States	FATF APG CFATF[2] MONEYVAL[1] EAG[1] ESAAMLG[2] GAFISUD[1]	AfDB, AsDB, EBRD, IADB, IOSCO, Egmont Group, IAIS, IMF, Interpol, OAS, OECD, UN, World Bank, WCO	North America
13.	Canada	FATF APG CFATF[2] MONEYVAL[1]	AfDB, AsDB, Egmont Group, Commonwealth Secretariat, IADB, IAIS, IMF, Interpol, OAS, UN, World Bank, WCO	North America
14.	Vietnam	APG		Asia
15.	Anguilla	CFATF		Caribbean
16.	Belize	CFATF		Caribbean
17.	Macao	APG		Asia
18.	Singapore	FATF APG	AsDB, Egmont Group, Commonwealth Secretariat, IAIS, IMF, IOSCO, Interpol, OGBS, UN, World Bank, WCO	Asia

1. Observer
2. Co-operating and Supporting Nations

75. 14 of the 18 respondents are member countries to the FATF. The four remaining respondents are members of FATF Associate member countries. Seven of the respondents are from Europe with two respondents representing North America, one representing Africa and one representing South America with five respondents from Asia and two respondents from Central America.

76. The chapter and the relevant questions are to be addressed in terms of geographic location. The purpose being to determine whether specific trends can be ascribed to certain regions.

A. PRIMARY ROLE-PLAYERS ASSOCIATED WITH THE ILLICIT TRADE IN TOBACCO (*I.E.,* DOMESTIC VS. FOREIGN ROLE-PLAYERS)

77. **Asia.** Answers obtained from jurisdictions were not substantial enough to provide a trend. The primary theme being that both domestic and foreign role-players have been involved.

78. **Africa.** Respondent 3 indicated that both domestic and foreign role players play a major role in the illegal manufacturing, importation and distribution of illicit tobacco with undocumented immigrants, and asylum seekers also recently being seen to form part of the specific transportation and distribution of the illicit product.

Box 2: **Case study –ITT cross border cash movement and money laundering**

Company Y was an established legitimate registered producer of cigarettes. In an effort to improve competitiveness said company mixed imported products with locally manufactured products. These products were then distributed in the host country at a discounted rate. The money that was obtained through the evasion of taxes was then used to further capitalize the company. Company Y also "round-tripped" their products back into the host country and proceeded to sell it locally as well. Duties were furthermore evaded by making use of bond to bond mechanisms. Company Y in the process of investigation admitted to importing close on 50 containers of cigarettes over an extracted period of time. Funds were moved offshore using various Special Purpose Vehicles. The matter was investigated by Tax Authorities with an assessment plus penalties raised to the value of USD 4 million.

Source: South Africa

79. **Europe.** EU countries indicated that domestic and foreign role-players were involved but that the majority of foreign role players were also nationals. Respondent 9 however indicated the involvement of East European nationals.

Box 3: **Case study – Operation 'Desert Tree'**

On 27 October 2009, as part of a Multi Agency Operation, Irish Customs Officers seized:

- a total of 120 304 000 contraband cigarettes;
- the general cargo vessel MV Anne Scan;
- 200 tons of Copra animal feed;
- three articulated vehicles; and
- a quantity of cash (approximately EUR 30 000)

Following an operation at Greenore Port, Co Louth and the surrounding area. The operation was supported by the Irish Air Corps, Irish Naval Service, An Garda Siochana (Police), HMRC, PSNI and the European Fraud Office (OLAF).

The vessel MV Anne Scan, IMO 9145126, The Philippines, on 15 September 2009 with a declared cargo of 1 490 bags of animal feed, the port of destination being Greenore, Co Louth, Ireland. The vessel was monitored on the high seas en route to Greenore Port, arriving at 0600 on Monday 26 October 2009. Surveillance of the vessel was maintained over a period of time.

Following the discharge of part of the cargo from the vessel on Tuesday 27 October 2009 onto awaiting trucks, which were allowed onwards to their place of offloading, the Multi Agency Task Force moved in and raided several premises in the Co Louth area, in addition to mounting an operation on the vessel.

Investigation

Documents uplifted and enquiries conducted during the course of the subsequent investigations have revealed that the vessel was chartered for one direct voyage from The Philippines to Ireland.

The Irish based importer provided all cargoes (cigarettes and copra) and various packaging material to the warehouse in advance of shipping to Ireland. He supervised the stuffing of cigarettes and copra in jumbo bags until completion of loading the outbound vessel.

The individual gave strict and specific instructions to change the descriptions of the goods and the vessel's final destination as Vietnam and the cargo as animal feeds 'in order to protect the cargo against piracy during the voyage'.

He paid the haulage firm in cash (USD) for rental of the warehouse, charter of the vessel, stevedoring, consolidation of jumbo bags and other related expenses. (The cash payment for the charter of the vessel alone amounted to USD 540 000.)

Track and Tracing of the cigarettes

The brands and quantities of cigarettes seized were Palace (99 431 000), Chelsea (13 240 000) and a mixture of other genuine brands.

The Imperial Tobacco branded products have been confirmed as genuine product, which was sold by Imperial Tobacco, UK to a bond store in India, which later shipped them to The Philippines. While the Palace and Chelsea branded cigarettes were traced as being shipped by Silver Eagle Manufacturing Tobacco Company, Cavite to the consolidation warehouse in The Philippines.

Conclusions

- Various jurisdictions were involved. India to Philippines to Ireland using Vietnam on the papers as final point of destination.
- Multiple nationalities were involved.
- Use of cash (EUR 540 000) for payment which was most likely not declared at ports of exit and entry or use of front companies.
- Key themes would have been tax and duties evasion, fraud (false declarations in terms of final destiny and type of commodity)
- Success was achieved through sound sharing of information and amongst multiple local and foreign law enforcement agencies.

Source: United Kingdom

80. **America.** Respondent 12 indicated that the primary international source of counterfeit tobacco products originated from China. Domestically, Indian reservations, importers, and duty free stores have been a source of untaxed tobacco products illegally into the commerce of the respondent's economical areas. A trend highlighted by the respondent was the use of the Internet to sell and purchase tobacco products. Mail and express consignment facilities were also being used

more often, instead of the traditional cargo container, to ship illicit tobacco products in small amounts which fall under prosecutorial guidelines in many jurisdictions.

Box 4: **Case study – Cigarette smuggling and protection fees**

In 2002, the European Community (EC) filed suit against an American tobacco company alleging money laundering activities surrounding cigarette smuggling. According to the complaint, the company violated the trade embargo with Iraq and paid the PKK a fee for every container that moved across the Kurdish region of Turkey during the 1990's. The cigarettes were smuggled from Turkey, through the northern border of Iraq, and into two PKK controlled areas of Iraq. The profits were suspected of funding the terrorist activities of the PKK and other terrorist organisations operating in Northern Iraq. Ironically, whereas the group controlled the flow of contraband cigarettes into Iraq during the 1990s, they now control the flood of counterfeit cigarettes streaming out of Iraq.

Source: United States

81. **Conclusions:** The answers and case study provided confirms the transnational nature to be ascribed to the illicit trade in tobacco.

a) All respondents indicated that tobacco tended to originate from beyond their borders. That would be because their tax rates probably act as an incentive for outside role players to offset their illicit products within their higher duty jurisdiction.

b) Little support could be found for products being produced and sold within jurisdiction only. Risk is limited by producing the tobacco products for export and then offsetting the product whilst evading the duties and income taxes due in both respective jurisdictions.

c) Various different role players facilitate the value chain of the illicit trade.

d) Investigations and enforcement actions were successful due to multiple foreign and domestic agency interaction.

B. THE FACILITATION OF ILLICIT TRADE IN TOBACCO.

82. The key themes to emerge from this section would also have to relate to question 1 insofar as the methodology utilised by smugglers.

83. **Asia.** Respondent one's answer was indicative that the illicit trade in tobacco is mainly approached from a single passenger perspective as methods of concealment was equated to crew members or airlines and ships make use of private luggage to store said contraband. Respondent two indicated the use of cross border vehicles and pedestrian crossings. The extent hereof is however not known.

Box 5: **Case study – Facilitation of illicit trade**

In 2008, Customs smashed an illicit-cigarette syndicate which was involved in delivering illicit cigarettes to street-level peddlers scattered all over the territory in Hong Kong for local consumption.

The syndicate head had never physically taken part in the distribution of illicit cigarettes. He hired culprits to do the illegal business and controlled them behind the scene. He made use of eight bank accounts (of his sister and wife) to deal with the proceeds of crime.

The total proceeds derived from illicit-trade in tobacco for the period January 2006 to November 2008 amounted to approximately HKD 114 million. The whole syndicate was rolled up in 2008. A total of 17 persons, including the syndicate head and his family members, were arrested with a total seizure of over 10 million sticks of illicit cigarettes.

The three core members of the syndicate and 14 peddlers were charged with money laundering offence(s) and/or forged trade mark offence(s). They were subsequently convicted and sentenced to imprisonment with 5.5 years being the maximum. Assets to the value of HKD 9.18 million were restrained for subsequent confiscation proceedings.

Source: Hong Kong, China

84. **Africa.** Respondent three indicated that cigarettes had in the past been found in trucks (false apartments in tankers and containers), falsely declared in containers, in commercial vehicles, hidden in passenger vehicles, planes, passenger trains, goods trains, border pedestrian crossings and carried across the border by persons (mules). Up to 200 mules at a given time and place can handle more than 1000 Master cases that are carried over the border per night at a single crossing point. The conclusion to be made is that ITT is rife and that diversified methods of distribution are being used.

85. **Europe.** All forms of transportation were sighted by the various respondents. Respondent five stated that as a transit country for trade with neighbouring countries (Such as France, United Kingdom, Germany, The Netherlands) and in accordance with the type of vehicles identified in the national police database (non-representative sample) the goods were transported by road (cars, lorries) and by sea. The port of Antwerp was sighted as an important gateway to Western Europe, especially for unloading containers with Chinese cigarettes. There are also sea links (and railway links) to the United Kingdom. Respondent 11 sighted that counterfeit and illicit white cigarettes in large quantities is primarily smuggled into the Jurisdiction via container or Roll-on Roll-off transport. Genuine cigarettes are predominantly smuggled by passengers and in passenger/small commercial vehicles - often via abuse of cross border shopping limits. It was lastly also mentioned that substantial quantities of counterfeit and loose tobacco are also smuggled via postal packets.

86. **America.** Respondent 12 indicated that ITT is facilitated predominantly through cargo vessels as well as mail and couriers as was also expressed by respondent 11. Respondent 13 mentioned that a significant amount of domestic grown tobacco originating from its jurisdiction could be making its way to illicit manufacturers but the cheaper costs of foreign tobacco from bordering jurisdictions have been intercepted whilst attempts were being made to smuggle the

contraband across borders to manufacturing sites. Container trucks, vehicles, boats appear to be the most common methodology and certainly mis-descriptions and even under-evaluation of shipments have been reported and were done for the purpose of avoiding detection at border crossings. It was also stated that illicit tobacco entered the respondent's jurisdiction primarily through tractor-trailer shipments, marine container shipments, commercial courier and postal shipments and by passengers in the air and highway modes. Respondent four also indicated that the land modality (77%) was regarded the predominant method.

87. **Conclusions:** Various methods were sighted to smuggle the illicit goods. Land, See and air modalities were used or combinations thereof. Methods sighted included:

- Use of trucks with or without false compartments.
- Use of commercial vehicles
- Use of passenger vehicles
- Planes
- Cargo Vessels
- Passenger and goods trains
- Mules
- Roll on roll off transport
- Abuse of cross border shopping limits
- Postal packets
- False declarations
- Under valuation

C. THE FINANCING OF ILLICIT TRADE

88. The purpose of this section is to determine whether the established illicit enterprises are run in isolation and or whether the criminal enterprises are vertically and or horizontally integrated or disintegrated. This is dependent on the size and level of development of the enterprise. The money flows are then indicative of this and may determine the propensity for ML to occur from said predicate offences.

89. **Asia.** Respondent two indicated as much "It is believed that perpetrators obtained start up capital from selling of illicit cigarettes at street level beginning with a small scale of operation. Crime proceeds obtained from small scale ITT operations were then used to buy more illicit cigarettes again and to finance/support the subsequent illicit cigarette business".

90. **Africa.** Respondent three's reply was indicative of more sophisticated networks at play within said respondent's jurisdiction. "Various models are possible here. Most of the illicit trade in tobacco involves the purchasing of manufactured products from the neighbouring countries. Therefore the origin of the finance could be from any source possible. Regarding the illicit trade in undeclared production, cigarettes meant for export and not exported, again the origin of the finance

could be from any source. Sometimes the tobacco products form part of the barter system whereby another illicit product is provided to the supplier".

91. **Europe.** Responses from the European based respondents indicated the use of fronting, cash based businesses as well as commingling with other forms of contraband. Respondent six indicated that: "Apart from legitimate businesses that buy loads of cigarettes with their (illegal) proceeds we find that companies in financial trouble (transporters) are often approached. "Black" money is injected into the company to keep it going but in return the company is later used to import illegal products. The manager of the company in trouble acts as a front man, initially sometimes without his knowledge".

92. Respondent 11 recently commissioned a project to evaluate its knowledge of the criminal finances associated with large-scale tobacco smuggling. The project is however still in its infancy with the respective body responsible for said project having committed to feeding the findings into the FATF typology. It was however noted that in one large-scale cheap white smuggling operation, alcohol fraud was used to acquire the necessary seed capital allowing for diversification into tobacco smuggling. The costs of production, sourcing raw tobacco and labour are kept low by working with a tobacco broker overseas who engages with manufacturers based in Free Trade Zones.

93. **America.** Respondents 12 and 13 once again highlighted the involvement of organised crime with respondent 13 specifically referring to "Organised Crime networks which have had smuggling networks in place since the early days if tobacco smuggling dating to the late 1980's. Many smaller players have seen themselves pushed out of the way or risk repercussions from these networks that then tended to simply consume the smaller groups into their own ranks". It would be interesting to determine what responsibilities these smaller players then had to take on as part of the bigger enterprise *i.e.*, selling of the existing project or sharing of profits from own operations, etc.

94. **Conclusions:** Various methodologies came to the fore.

- Seed capital obtained from small scale sales which are accompanied by a systematic increase in size of the illicit trade.
- Bigger role players absorbing smaller role players within the OCG environment
- The maturity cycles as applied to normal business operations are applicable within this realm as well *i.e.,* introduction, growth, maturity and decline phases.
- Commingling of funds and or products with linkages between the proceeds of illegal alcohol then used for trade in illicit tobacco to eventual bartering for drugs. **Remark.** The ITT then either having its own value chain or making up a part of a more sophisticated/diversified product range.

D. ORIGINS OF ILLICIT TOBACCO

95. It must be noted that only 12 out of the 18 respondents provided information pertaining to where they perceived the illicit tobacco to originate from. The sample is therefore not regarded as representative

enough to warrant serious consideration at this stage. It can however be stated at a rudimentary level that 17 countries were sighted as possible points of origin with China and Dubai being the most sighted. Only two respondents highlighted that illicit tobacco was sourced domestically.

Box 6: **Case study – Origins of illicit tobacco**

In 2009 a smuggling organisation was identified by the Austrian customs investigation service which was responsible for smuggling of about 540 million sticks of cigarettes in the period from 2003 to 2009. The cigarettes were concealed in containers from China behind legal cover loads.

The consignments were customs cleared in Germany, Netherlands, Belgium and Austria. All consignees were given only addresses at various tax consultants but no real business addresses. The companies were all run by the same person who used fake identities for each separate company. After each seizure the concerned company name was not used anymore and all documents were destroyed.

Source: Austria

E. POINTS OF SALE

96. The purpose of this section is to determine the destination (*i.e.,* country, province, city, reservation etc in the case of countries used as transit) for illicit tobacco as well as the nature of the final point of sale per jurisdiction. The answers obtained varied.

97. From a destination perspective most respondents indicated that the illicit tobacco was destined for local consumption within the jurisdiction. Some respondent's answers also indicated that their jurisdictions could also be utilised for transit purposes to other more profitable jurisdictions with the reason being the utilisation of infrastructure which match the smugglers modus operandi. Respondent 6 for instance indicated that transit goods are usually destined for the United Kingdom or France. Respondent 8 indicated that tobacco was predominantly destined for local consumption but were identified as transit goods usually destined for the United Kingdom as well.

98. Respondents 11 and 18 provided more information related to the nature of the point of sale. Localities identified included local pubs, clubs and other centres of the community; alongside legitimate products in small retailers; at local markets and car boot sales; via 'tab' houses and 'international' shops. More rudimentary points of sale listed were tobacco usually sold by peddlers discreetly along streets and alleys.

Box 7: **Case study – *Modus Operandi* on methods and point of sale, counterfeit cigars**

A joint investigation conducted by Federal, State, and local authorities identified two subjects engaged in the counterfeiting of Swisher Sweet cigars. While executing a search warrant, unrelated to the cigarette counterfeiting offense, at the residence of Subject 2, handwritten notes referencing counterfeit cigars were discovered. Surveillances were initiated on both subjects which determined that Subject 2 was receiving cigars (legally) from India, and Subject 1 was receiving counterfeit Swisher Sweet labels from the People's Republic of China. Both items were married into a

counterfeit Swisher Sweet Cigar then sold at convenience stores throughout three southern states. Controlled purchases of counterfeit cigars were conducted utilizing a confidential informant and sufficient evidence was developed to obtain two state-issued search warrants that were executed at the residences of Subject 1, resulting in the seizure of approximately 50 000 counterfeit cigars. Subject 1 and Subject 2 were subsequently indicted for conspiracy and trafficking in counterfeit goods (18 USC 371 and 2320). Both subjects pled guilty to all charges. Subject 1 was sentenced to 12 months incarceration and ordered to pay USD 6 000 in restitution and Subject 2 was sentenced to 18 months incarceration and ordered to pay USD 6 000 restitution.

Source: United States

Box 8: **Case study – Terror financing**

The Real IRA has flooded Ireland with contraband cigarettes and imported counterfeit versions of popular brands and cigarette smuggling has emerged as a top funding source for the organisation. The combined IRA groups have reaped an estimated USD 100 million in proceeds from cigarette smuggling over a five-year period.

Source: United States

F. PRICE COMPARISONS OF LEGAL AND ILLICIT TOBACCO

Table 3: **A price comparison between legitimate and illicit tobacco (USD, per pack of 20 sticks)**

Region	Respondent	Price Legitimate	Price Illicit	Difference
Asia	1	[1]	[1]	0
	2	6.40	3.30	3.10
	14	[1]	[1]	0.00
	17	[1]	[1]	0.00
	18	9.30	3.90	**5.40**
Africa	3	3.50	1.20	2.30
Europe	5	4.60	3.20	1.40
	6	[1]	[1]	0.00
	7	6.90	5.15	1.75
	8	5.79	2.57	3.22
	9	1.00	0.80	0.20
	10	[1]	[1]	0.00

Table 3: **A price comparison between legitimate and illicit tobacco (USD, per pack of 20 sticks)**

Region	Respondent	Price Legitimate	Price Illicit	Difference
	11	10.00	6.17	**3.83**
America's	12	5.00	4.00	1.00
	13	9.00	1.00	**8.00**
	14	1.72	0.83	0.89

1. No information

6. THE MODUS OPERANDI PERTAINING TO THE LAUNDERING OF THE PROCEEDS OF ILLICITLY TRADED TOBACCO

99. The previous chapter provided an overview of the modus operandi followed in terms of the predicate offences to be associated with the illicit trade in tobacco. An estimation of the finances involved was provided which then also underscores the need for perpetrators to launder said proceeds.

100. The questions asked, which if answered, should provide a broad overview of whether money laundering is firstly, associated with ITT and secondly, whether differing techniques might have been identified which could be regarded as unique to this specific commodity. The said questions were:

a) Question 1: How do perpetrators of illicit trade in tobacco launder the proceeds thereof and or finance terrorism?

b) Question 2: What aggregated amount (total as per cases per year since 2005) has been laundered or used to finance terror?

c) Question 3: Which acts of terror can directly be associated with the proceeds that stem from the illicit trade in tobacco?

A. METHODS UTILISED TO LAUNDER THE PROCEEDS ASSOCIATED WITH ITT

101. The answers obtained indicated the extent of the ITT as defined by the varying respondents and their respective law enforcement agencies.

102. **Africa.** Respondent 3 indicated that most of the proceeds associated with ITT were illegally moved to offshore accounts. It was sighted that there were known cases of couriers whose purpose it was to move money to these accounts. These suspects specialised in this function and are said to smuggle the money using private jets and yachts. Some of the operations are run by foreigners who simply move the money to the countries of origin using front companies. Sometimes the money is washed through legitimate operations and consumed locally.

103. **Europe.** Respondent 6 indicated that foreign currency was changed at well-known exchange offices in one of its major centres. An increase in oversight has resulted in "messengers" changing money into small denominations to avoid any suspicion. Money remittance transactions were carried out using well known money remittance agencies. When they were found out as part of a banking investigation messengers were used. It has also been mentioned that money is transported in cash to the final destination. The use of money remitters were also highlighted by respondent 7. Respondent 11 showed that the nature of ML was determined by the scale and size of the smuggling operation. Perpetrators will use a variety of methods to launder their proceeds. It was also mentioned that they will use, hawaladars, cash couriers (either individuals or their continued use of complicit haulage companies), money service businesses and the international banking system. It was also mentioned that no evidence could be found to link the proceeds of ITT with the financing of

terror. The primary theme was that money was used to improve and maintain lifestyles of the perpetrators.

104. **America.** Respondent 12 indicated that the perpetrators involved in the illicit tobacco trade use similar methods to launder the proceeds of their illegal activities as in other criminal schemes. Some of these methods include bulk cash smuggling of currency out of the US and exploitation of the US and international banking systems. Furthermore, they are also known to launder proceeds of their illegal activities through complex trade based money laundering schemes and engage in terrorist financing.

Box 9: **Case study – Contraband cigarettes, money laundering and wire fraud**

In 2004, 10 people were arrested and charged with possession and distribution of contraband cigarettes, wire fraud and money laundering as part of a scheme to smuggle more than USD 2 million in cigarettes bought in Virginia to New York. One subject was arrested in Detroit and found with hundreds of thousands of dollars in wire transfer receipts showing payments to people associated with Hezbollah.

Source: United States

Box 10: **Case study – use of money transmitters**

Company X and Company Y

A multi-agency Federal investigation revealed that Company X was operating as an illegal money transmitting business. The investigation revealed that Company X was involved in the illegal transfer of monies from the U.S. to Pakistan without the proper State of Illinois Transmitter of Money Act (TOMA) license and registration in violation of 18 USC 1960, illegal money transmitting business. Subject 1 was listed as the registered agent/president for Company X and was the primary signer on all the financial accounts associated with Company X.

Company Y was incorporated at the same address as Company X. The president was listed as Subject 2 and is the brother of Subject 1. The secretary of Company Y was listed as Subject 3 and is the son of Subject 1. Company Y registered with FINCEN in March 2005 and received a license from the Illinois Department of Financial and Professional Regulation in March 2005 as a money service business.

Investigative analysis of financial records revealed that Company X transferred in excess of USD 5 994 502 to Pakistan without a license. Analysis further revealed that Company X structured approximately USD 3 954 136 into several domestic bank accounts.

An undercover operation successfully transferred a total of USD 100 200 represented to be proceeds from the sale of counterfeit cigarettes to an unwitting recipient in Karachi, Pakistan through Company Y. Subject 1 conducted each of these transactions with the undercover and wilfully structured USD 97 000 in order to avoid filing a Currency Transaction Report (CTR). Two of these undercover transactions were conducted at the residence of Subject 1.

As a result of the investigation, Subject 1 was indicted on 35 counts of structuring in violation of 31

USC 5324 and 18 USC section 2, and subsequently pled guilty to money laundering in violation of 18 USC 1956 and was sentenced to two years probation.

Source: United States

Box 11: **Case study – Money laundering stemming from ITT (Counterfeits)**

Cigarette smuggling

This investigation targeted a cigarette smuggling and distribution organisation operating in the North-eastern United States. The organisation obtained and sold genuine/counterfeit and taxed/untaxed cigarettes to convenience stores in the North-eastern United States. The proceeds from this organisation were believed to be laundered through various methods including, including bulk cash smuggling.

Federal Authorities seized approximately USD 61 625 in US Currency from an individual associated with the target (TARGET 1) of the investigation. This seizure was the result of an enforcement action initiated from a communication between the individual and his associates (TARGET 1 and a third individual) regarding the purchase of 30 master cases of un-taxed cigarettes, valued at approximately USD 63 000. Pursuant to a consent search, approximately USD 61 625 was discovered in the vehicle the first individual was operating. The first individual did not claim ownership of the currency, but provided incriminating statements as to his involvement in the purchase and transportation of stolen merchandise and untaxed cigarettes. The currency was seized and was administratively forfeited.

Source: United States

105. Respondent 13 gave a substantial account of ML to be associated with ITT. The illicit tobacco trade use all the standard methods of money laundering, from the use of cash to purchase goods, property and deposit to the accounts of financial institutions, to the use of professionals such as lawyers and accountants when organised crime groups are involved. It has been noted that illicit tobacco funds have been moved between first nations communities using the "bulk cash smuggling method". It should also be noted that several first nations communities are found on and covering the border between the United States and Canada. This allows illicit funds to be moved between the two countries in these regions.

106. In reviewing over 40 ML/TF FIU case disclosures linked to illicit trade in tobacco, several money laundering methods were identified, including:

- **Commingling** by mixing illicit revenues with the revenues of a non-profit organisation, cigarette manufacturers, auto parts businesses, pizza parlour businesses, frozen food companies, financial services, cigarette wholesale distributors, construction companies, transportation companies, private casinos and bars/night clubs.
- **Smurfing** consists of several cash deposits by members of the same group.

- **Structuring,** which involves numerous transactions (deposits, withdrawals, transfers), or a number of people, or high volumes of small transactions, or numerous accounts to fall below the reporting threshold at banks and money service businesses (MSBs). Currency exchange transactions at MSBs.
- **Use of nominees or 3rd parties** (including family members) to deposit cash or cheques into accounts then transfer the funds to a beneficiary account all to obscure the identity of persons controlling the illicit funds.
- **Use of lawyers and/or accountants** as professional intermediaries in the movement of funds. Used both to obscure the identity of the person controlling the illicit funds and the source of funds.
- **Complex movement** of funds to hide the origin of funds. For example, cash deposits made at one institution and issuing cheques to be deposited at a third institution and (again) issuing cheques payable to third parties.
- **Refining at casinos** by exchanging USD 20 dollar bills into USD 100 at casinos. As well as purchasing casino chips with no gaming activities, then requesting monetary instruments (ex: casino cheques).
- **Purchase of real estate property** to invest illicit proceeds in high-value negotiable goods in order to obscure their source.
- **Investment in various entities**
- **EFTs to beneficiaries**
- **EFTs to individuals/entities linked to terrorist organisations**

B. AGGREGATED AMOUNTS (TOTAL AS PER CASES PER YEAR SINCE 2005) TO BE ASSOCIATED WITH ML/TF

107. Only two of the 18 respondents provided an answer to this question. Lacking data makes it therefore unfeasible to provide answers to this question.

C. ACTS OF TERROR OR TERROR FINANCING TO BE ASSOCIATED WITH ITT

108. Phony cigarette tax stamps were found in apartments used by the perpetrators in the 1993 bombing of the World Trade Centre in New York.

Box 12: **Case study – Acts of terror and the financing thereof to be associated with ITT**

Terrorist Financing and Cigarette Smuggling

Subject was born in Lebanon, moved to the United States illegally in 1992 and lived there by virtue of three sham marriages to US citizens until his arrest on 21 July 2000. Subject, along with two of his brothers and 22 others, were indicted and convicted of providing material support to Hezbollah, cigarette smuggling, money laundering, conspiracy, racketeering, and immigration fraud. His guilty

verdicts rendered by the jury were upheld by the Supreme Court of the United States.

Subject was a student and member of Hezbollah as a youth in his home country and moved to the United States on a Hezbollah-driven mission. He accomplished his mission by creating a criminal enterprise which smuggled more than USD 8 million worth of cigarettes from North Carolina to Michigan with profits sent to Hezbollah in Lebanon. He purchased businesses in the U.S. and preached radical Muslim fundamentalism as he led a clandestine terrorist cell in Charlotte, North Carolina and raised funds for the cause through cigarette smuggling.

During his imprisonment and while awaiting trial, he ordered the murder of the prosecuting attorney and the bombing of Charlotte's federal courthouse. The 2002 trial was the first in the country of a federal "material support to a designated terrorist organisation" charge. The investigation and prosecution involved law enforcement cooperation at every level: state, federal, and international, involving the substantial assistance of Canadian intelligence officials.

The case was investigated by agents and officers of the Federal Bureau of Investigation, Alcohol, Tobacco, and Firearms, Department of Homeland Security–ICE/Homeland Security Investigations, US Citizenship and Immigration Services, IRS Criminal Investigations, the Charlotte-Mecklenburg Police Department, and the Iredell County, N.C. Sheriff's Office. These law enforcement agencies received substantial assistance from the Canadian Security Intelligence Service and the Royal Canadian Mounted Police.

Source: United States

7. A RESPONSE FROM LAW ENFORCEMENT AND SUPPORTING AGENCIES

109. Preceding chapters have shown the nature and extent of the illicit tobacco trade is voluminous, intricate and has far-reaching consequences across varying illicit value chains. Those engaged in the trade operate across various jurisdictions and perform multiple functions in the growing, production, supplying and distribution of the product.

110. The purpose of this chapter is to highlight the response to the illicit tobacco trade by differing agencies across the globe. This will not only encompass the actions of governments within the varying jurisdictions but also highlight the extent and / or lack of cooperation amongst these bodies to curb the phenomenon. Four primary agencies were identified as the most relevant bodies involved in the counter illicit tobacco trade environment. They are:

a) Customs Services

b) Financial Intelligence Units/Centres

c) Relevant Law Enforcement (*i.e.,* Police Services, Federal agencies etc)

d) Taxation Authorities

111. The chapter is to highlight similarities in approaches to better determine what could be considered best practices regarding operational and intelligence best practice, with special emphasis on the inclusion of money laundering as an offence.

A. CUSTOMS AUTHORITIES

112. The overarching themes emerging from the responses of Customs Authorities are:

a) A disconnect between the investigation of the predicate offence and any associated money laundering investigation(s). Many of the Customs Authorities do not have the capability or authority to undertake a ML investigation and if a cross-agency platform is not in place, the focus remains on the predicate customs or tax offences.

b) The importance of information collection and sharing, nationally and internationally, to effectively develop strategies to respond to the threat. While many of the Respondents collect relevant trade data, their answers do not confirm to what extent this is analysed and trends or patterns are identified.

113. On such matters, the World Customs Organisation (WCO) has an important role to play in facilitating dialogue between international partners. While several Respondents identified the WCO as a key partner, it noted in its Customs and Tobacco Reports for 2008, 2009 and 2010, and not all countries were returning data to the Customs Enforcement Network (CEN) database, which can compromise the ability to quantify the illicit tobacco trade. This data is vital in providing an accurate picture of the national and international risk that the ITT presents, as well as identifying possible developments or new methodologies with any associated money laundering.

114. In recognising the risk from the illicit tobacco trade, the WCO states that "…tobacco and cigarette smuggling remains a global problem, which continues to increase in spite of Governments' enforcement strategies." In tackling the problem, the WCO notes "…that many countries are the targets of cigarette smuggling so enhanced multi-agency cooperation at the national level is urgently needed. The WCO has been working with other regional and international organisations in an attempt to identify the best possible enforcement strategies to counter this problem, including joint Customs enforcement projects."

115. The following is a summation of answers as received from the various respondents.

CUSTOMS AND THE CONDUCTING PREDICATE AND MONEY LAUNDERING OFFENCES RELATED TO THE ITT

116. Table 4 captures the variety of approaches used in tackling the illicit trade in tobacco and related money laundering investigations. Many of the respondents included additional narrative clarifying the approach within that jurisdiction, which has been included to provide context for the subsequent analysis of the data.

Table 4: **ITT and Customs jurisdictional approaches**

Resp. No	Do Customs investigate ITT	Do Customs investigate money laundering	Description
1.	Yes	No	Money laundering investigations are conducted by the police agency.
2.	Yes	Yes	
3.	No	No	No, the Customs Border Management (CBM) division through the Customs Border Control Unit (CBCU) conducts interventions on illicit trade in tobacco. The Revenue authority, of which CBM is a division, has an investigating arm in the National Investigations unit within the Enforcement division, which conducts the appropriate investigations. CBM conducts interventions including all the follow-ups that pertain to those specific interventions. The CBM's function is to handle the customs contraventions. The cases on this trade are investigated within the Enforcement division; however investigations into money laundering are handled by the police (commercial crimes).
4.	N/A	No	The responsibility for money laundering rests with the FIU.
5.	Yes	No	The matter is reported to the FIU.
6.	Yes	No	
7.	Yes	Yes	The Customs Investigations Directorate and the National Judicial Customs Department conducts investigations into tobacco smuggling. For money laundering cases, Customs works in conjunction with other financial investigation services.
8.	Yes	Yes	Next to the Customs Investigation Service also other Customs divisions, mainly responsible for checking/controlling the trafficking of persons and goods, carry out investigations
9.	No	No	Collected information is forwarded to other law enforcement agencies for the development of the investigations.

Table 4: **ITT and Customs jurisdictional approaches**

Resp. No	Do Customs investigate ITT	Do Customs investigate money laundering	Description
10.	Yes	No	
11.	Yes	Yes	Revenue & Customs has operational responsibility for investigating tobacco smuggling. If its Criminal Investigation directorate has adopted the case, a financial investigator is appointed to develop the appropriate confiscation investigation, which may include money laundering offences. If the investigation is civil in nature, there is no confiscation or money laundering investigation conducted in tandem.
12.	Yes	Yes	A separate investigative agency has The Customs authority and is responsible for enforcing customs laws within the respective jurisdiction, and conducting investigations related to tobacco smuggling. These investigations include, but are not limited to, the domestic and international smuggling of cigarettes; counterfeit or genuine, trafficking in counterfeit cigarettes; trafficking in stolen cigarettes; smuggling of cigarettes in violation of embargoes; and international money laundering investigations where one of the underlying crimes is tobacco-related.
13.	Yes	No	In this case, the Customs authorities work closely with police with initial information stemming from customs.
14.	Yes	N/A	
15.	No	N/A	Customs is represented on the country's Money Laundering Reporting Authority.
17.	Yes	No	Customs would conduct investigation into the illicit tobacco trade, but if criminal activity is involved the case would be passed to the Judiciary Police. The authority to investigate money laundering activities, including trade related offences, is vested with the Anti-Money Laundering Division of the Judiciary Police
18.	Yes	NA	Offences with suspected money laundering links are referred to the Commercial Affairs Department for further investigations
19.	Yes	Yes	There is a government institution which in is charge of tackling money laundering, so these cases are referred to this agency (MASAK). Customs inspectors can be assigned to conduct some aspects of a money laundering investigations on behalf of MASAK.
20.	Yes	No	
21.	Yes	No	Investigations into money laundering is referred to NAM POL
22.	Yes	No	

117. **Conclusions:** The majority of Customs authorities can investigate any customs offences related to the ITT. However, only around half of these authorities would also conduct a money laundering investigation, with the remaining respondents referring the matter to other agencies, such as the Police, the Financial Intelligence Unit (FIU) or a specified anti-money laundering agency. In such circumstances, it is possible that cases suitable for money laundering investigation are not pursued, due to jurisdiction and enforcement limitations of the Customs authority concerned. In such cases, unless detections are referred for financial investigation elsewhere only predicate

customs or taxation offences are likely to be pursued. This may be indicative of the lack of money laundering investigations associated with the illicit tobacco trade.

118. The following case study highlights a typical investigation into the predicate offence, which also included a money laundering angle. It also reinforces the need for international agreement in tackling the risks posed by the illicit tobacco trade.

Box 13: **Case study – Press release, customs related investigations**

The United States Attorney for the Southern District of Florida and the Special Agent in Charge, U.S. Immigration and Customs Enforcement (ICE), Office of Investigations, announced that an individual was arraigned on an indictment returned by a federal grand jury in Miami yesterday. The charges were conspiracy to commit mail fraud and wire fraud in violation of 18 U.S.C. § 1349, mail fraud in violation of 18 U.S.C. § 1341, and smuggling goods out of the United States in violation of 18 U.S.C. § 554. The individual was released pending trial on bond on February 20, 2009.

According to the indictment and an affidavit filed with the complaint, the investigation revealed that an organisation smuggling cigarettes out of the Port of Miami operated out of Spain, the United Kingdom, Ireland and Florida. The individual indicted ran the Miami portion of the operation, arranging for the purchase of hundreds of cases of cigarettes from Panama and the transportation of those cigarettes into the Port of Miami.

They then arranged for the purchase of other cargo, such as wood flooring and building insulation material, for use as cover loads to conceal the cigarettes, which were re-packed with the cover load material. False bills of lading were prepared that only declared the cover load material and were subsequently presented to the shipping companies and overseas customs services. No duties or taxes were paid on the cigarettes.

Information contained in the affidavit linked the defendant to two separate occasions consignments of approximately 13.3 million cigarettes shipped to Ireland and the United Kingdom respectively. Based upon the false bills of lading, custom duties and taxes paid on these shipments were approximately, USD 2 900 and USD 2 500, respectively. The true customs duties and taxes that should have been paid on these shipments were USD 2.1 million each.

The Attorney for the Southern District of Florida thanked Immigration and Customs Enforcement, Office of Investigations, and OLAF for their outstanding joint working on this case. Extensive assistance was provided by law enforcement agencies from Ireland, the UK, Germany and Spain as well as the U.S. Department of Justice, Organized Crime and Racketeering Section, Criminal Division.[1]

1. *Related court documents and information may be found on the website of the District Court for the Southern District of Florida at http://www.flsd.uscourts.gov or on http://pacer.flsd.uscourts.gov.*

Source: OLAF (2009)

119. The following section is to determine whether any mechanisms were put in place to ensure a cross-cutting approach in tackling both the predicate customs offences and any related financial / money laundering investigations.

CUSTOMS PARTICIPATION IN JOINT FINANCIAL INVESTIGATION/MONEY LAUNDERING TASK TEAMS

120. Only six of the 22 respondents indicated its Customs authorities do not take part in any form of joint financial investigations.

121. Respondent 8's Customs Investigation Service is part of a series of Joint Financial Investigation Groups, established in 1992. Within the Federal Criminal Police Office and the Bureaus of Criminal Investigation, were established specialised departments for financial investigations, where customs officials and the police work together as Joint Financial Investigation Groups.

122. Respondent 18 indicated that although there is no formal task force, relevant agencies including the Customs and the Commercial Affairs Department, have conducted joint and parallel money laundering investigations.

123. Exploring these differing approaches further, the following section sought to determine what impediments (if any) Customs authorities experienced in conducting investigations into the illicit tobacco trade.

IMPEDIMENTS ENCOUNTERED WHEN CONDUCTING INVESTIGATIONS

124. Only seven respondents replied making it difficult to extrapolate these as the main common difficulties experienced. However, for those who did reply, two primary themes emerged:

a) Jurisdictions can struggle with the deployment of resources in tackling all risk areas.

b) There is a need for better cooperation and coordination between jurisdictions.

125. The following feedback from Respondent 11 captures the breadth of the issues articulated by the other six respondents:

a) Difficulties in aligning available resources at mutually convenient times to execute operational strategies that cover the range of risk areas associated with the illicit tobacco trade.

b) Sharing relevant intelligence and information because of legislative difficulties for domestic and international matters.

c) Difficulties with IT systems hampering effective information sharing or more importantly extraction and evaluation.

d) For operations with an international dimension, it can be difficult to tackle the illicit tobacco market upstream, particularly if no offence has actually been committed in the source country (e.g. manufacture of cheap whites / purchase of genuine brands).

126. **Conclusion:** While the investigation of tobacco offences and any parallel money laundering offences occurs as standard, capturing strategic and tactical intelligence is critical to develop a more holistic understanding of the risks of the illicit tobacco trade and enhance the operational impact.

INFORMATION COLLECTION, ANALYSIS AND MANAGEMENT

127. All but seven of the respondents collected customs data, including the details in the question asked. Many will also seek additional information from a wide variety of other sources, including national and local police forces, immigration and border control authorities, enforcement agencies in neighbouring countries, the tobacco industry, health providers and health policy makers. This gives the Customs authorities an extremely broad information base to work from and supports enforcement activity geared to predicate customs and tax offences. In some cases, it may help Customs authorities quantify the financial risks attributable to the illicit tobacco trade.

128. This breadth of information is best illustrated by Respondent 12, which detailed the customs information it collects: "framework of fields that assist which are entry number, entry type, surety number, bond type, port of entry, entry date, importing carrier, mode of transport, country of origin, import date, export date, bill of lading/air waybill number, manufacturer ID, exporting country, immediate transportation number and date, missing documents, foreign port of loading, port of unloading, location of goods, consignee number, importer number, ultimate consignee name and address, importer name and address, description of merchandise, HTS number, gross weight/manifest quantity, net quantity in HTS units, entered value, charges, relationship, HTS rate, duty tax, broker/filer (name, address, telephone number, and number)"

129. However, several respondents identified opportunities to widen the breadth of information collected. For example, Respondent 11 "engages with the key Tobacco Manufacturers who are undertaking their own efforts in analysing and quantifying the risk from the illicit tobacco trade". Respondent 21 does not currently carry out trade-based analysis but "a risk management section about the illicit tobacco trade has been created and such analysis will be done in the near future".

130. As noted, a small number of respondents indicated that no information is collected, but it would be disingenuous to draw too many inferences. For example, is it reflective of the extent of illicit tobacco trading in the jurisdiction or its importance against other crime types? Alternatively, was it too difficult for the respondents to research the information from their Customs authorities? Initially Respondent 1 answered, "No information" when asked to describe information collected but was able to confirm in the following question "based on customs information regarding shipped goods, analysis is being conducted in order to crack down on illegal export/import". Respondent 14 left the question regarding information collected blank but confirmed in the following question that analysis of trade information took place with the information collected from the Police agency and the market control agency.

131. When the captured trade data is analysed, just over half of the Respondents noted that illicit tobacco goods were usually trans-shipped. Some respondents like Respondent 5 listed generic routes – "East/southeast to Rotterdam, United Kingdom and France", while others like Respondent 3 gave more precise routes, suggesting it is both a point of distribution and a nexus point for smuggling into neighbouring countries:

- UAE (Dubai) – South Africa,
- UAE (Dubai) – Namibia – South Africa,
- UAE (Dubai) – Namibia- Angola – Botswana/Namibia – South Africa,

- China – South Africa
- China- Namibia-South Africa- Zambia
- Zimbabwe – South Africa – Mozambique…"

132. However, not all Respondents provided data on the origin or destination of suspected loads of illicit tobacco products so the answers are indicators rather than trends. Dubai was noted as a key jurisdiction for the production and distribution of cheap white cigarettes, while China was linked heavily to the production of counterfeit cigarette products. Some respondents also identified production sites in Eastern Europe and the Far East.

133. Unsurprisingly, nexus points were spread across the globe. Due to the fluid nature of the criminality, it is difficult to pinpoint specific jurisdictions because as soon as the smugglers perceive an increased risk in detection or other instability factor, they will identify a new methodology or nexus point limiting the disruption to their supply chain. The receiving countries were predominately in Western Europe, with the United Kingdom and Republic of Ireland featuring in a number of responses.

SHARING OF INFORMATION

134. The majority of the respondents provided positive feedback, mentioning a wide array of local and international bodies as potential sources of information. These International bodies included; the World Customs Organisation (WCO), Europol, Interpol, SECI Centre, OLAF the European Anti-Fraud Office as well as other countries' customs and law enforcement agencies.

135. Another positive element is the liaison with national and overseas Financial Intelligence Units (FIUs). The nature of the requests are dependent on the extent of the investigation and trends and patterns which may be unique to specific jurisdictions, but overall it confirms the value of such Units in supporting predicate and money laundering investigations. Some of the responses about sourcing information were:

a) "If required, Customs seeks information from the FIU for information on Suspicious Transaction Reports, Police for criminal records, Immigration Department for passenger movement records, Inland Revenue Department for tax returns and Company Registry for company records, etc. Information will also be sought from overseas LEAs. Requests for information from overseas FIUs on STRs will be routed through the local FIU. Information on the modus operandi of illicit cigarette syndicate(s), persons and companies, shipment and bank records etc, would typically form part of the requests for information".

b) Respondent 8 highlighted existing structures within the WCO domain. "Gathering information from internal partners results already logically from the organisational structure of the Customs investigation service. In the framework of mutual legal assistance treaty in criminal and administrative matters the authorities also receives information from international partners. The information gathered from international partners during investigations depends on the needs of the investigators. Apart from that, international partners forward case independent information which is usually shipment data."

c) Respondent 11 identified a number of information requests depending on the scope and scale of the investigation, including the assessment of risk to revenue:

i) The location of tobacco production or if unknown, the jurisdiction(s) where the goods are exported to for onward transportation.

ii) The key individuals involved in the various aspects of the smuggling operation.

iii) Financial intelligence including how the goods are purchased and any other costs generated in smuggling the goods into the jurisdiction – *i.e.,* distribution, storage, security / risk management.

iv) The methodologies used to launder the profit generated from the sale of the smuggled goods and the jurisdictions used as money laundering nexus points and final destination.

v) The location of any assets associated with known individuals and the opportunities of collaborative asset recovery / denial work."

136. Several of the Customs authorities have officers deployed in foreign jurisdictions to aid operational work and promote international intelligence sharing. Respondent 11 has a network of Fiscal Crime Liaison Officers (FCLOs) based in a number of jurisdictions across the world and they receive tasking about supporting operational activity or building and developing intelligence or relationships with law enforcement partners about key assigned matters, including tobacco smuggling. These overseas law enforcement partners have also provided support with overseas surveillance and assisted with controlled deliveries. The service also contributes to international forums such as the WCO, OLAF and ASEM.

137. Respondent 13's reply should be noted due to the different perspective to illicit tobacco trade in its country "While we are a participant with the World Health Organisation's (WHO) Framework Convention on the Tobacco Controls (FCTC), most domestic issues pertaining to illicit tobacco are unique in nature to our jurisdiction with the occasional tie to another countries who may source precursors but overall very little international interactions"

138. The following case study illustrates the importance of international cooperation and information sharing in targeting and interdicting against a sophisticated organised crime groups with links to counterfeit cigarette smuggling in the US, France and Belgium. It also highlights the value that international bodies such as OLAF have in facilitating dialogue between overseas investigative agencies.

Box 14: **Case study – Multiple jurisdiction case of ML to be associated with ITT**

Case Barrie

On 28 September 2005, Customs in Antwerp harbour carried out administrative verification on container no. TEXU 534506-7 arrived on 22 September 2005. Some aspects particularly drew customs officers' attention.

- The title of the bill of lading: « Delivery bamboo articles

- The Origin: China – Destination: Belgium
- Final destination: Rue de Brabant in 1030 Brussels, in the neighbourhood well known for counterfeiting of all sorts of goods. On this suspicious ground, customs decided to put in place a controlled delivery.

A truck loaded with the container left Antwerp harbour in the direction of Brussels. However, instead of going directly to Rue de Brabant, the truck went to Chaussée de Ninove at 1070 Brussels after having picked up one Alpha Mamadu BARRIE.

The address was found to be that a company called SHURGARD SELF STORAGE. Customs officers stopped and controlled the truck and the container. Instead of bamboo items, the container was loaded with 9 800 000 counterfeit cigarettes Marlboro red. It also appeared from the controlled delivery that the cigarettes boxes were sealed with a false tax seal. A quick estimation was made with the container then holding tobacco amounting to a fraud of about EUR 2 million. Customs informed the Brussels prosecutor's office at the end of the preliminary verifications and the Federal judicial police (Economic and financial crime unit) continued to investigate the case.

The Investigation

The 1st Phase

When under arrest, the conveyor, Alpha BARRIE, carried EUR 1 150 and 3 mobile phones (even though he had no other income other than social revenue). He had committed similar acts in 2004, for which he had been indicted and expected the trial. He also had 3 rental contracts between SHURGARD SELF STORAGE and a so called Mahmood BARRY (the phone number on the contract was actually BARRIE's number).

Then BARRIE's car was searched and the following goods and documents were found:

- Another rental contract at SHURGARD SELF STORAGE used the name Mahmood BARRY;
- A bedroom's (magnetic) card at SHERATON Brussels.

We asked Alpha BARRIE why Mahmood BARRY rented storage at SHURGARD SELF STORAGE. Alpha BARRIE explained that Mahmood BARRY's ID card was given to him by a person called "Mr. UNIT" for the renting several boxes at SHURGARD SELF STORAGE. He declared that he did not remember why he was asked to rent these boxes for Mr UNIT. We carried out a search at Alpha BARRIE's. There a business card TUNG CHUN FAI INTERNATIONAL – TONY LAM was seized. Alpha BARRIE declared that Mr UNIT is actually Mr. Tony LAM (from Asia). Alpha BARRIE also said that he needs to contact Tony LAM; he dials a specific mobile phone number. He knows that when he is in Belgium, Mr. LAM drives a grey BMW. He said that Mr. LAM has already been with him at the SHURGARD's boxes in Brussels.

We were then informed that a second container could be linked to the container seized on 28 September 2005 and was to be delivered in Mechelen. This second container is linked to Mamadou Bailo SOW. It comes from verifications that Sow is known from French Justice and that Alpha BARRIE is involved in another legal cases in Belgium (BARRIE I in 2004).

The link between the two containers was the beneficiary company mentioned on the bills of lading

namely FIMIDRA. Customs officers indicated that this company could be linked to seven more containers. According to the customs data base, the manager of FIMIDRA was also involved in another company named EUROPEAN CAR with a further two containers to be linked to lastly mentioned company.

This amounted to a total of 9 containers inbound from China, including the 2 seized on 28 September 2005. A quick evaluation indicated that a total of about 100 million smuggled cigarettes have been imported into the target country and that this represented a fraud of more or less €16 million. Customs furthermore confirmed the participation of: BARRY Alphonse, SOW Mamadou, and VERSTREPEN Stéphanie.

The origin of the counterfeit cigarettes was obtained from Chinese authorities through the assistance of OLAF (European anti-fraud office). EUROPOL also indicated that SOW, BARRIE Salam and SANI Lassana were furthermore involved in criminal proceedings in France. SANI Lassana was indicted for money laundering in Belgium EUR 285 000.

During the investigation (2006), Mahmood BARRY was involved in another case of counterfeit perfumes and cigarettes. The investigating magistrate required OLAF's assistance. OLAF informed us that another container had been seized in Shanghai on 9 September 2005. It contained 9 750 000 cigarettes for the company FIMIDRA in Brussels.

Through contacts with the US authorities, OLAF learned that a person named LAM Wei Tung had been arrested in Arizona. He had contacted a Belgium national named Corinne THISSEN from prison. Further investigations revealed that LAM was involved in an additional 2 cases in the US, in Arizona & California. To summarise:

1. The investigation that revealed that an organised group was involved in the smuggling of counterfeit cigarettes. Its financial impact was regarded as significant.
2. The indicted persons were involved in 9 related criminal proceedings.
3. To be more effective, research/investigation was streamed in 8 points of focus.
4. A total of 11 containers could be linked with the company FIMIDRA (and/or its managers). This observation was made on the basis of the bills of lading.
5. FIMIDRA was found to be a shell company owned by BARRIE Salam since 2005.
6. This company would be the beneficiary of the container seized in Shanghai on 9 September 2005.
7. To purchase FIMIDRA, BARRIE Salam received financial and technical support from CHASSEUR (stepfather of Corinne THISSEN), SANI and CEUPPENS.

The 2nd Phase

2nd issue / trail for the investigation focused on the rental contracts and taking account of the fraudulent use of an identity card. A copy of the video surveillance of SHURGARD was seized. We found out that on 27 September 2005, in the evening, an African person driving a metallic grey car arrived. Here he met SHURGARD and inspected the premises with SHURGARD showing the capacity of the storage area. Alpha BARRIE was provided with a document that proved the rental of storage

boxes. This document was found in his vehicle when searched. Once the administrative arrangements were made, Alpha BARRIE joined back an Asian who was then identified as LAM Wei Tung. BARRIE proceeded to show to LAM the boxes he just rented. BARRIE and LAM left the storage area together. LAM goes back to BARRIE's car. BARRIE confirms the rental of the boxes. Then they leave together with Alpha BARRIE's grey car.

The 3d Phase

3rd issue / trail for the investigation: WAREHOUSE IN MECHELEN: concerning the 2nd container (dated 28 September 2005), the bill of lading indicated some elements similar to those of the container seized at the SHURGARD. On this ground, the warehouses Mechelen were searched. The 2nd container was found and seized. The security seals were on the floor and rental contracts were found that demonstrated links with 5 containers which had been loaded with smuggled goods. In Mechelen (at least 3 containers), it was established that BARRY Alphonse and VERSTREPEN Stéphanie with a third unidentified person rented the warehouses using false identity.

The 4th Phase

4th issue / trail for the investigation: TRANSPORTS MAGEMAR: on the basis of elements of proof found during the search and statements, we found that 4 containers were directly related to CHASSEUR, BARRIE Alpha, BARRIE Salam and LAM Wei Tung.

The 5th Phase

5th issue / trail for the investigation: SHERATON HOTEL: A hotel magnetic key was seized in Alpha BARRIE's car. It was a card from the SHERATON in Brussels. On this ground, the hotel was requested to communicate the dates and identity of the person who paid for the room. It was KITTY Jie Fan, LAM Wei Tung's wife. The dates match with the dates of arrival of 4 containers.

The 6th Phase

6th issue / trail for the investigation: in FRANCE: two French cases were reviewed. These cases related to 7 containers. The bills of lading show the same features than those targeted in Belgium. It was found that the scheme used the same modus operandi in France as in Belgium, *i.e.,*:

- China Belgium France
- Similar Bills of lading
- Involvement of FIMIDRA (company)
- Involvement of SOW – BARRIE Salam – BIDANESSY Séta – LAM Wei Tung

We learnt that

- LAM bought a house in France for EUR 586 000 in 2003;
- He had several issues with customs authorities concerning cash transportation while entering in the UK, France and Senegal. When we returned from France, we verified whether LAM had similar issues in Belgium. In 2003, he did not declared USD 350 000 and EUR 900 000 while arriving at Brussels airport. He declared to the customs officers that he needed large amount of cash for his business in Africa.

The 7th Phase

7th issue / trail for the investigation: while executing a mutual legal assistance in conjunction with OLAF (EU anti-fraud office) in the US, contact was made with US law enforcement agents – ICE in Arizona. Information was shared with respect to a consignment of counterfeit shoes. In that case LAM had been convicted to 30 months custody. Investigators also met with ICE officials California. They also gave us access to their information concerning the trafficking of counterfeit shoes and cigarettes. The information confirmed the active participation of Corinne THISSEN, CHASSEUR's stepdaughter, in the trafficking in counterfeit cigarettes with LAM Wei Tung. It also appeared that LAM had a problem concerning a declaration of cash at JFK airport in 2006 (USD 131 000).

The 8th Phase

8th issue / trail for the investigation: EUROPEAN CAR: 2 containers could be linked to the company EUROPEAN CAR. CEUPPENS, Alpha BARRIE and CHASSEUR were involved in taking over this second shell company. The company was to be used as FIMIDRA had become too exposed and was by then well-known to Belgian Judicial Authorities. One of the two last containers was related to Alphonse BARRY and contained counterfeit cigarettes 'BENSON & HEDGES' (more probably for the UK black market).

Investigative Findings

At the end of these investigations, the investigating magistrate kept the following offences :

- Forgery and use of forged documents;
- Criminal organisation;
- Money laundering;
- Counterfeiting of goods;
- Offences to the Customs and excise legislation.

On this basis, LAM Wei Tung was extradited in July 2009 from the US to Belgium where an arrest warrant had been issued against him.

In April 2010 the criminal organisation trial started. The court decided as follows:

- LAM Wei Tung as head of the criminal organisation;
- CHASSEUR Roger member of the organisation;
- Company FIMIDRA as member of the organisation;
- BARRIE Alpha & BARRY Alphonse as members;
- CEUPPENS Daniel & BARRIE Salam as architects of the fraud scheme.

In total, cumulated penalties were established as follow:

- 19 years and 4 months of imprisonment;
- Confiscation of 2 containers + 2 cars + EUR 1 561 154;

- Criminal fines: EUR 435 500;
- Tax fines: EUR 62 474 594.

Source: Belgium

139. **Conclusions:** It is apparent that Customs authorities capture or can access a huge library of information, which could support a robust analysis of the risks to their jurisdiction. A key issue is the extent to which information management systems supports existing investigative work and identifies new risk areas, with appropriate analysis of the data to support the development of strategies and policies to help combat the illicit tobacco trade. The issue of data extraction and analysis is explored in more detail in the following section.

UTILISATION OF DATABASES

140. The majority of Respondents hold databases, which contain customs information based on data entered on custom declaration forms. Respondent 7 has a searchable database that "contains the details of the import and the export declarations of the last three years"; however, no other respondents confirmed how far back they kept records on their own databases.

141. Just under half of the respondents confirmed they were able to cross-reference this information with other government databases. For example Respondent 11 indicated that while "no specific intelligence database is held even though we do hold details of goods and seizures, whenever the service commences an investigation into an individual or Organised Crime Group a number of basic intelligence checks are completed. These checks scan across a variety of intelligence databases, including the FIU, Companies House, credit reference agencies, the Police National Computer and any relevant customs owned databases to evaluate our previous dealings (if any) with the suspected individuals." .

142. However, access to such wide-ranging data is not without its difficulties, Respondent 13 highlighted the issue of access to sensitive information and the need to obtain the correct permissions; "personal or industry documents can only be obtained through a judicial authorisation if we are conducting a criminal investigation as not all information can be feely shared."

143. **Conclusions:** The responses reconfirmed several of the issues raised when the Customs authorities were asked about the impediments to successful illicit tobacco trade investigations. It is clear that more needs doing internationally to piece together a global intelligence picture about the continued and expanding threat from the illicit tobacco trade.

INDICATORS AND RED FLAGS OF ML AND OR TERROR FINANCING TO EMANATE FROM ILLICIT TRADE IN TOBACCO

144. Very few Respondents completed this question. Of those that did, three Respondents were able to list some indicators of money laundering or terror financing emanating from the illicit tobacco trade. Two respondents stated that there was "no relation to such activity to date". The indicators and red flags included:

a) Deposit of a large amount of cash in bank accounts.

b) Abnormal and frequent bank transactions without legitimate business reason(s).

c) Payments to unrelated third parties via:

   i) Cash.

   ii) Wire transfers.

   iii) Checks, bank drafts or postal money orders from unrelated third parties,

d) False reporting: such as commodity misclassification, commodity over-valuation or under-valuation.

e) Carousel transactions: the repeated importation and exportation of the same high-value commodity,

f) Commodities being traded do not match the business involved,

g) Unusual shipping routes or transhipment points,

h) Packaging inconsistent with commodity or shipping method.

i) Double-invoicing

B. LAW ENFORCEMENT

145. The following section follows the same train of thought as covered under customs. The purpose for the differentiation is to determine the differences in approaches in terms of the investigation of ML and or TF to emanate from ITT when compared amongst jurisdictions and their respective agencies tasked with conducting the investigation as well as determining whether certain best practices can be ascribed to differing models.

146. The first differentiator lies with which department has the mandate to conduct the ML investigation. In certain cases as mentioned above, the customs authorities have the mandate to conduct the ML investigation. The opposite model as mentioned implies that customs authorities provide relevant information to law enforcement to pursue money laundering investigations.

147. It should therefore be noted that some of the answers provided in this section will be the inverse of the aforementioned but that focus is to be placed on law enforcement's approach as opposed to looking solely at the role of customs. The following section will therefore aim to highlight this.

THE NUMBER OF ML/TF CASES/INVESTIGATIONS TO STEM FROM THE ILLICIT TRADE IN TOBACCO SINCE 2006

148. From a money laundering perspective, respondents indicated internal difficulties in terms of linking amounts/volumes of tobacco seized as a result of investigations to possible funds laundered that could be associated with the predicate offence. Herewith some of the responses:

a) Respondent 6 indicated that "Money laundering is an autonomous offence. As a result we cannot determine the exact nature of the predicate offence from the money

laundering reports registered in the national police database. When examining the details of the investigations we received (and when the quantities of goods were provided) we found that the cases investigated by the police related to intensive trade of illicit cigarettes (between 1.4 to 8 million cigarettes in each case). In these cases cigarettes were transported and imported. The quantities found at local points of sale are much smaller (several hundred packets). We do not have any information on the laundered amounts".

b) Respondent 11 indicated that it "does not keep complete records on the amount and volume of tobacco involved in its adopted criminal investigations. Often, as the extent of the smuggling is unknown, making inferences on the number of cigarettes seized is likely to under-estimate the amount and volume of tobacco involved in the investigations. This measurement problem also applies to accurately assessing the scale and scope of associated money laundering. However, as part of the aforementioned project into the criminal finances of tobacco smuggling, it is an area in which the relevant service wishes to expand its understanding.

149. **Conclusions:** Cigarettes are a legal commodity that can be transported and sold on the open market making it simple to establish a supply source, distribution channels, and move in large quantities. It is a low risk, high profit enterprise that entices traditional criminal traffickers to move into more lucrative and dangerous criminal enterprises such as money laundering, arms dealing, and drug trafficking. Law enforcement investigations have directly linked those involved in the illicit tobacco trade to terrorist organisations who are looking for a high-profit, low-risk way to finance their operations.

LAW ENFORCEMENT AND THE CONDUCTING OF INVESTIGATIONS INTO ILLICIT TRADE IN TOBACCO AND MONEY LAUNDERING

150. Perhaps of the most pertinent reasons for lacking ML cases to stem from ITT was provided by respondent 6. "The police carry out reactive investigations, mostly based on international requests (sic) but also based on local information (identification of retailers), or based on disclosures to the jurisdictions FIU or based on complaints of manufacturers. Apart from investigations launched on the basis of a report by the FIU *we do not automatically open money laundering files. This is not appropriate when the goods have already been seized and when the financial flows have already been identified*. Investigation into the assets suffices to secure the seizure and confiscation of the illicit assets. *Opening a section on the financial aspect or money laundering complicates the procedure*. The Public Prosecutor can decide to open a money laundering investigation when appropriate. This investigation is then carried out by the economic and financial department of the federal police.

151. Respondent 11 also indicated that financial investigators are assigned to cases but that the decision to add ML as a charge was dependant on a case by case basis. This was done in conjunction with the prosecution service and dependant on the evaluation of the strength of the generated evidence.

152. Respondent 12's respective agency covers the aforementioned as said agency has the responsibility of enforcing customs laws within the jurisdiction, and conducting investigations related to tobacco smuggling. These investigations include, but are not limited to, the domestic and

international smuggling of cigarettes; counterfeit or genuine, trafficking in counterfeit cigarettes; trafficking in stolen cigarettes; smuggling of cigarettes in violation of embargoes; and international money laundering investigations where one of the underlying crimes is tobacco-related.

LAW ENFORCEMENT AND THE CONDUCT OF JOINT FINANCIAL INVESTIGATIONS

153. Only three respondents provided answers to this question. The primary theme being that inter departmental work groups had been established to address AML/CFT. No indication was however given where ITT was seen as a separate commodity to warrant intergovernmental arrangements for this specific commodity.

154. Respondent 9 indicated that the Guardia di Finanza is the main law enforcement agency involved into investigation on tobacco smuggling. At the same time, the Guardia di Finanza has the charge of investigative development of STR's also and has the knowledge to carry out financial investigation in general. For these reasons Guardia di Finanza is able to ensure investigation on all the aspects related to tobacco smuggling, keeping contacts, when it is necessary, with the FIU and any other authority which may be interested into investigation carried out If suitable, it may commence a separate ML investigation into a complicit business (*e.g.* a MSB) outside of the predicate investigation into tobacco smuggling.

155. Respondent 12 indicated that the Joint Terrorism Task Force (JTTF)) serves as a centralised, coordinated entity for law enforcement information or investigation of suspected or real terrorist activities, including terrorist financing. The JTTF uses the concept of enhancing communication, coordination and cooperation between federal, state, and local government agencies representing the intelligence, law enforcement, defence, diplomatic, public safety, transportation and homeland security communities by providing a point of fusion for terrorism intelligence to identify disrupt and dismantle any potential terrorist threat.

Box 15: **Case study – ITT and linkage to TF and ML**

Cigarette Smuggling, Money Laundering, Firearms, and Conspiracy

In 2009, the Joint Terrorism Task Force investigated a subject who smuggled 20 000 cartons of cigarettes and profited the USD 1.38 margin between Tennessee's USD 0.62 tax and Michigan's USD 2 tax. His Knoxville to Detroit operation reportedly cost Tennessee and Michigan more than USD 500 000 in tax revenue. During the course of the investigation, a wiretap caught the subject recruiting for Al-Qaeda and discussing blowing up a shopping centre. In 2010, the subject pled guilty to 16 counts including firearms, conspiracy, cigarette smuggling, and money laundering.

Source: United States

156. Respondent 13 indicated that the Judiciary Police is a member of the interdepartmental Anti-money laundering working group which comprises government agencies in charge of judicial, supervisory, law enforcement and FIU responsibilities. The working group meet every quarter to discuss recent trends in money laundering/terrorist financing, exchange views and ideas on that

and initiate necessary actions in relation to AML/CFT. However, the AML working group by itself has no investigative power, and such investigation could only be conducted by the Judiciary Police under the guidance of the Public Prosecution Office.

157. **Conclusion:** It should therefore be noted that cooperation amongst law enforcement is important and that this extends beyond internal engagements. The following section then serves to identify other impediments to the investigation of ITT.

IMPEDIMENTS ENCOUNTERED WHEN CONDUCTING INVESTIGATIONS?

158. Once again only three responses were received from which any deduction could be made. It is possible that this could extend into other areas of investigative endeavour and includes:

a) Borders often slow down such investigations. Customs can act based on a "request for mutual assistance".

b) Some countries are not very cooperative.

c) Finalised investigations show that the interest of foreign partners largely depends on their own interest in an investigation.

d) Illicit Tobacco is one of many substantive offences related to proceeds of crime and money laundering investigations. The financial crime units have to prioritize on what investigations to undertake and illicit tobacco is not always at the top.

e) Respondent 18 stated that in cases involving foreign predicate offences, while they have been proactive in commencing domestic money laundering investigations, were reliant on foreign counterparts to be forthcoming with evidence in a timely manner. When this is not done, or if the foreign country decides to enter into plea bargains with the suspects, said respondent would not be able to take further action.

THE USE OF CORPORATE STRUCTURES BY CRIMINAL SYNDICATES TO SMUGGLE TOBACCO AS WELL AS LAUNDER THE PROCEEDS OF THE ILLICIT TRADE IN TOBACCO

159. This section aims to provide an overview of multiple jurisdictions identification of specific methods utilised by perpetrators to launder the proceeds of ITT. Three respondents provided a detailed overview of methods utilised by groupings.

a) Respondent 6 "Our investigations have identified various structures: The use of companies managed by a front man. The goods are sent to these companies and used to set up the lease of warehouses. The front man is usually unaware of the procedure used. The use of fictitious buyers with fake invoices and CMRs. The use of companies in financial trouble. Using payment in kind money is injected into this company. This easy money is attractive to the managers of these ailing companies and once they are caught up in this system they cannot get out. Managers of legitimate businesses use dirty money to purchase loads of cigarettes and finance the trade. The profits are channelled abroad using money remittance or cash couriers and invested in foreign property. Furthermore, transport companies allow cigarettes to be hidden in the cargos of legitimate products.

b) Respondent 11 indicated the following "This is an area the responsible agency is investigating as part of the aforementioned project into the criminal finances associated with tobacco smuggling. There is operational intelligence to suggest Organised Crime Groups (OCGs) will establish seemingly legitimate import/export companies involved in bulk consumer goods, which act as suitable cover loads to support the illicit tobacco trade. For ML, the OCGs may own or become involved with criminally complicit Money Service Businesses, which provides an element of legitimacy in handling consistent volumes of cash. There is limited intelligence to suggest the involvement of offshore companies. The responsible agency is hoping to improve its understanding of how prevalent this methodology is in supporting the ML of funds generated by the trade of illicit tobacco products. In one large-scale operation, the overseas cheap white tobacco purchaser and distributor is linked to non-tobacco related companies in the UAE, Singapore, Malaysia and Greece. It is suspected these businesses provide a legitimate front for global import / export of goods acting as cover loads for smuggled cheap whites. This type of methodology is repeated by other OCGs but should not be considered as the prevalent MO. OCGs have proved flexible and fluid in setting up other corporate structures to support smuggling and the associated money laundering."

c) Respondent 13 stated that it is difficult to say with accuracy whether credit companies or banks are permitting the use of debit machines within retail outlets that sell illicit products then in a sense they could be facilitating illicit sales. However in many instances they would probably be totally unaware of where and to what end their services are being used to sell illegal tobacco products. It was sighted that corporate structures could be used depending upon the sophistication of the organisation. At the least corporations could be used for nominee ownership, banking, and tax evasion, within criminal organisations they could hire professionals to set up corporate structures to layer and then integrate the illegal funds in money laundering schemes. Based on FIU's analysis of numerous cases related to illicit tobacco, the following types companies were either subjects of investigations or ordered/benefited from financial transactions, including international wire transfers:

- Cigarette suppliers/manufacturers/ distributors
- Real estate companies
- Auto dealerships/repairs/parts
- Construction/landscaping companies
- Financial services
- Import/export or trading companies
- Restaurants/bars
- Non-profit organisations
- Transportation companies
- Pawn shops

CONCLUSIONS

160. The information as provided by the respondents once again indicates that law enforcement agencies do investigate Organised Crime activities to be associated with ITT but very few examples were sited where ML was also investigated. In the Customs section strong emphasis was placed on the fact that Customs hand over potential money laundering cases or financial investigations to be associated with ITT. It is however clear that very few of these cases are investigated from a money laundering perspective.

C. FINANCIAL INTELLIGENCE UNITS

161. In the previous sections it became clear that FIU's play a pivotal role in the coordination or facilitation of information sharing amongst law enforcement agencies. The following section therefore provides an overview of how FIU's interact with other agencies as well as assess money laundering and terror financing to be associated with the illicit trade in tobacco.

SUSPICIOUS TRANSACTION REPORTING TO BE ASSOCIATED WITH ITT

162. The responses varied with countries focused on ITT once again providing a more detailed response. Not all jurisdictions could place a financial value on said STR's. Some jurisdictions also provided an overview of how their respective reporting regimes function. Certain jurisdictions also highlighted which other jurisdictions could be linked to their domestic smuggling aspects.

163. Respondent 3 indicated that for the required reporting period a total of 245 STR's had been received. The figures had increased drastically from six STR's received in 2007 to 43, 57, 95 and 44 for the respective years 2008-2011. Financial values were not included.

164. Respondent 11 indicated its reporting institutions are not required to identify suspected predicate offences and in many cases will not be aware of the predicate offence. This means that many reports are received on suspicious activity that has taken place without knowledge or suspicion that the money or arrangement relates to illicit tobacco trade. Some reporters, however, may suspect this crime is taking place and indicate this in their SARs.

a) Since January 2006 said jurisdiction identified: 953 SARs containing the word "tobacco": 68 SARs containing "tobacco" and "smuggling" 793 containing the XXF2XX glossary code (this glossary code refers to Excise Fraud, of which tobacco forms only a part).

b) Domestic: All SARs are made available to law enforcement via a nationwide database.

c) International: Due to information recording methods, reliable statistics (specific to illicit tobacco trade) is not available.

165. Respondent 13 in turn indicated that its FIU had between 2007 to 2011, disclosed 59 money laundering cases linked to illicitly traded tobacco. These disclosures were sent to domestic and international law enforcement and intelligence agencies. Nine of the cases actually originated from a suspicious transaction report (STR) received by the FIU's reporting entities. Of the 59 disclosures, a total of 48 cases contained at least one STR linked to an individual or entity under investigation.

(i) & (ii): All STRs combined for cases related to illicit trade in tobacco totalled to 377 reports. (iii): The total monetary amount indicated in the 377 reports came to USD 40 821 493.70.

166. Respondent 18 declared that its respective FIU had from 2006 to 2010, received 21 Suspicious Transaction Reports (STRs) relating to illicit tobacco trade Of the 21 abovementioned STRs, 9 STRs were detected which disclosed possible offences of illicit trade in tobacco and these were referred to domestic and international authorities.

167. **Conclusion:** It is therefore clear that various jurisdictions do have STR's associated with ITT. It is disconcerting to note that several of these STR's cannot be linked to subsequent ML law enforcement investigations. This could be reflective of the method used to obtain information for the purposes of developing this typology or be indicative of STR's related to ITT not being converted to ML investigations.

THE FIU AS PART OF A JOINT FINANCIAL INVESTIGATION/MONEY LAUNDERING TASK FORCE

168. Previous sections highlighted the role FIU's play in conjunction with other law enforcement agencies. This section aims to highlight the specific role played by FIU's in terms of countering ML or TF to stem from the illicit trade in tobacco. Invariably the role of the FIU is dependent on whether it has investigative and or administrative capacities.

169. The majority of the respondents indicated that they do not take actively part in joint financial investigations but do however disseminate information to other law enforcement and Customs agencies. Respondent 13 provided a sound summation of the aforementioned *i.e.*, their respective FIU is an administrative FIU and does not conduct investigations. However, law enforcement and other government institutions or agencies are able to provide voluntary information to the FIU. If, on the basis of analysis and assessment, the FIU has reasonable grounds to suspect that designated information would be relevant to investigation or prosecution of money laundering or terrorist activity financing offences, the FIU must disclose the information to the appropriate domestic disclosure recipient. The FIU may also disclose internationally to an equivalent agency when there is an MOU in place.

170. **Conclusion:** FIU's seem to act predominantly as investigative support function and as conduit in terms of obtaining and distributing relevant information. The FIU's therefore are not necessarily part of a task team but through their functioning can support existing task teams. Indications were that STR or SAR's had been obtained and forwarded. Difficulties will however be experienced to link said reports to successfully concluded ML investigations to stem from ITT.

IMPEDIMENTS ENCOUNTERED WHEN CONDUCTING INTELLIGENCE GATHERING

171. All respondents indicated that there were no impediments in terms gathering intelligence and day to day functioning. Respondent 13 did however indicate that its FIU is one of many key players in its jurisdictions anti-money laundering/terrorist financing regime. The Centre provides disclosures of tactical financial intelligence to its disclosure recipients as described above. The FIU also shares its strategic intelligence products with domestic and international partners.

172. In terms of intelligence gathering, it is important for administrative FIUs (especially) to have access to as many law enforcement databases as possible. For example, in these types of cases, having access to customs and intelligence files on suspected smugglers would assist analysis greatly.

THE RELATIONSHIP BETWEEN FIU'S AND CUSTOMS AGENCIES

173. This section relates specifically to the relationship between FIU's and customs agencies. The purpose was to highlight the ability to report and receive information relating specifically to ITT. The majority of respondent's inputs were in the positive.

174. Custom agencies can receive financial information from the FIU under the following circumstances: (1) Referrals: Where STRO's analysis detects possible offences under Customs purview, STRO will disseminate the analysis results to Customs; and (2) Screenings with STRO: STRO allows domestic agencies, including Customs, to conduct screenings against the STRO database.

175. Respondent 13s Border Agency can receive financial information from the FIU. There is a dual threshold that applies as explained below. The FIU is able to disclose to the agency if the Centre, on the basis of its analysis and assessment, has reasonable grounds to suspect that the designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence AND If the Centre determines that the information is relevant to: An Offence of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the agency and investigating or prosecuting an offence of smuggling or attempting to smuggle goods subject to duties or an offence related to the importation of goods that are prohibited, controlled or regulated under the Customs Act.

176. Respondent 6 specifically stated that where the notification contains information regarding the laundering of money derived from an offence related to serious and organised fiscal fraud setting in motion complex mechanisms or using procedures with an international dimension, or from an offence within the competence of the Customs and Excise Administration, the FIU shall inform the Minister of Finance of this notification.

177. **Conclusion:** It is clear that many FIUs do provide the information to Customs authorities. The challenge would be to determine whether said customs agencies then red flag suspects and or identify the potential to forward said information or work in conjunction with law enforcement agencies.

THE SHARING OF FINANCIAL INTELLIGENCE (FIU TO FIU, FIU TO LEA ETC)

178. This section was to then also highlight the importance of sharing of information across borders as opposed to within jurisdictions only. Unfortunately the answers provided were not indicative of significant international sharing of information on the illicit trade in tobacco.

Box 16: **Case study – FIU and the sharing of information**

The case was triggered from a suspicious transaction report (STR) filed by a financial institution describing unusual large cash deposits conducted into a joint personal account held by Individual A

and Individual B. The STR revealed that Individual A is employed by Entity X

Over a period of 6 years, approximately 120 large cash transaction reports involving the two individuals were reported to FIU. In an article published in a local newspaper, it was stated that Entity X, a construction company, was used as front company by an organised crime group to smuggle tobacco products between Canada and the United States. Under the Canadian excise tax law, the owner of the company was sentenced to pay a large fine.

Entity X was also identified in the media as part of company consortium linked to suspected drug trafficking and organised crime.

Comment

In this case, FIU was able to link an article in a local newspaper with financial transactions conducted by Individual A and Individual B. The case also shed light on money laundering methods used by cigarettes smugglers. Money from cigarette smuggling was given to the front company's employee to be deposited into his personal account.

Source: Canada

Box 17: **Case study – ITT ML between the UK and Belgium**

In the past transactions mainly consisted of changing GBP (and to a lesser extent SCP and NIEP) into EUR that could be linked to tobacco smuggling between Belgium and the United Kingdom. Since 2007 the transactions have mainly been cash deposits followed by cash withdrawals. In several files the accounts of Belgian companies selling tobacco were credited by cash deposits followed by cash withdrawals.

Information from the special tax inspectorate – Fraud scheme information service the list of suppliers of these companies showed that the tobacco was purchased without being declared. Given the discrepancy between the amounts listed for the purchase compared to the amounts sold we can conclude that some of the purchased goods were resold without being declared.

Due to the large amounts it is beyond doubt that the actual nature of the business transactions involved paying excise duties in the United Kingdom, which are considerably higher than the excise duties applicable in Belgium. EUR were purchased using GBP which are the proceeds of fraudulent tobacco sale in the United Kingdom for which excise duties and VAT in the United Kingdom were not paid. The EUR were used to supply smuggling networks with purchases that are supposedly carried out by individuals.

This money laundering is also detrimental to the financial interests of the European Communities because by not paying excise duties in the United Kingdom the fraudsters also do not pay the applicable VAT and 10% of this amount goes to the budget of the European Union.

Typologies related to the individuals involved. Some of the individuals involved in these transactions are British nationals. They either lived in the United Kingdom or in Belgium. Often they have already committed this kind of illegal activity or drug trafficking or state that they change currencies to purchase cigarettes or tobacco in Belgium. They changed EUR at exchange offices but

also at bank branches in the Belgian coastal region. Over time CTIF-CFI has found that money launderers moved their activities to Brussels to avoid any suspicions. Transactions were also split among various people as to not arouse suspicions.

Other files involved Belgian nationals that could be linked to the United Kingdom; they were lorry drivers who often travelled in the United Kingdom. CTIF-CFI forwarded several files linked to illicit trade in tobacco to the judicial authorities. Links with the United Kingdom were identified in these files. The excise duties in the United Kingdom are considerably higher than those in Belgium. In these files British nationals changed considerable amounts of GBP, SCP and IEP into EUR. Some of them lived in Belgium and CTIF-CFI's analysis showed that they could be linked to the United Kingdom. Many of them were lorry drivers who often travelled in the United Kingdom. Several individuals involved in these files were given prison terms. Nationals of Central and Eastern European countries that were not linked to Belgium in any way were also often involved in this kind of trafficking. Several nationals of Central and Eastern European countries repeatedly went to the same exchange office in Brussels to change GBP into EUR. Several thousand EUR were changed into EUR in a few months' time. These individuals were not officially registered in Belgium and did have any professional links to our country. They were known to the police for illicit tobacco trade. The GBP changed in Belgium were probably proceeds of this illicit trade, which were laundered by purchasing these EUR.

Source: Belgium

D. TAXATION AUTHORITIES

179. The concluding government stakeholder to be addressed is taxation authorities. Of importance to note is that various jurisdictions ascribe differing responsibilities to their taxation authorities and are therefore not always comparable when viewed from a law enforcement functionality perspective.

a) Firstly, some revenue services are a combination of Inland Revenue and Customs Services. It is therefore possible that differing responsibilities and mandates will come to the fore where combined services are utilised.

b) Secondly, cognisance should also be taken regarding the various jurisdictions approach in terms of whether tax crimes are considered a predicate offence to ML or not and or whether the illicit trade in tobacco is viewed as a taxation offence.

180. If one were to assume that tobacco smuggling and the accompanying false declaration occurs for the purposes of tax (duty) evasion, and that said jurisdiction does not consider tax crime a predicate offence to Money Laundering, one could then conclude that the possible money laundering to stem from the illicit trade in tobacco will possibly not receive the same impetus when viewed from an investigative perspective when say perhaps that as perpetrated by a drug smuggler or smuggling ring. The following section will centre more on the differing approaches as followed by the responding jurisdictions, the identified successes, weaknesses, shortcomings as well as the affected standards.

TAXATION AUTHORITIES: THE CONDUCT OF INVESTIGATIONS INTO THE ILLICIT TRADE IN TOBACCO AND MONEY LAUNDERING.

181. Respondent 2 stated that the Field Audit and Investigation Unit of the Inland Revenue Department ("IRD") is responsible for conducting field audits and investigations on businesses and individuals with a view to combating tax evasion and avoidance. The IRD does not differentiate transactions involving illicit trade in tobacco and/or other types of arrangements which have led to tax evasion or avoidance. IRD does not conduct money laundering investigation for the reason mentioned above. Money laundering investigations will be investigated by Customs, Police and the Independent Commission Against Corruption respectively

182. Respondent 3 stated that it sees the Illicit Trade in tobacco as a significant problem and that a national project has been registered relating to high risk entities within the tobacco industry. It is not the mandate of the Tax/Customs Authority to conduct investigations into money laundering. These investigations are referred to the Assets Forfeiture Unit (AFU) under the National Prosecuting Authority (NPA) as well as the Financial Intelligence Centre (FIC).

183. Respondent 11 stated that its Tax Authority conducts criminal and civil investigations into the illicit trade in tobacco.

184. Respondent 12 has a specific agency charged with this responsibility and has the primary jurisdiction of collecting the domestic Federal tobacco excise tax, as well as enforcing other related provisions of the Internal Revenue Code. In enforcing this jurisdiction, the agency works to target individuals and companies that are wilfully seeking to avoid excise taxes, defraud the Federal government and participate in illegal activities. Some examples of illegal activity investigated by the agency includes: the evasion of FET on manufactured tobacco products; illegal manufacture of tobacco products; smuggling of tobacco products into the United States without payment of FET; and the diversion and non-payment of tax on tobacco products which were held by wholesalers and distributors when a subsequent FET Floor Stocks tax became due. Agency auditors and investigators are able to detect money laundering and other financial fraud schemes while conducting their audits. However, the agency currently does not have a permanent criminal enforcement component. Under special appropriations that expired September 30, 2011, the agency was appropriated funding for use towards the "hiring training and equipping of special agents" to conduct criminal investigations. Under this authority, the agency negotiated and signed an Interagency Agreement with the Internal Revenue Service (IRS) in which the IRS provided criminal investigation services to the agency. This partnership proved to be very successful. The investigations conducted by the Special Agents assigned to the agency included money laundering as one of the related offences. The agency has requested funding to permanently continue a criminal enforcement program, however; until such time as additional monies are received, the agency must again look to other law enforcement agencies, including the Criminal Investigative Division at IRS, to accept and conduct any new criminal related investigations on behalf of the agency.

185. Respondent 13 indicated that vast steps have been taken to enable said investigations. The agency has in the past conducted both civil audits and criminal investigations into the illicit tobacco trade. Under its special enforcement program, it audits criminals engaged in this sector. The agency

will conduct investigations into this sector when it suspects tax evasion and/or tax fraud. The recent changes (July 2010) to the jurisdictions Criminal Code has seen tax evasion become a designated offence to money laundering. As such, the agency and its investigative component can conduct its own investigations into ML aspects of these cases.

186. In contrast respondent 17 indicated that its Tax Authority does not conduct any investigations regarding illicit trade in tobacco, but audits would be done for taxation purpose. The Tax Authority does not conduct the money laundering aspect of the investigation. Judiciary Police is the government agency vested with the power to conduct money laundering investigations. Respondent 18 responded similarly insofar as that there are no specific programmes by the tax authority to target the illicit trade of tobacco. Investigations on criminal activities with financial implications such as money laundering of criminal proceeds are handled by other agencies with tax offences then also not currently being a predicate offence for money laundering.

187. **Conclusions:** The following primary themes were identified:

a) Some jurisdictions allow for tax evasion (as derived from the smuggling or illicit trade) and the Money Laundering associated with it to be investigated by the tax authorities. The statistics where provided however reveal that very few Money Laundering cases have been investigated within these jurisdictions even where they have the mandate to do as such. The emphasis thus remaining with the investigation of the predicate offence.

b) Some jurisdictions indicated that they are responsible for investigating the tax evasion offences but that the ML offence investigation is referred to another law enforcement agency. No statistics were provided to indicate the number of cases provided as well as the success rate when viewed from a prosecution perspective.

c) One respondent indicated that it does not conduct any form of investigation into ITT as well as ML investigations with a last respondent indicating that its customs authority is responsible for investigating the ITT and local law enforcement investigating the ML offence. Once again no corresponding statistics were provided.

d) It can therefore ultimately be summated that the responses indicate that the majority of tax authorities do not single out ITT as a significant tax evasion offence and that very few of the authorities conduct ML investigations or refer possible ML investigations to stem from ITT to law enforcement.

TAXATION AUTHORITIES: STATISTICS ON THE NUMBER OF ILLICIT TRADE IN TOBACCO, RELATED TAX EVASION CASES AND THE MONEY LAUNDERING TO STEM FROM IT.

188. The answers here are dependent on whether the tax authority is responsible for tax evasion investigations to stem from the illicit trade in tobacco as well as whether said authority differentiates and maintains databases or statistics in terms of the origin of the investigated cases of tax evasion. Only four of the respondent's replies were indicative of this.

189. Respondent 3 has registered a project which focuses solely on tax evasion offences to stem from the illicit trade in tobacco. The tax authority can be described as a combined customs and Inland Revenue service. Multiple tax entities related to the illicit trade in tobacco have been

identified with the various remedies at the authorities' disposal being used to counter the illicit value chain to be associated with the groupings activities. This includes search and seizures as well as the raising of tax assessments across various tax types. The total tax liabilities regarding only four of the investigated entities is in excess of USD 45 million. No money laundering cases have been associated with the project.

190. Respondent 11's response was indicative of a similar approach. The tax authority is also a combined agency of Inland Revenue and customs. In its response it is noted that following any successful prosecution, the said agency, will seek to recover the proceeds of an individual's involvement in unlawful conduct. As the jurisdiction operates a value-based confiscation system, this is not necessarily linked to the recovery of assets. However, where possible Financial Investigators will assess an appropriate benefit figure to deny the individual access to or ownership of legitimate and illicitly obtained assets. If prosecution has not been successful or is unlikely to succeed, the agency will evaluate the opportunities it has to mount a civil investigation into the individual(s) with the aim of recovering (at the very least) monies owed to the fiscal authorities.

191. Respondent 12 has a dedicated agency responsible for the collection of excise taxes on tobacco products, and for eliminating or preventing tax evasion and other criminal conduct in regard to regulated tobacco commodities. Tobacco manufacturers and importers, among other entities must obtain a permit from the said agency in order to operate. They also must comply with recordkeeping and tax payment requirements under local legislation. Violations of the Internal Revenue Code with the intent to evade excise taxes may result in a civil fraud penalty or criminal prosecution. Over the past 5 years, the agency has had 47 tobacco cases involving tax evasion. Ten of these cases are current criminal cases that are still under open investigation, 14 are still open audits/investigations, 4 were resolved with no further action and 19 of these cases were resolved administratively through adverse action. Adverse action can include: offers in compromise (OIC), basic permit suspension or the voluntary surrender of a basic permit by an industry member. The 19 adverse action cases were resolved via the following manner: The total tax liability estimated for the 10 criminal cases is estimated to be USD 13 161 995, although since the investigations are on-going, this amount could turn out to be significantly higher. Further, there are likely to be as yet unidentified money laundering charges that will stem from these cases. The 23 cases that were resolved administratively had no monies associated with them. Three other cases that were settled totalled USD 5 million.

192. The reply from respondent 13 also indicated successes to be had should tax authorities utilise their specific mandates. The specific Revenue Agency has worked alongside its Ministry of Finance to tackle the illicit tobacco trade from both a civil liability and a tax evasion point of view. In around 2005 the Agency and the specific jurisdiction entered into a Joint Forces Operation (JFO) that saw referrals from the jurisdiction to the Agencies Special Enforcement Program (SEP). Those cases that had indications of possible tax evasion were referred from the SEP to the Criminal Investigations Program (CIP). There were a total of 4 cases that were referred to the CIP in the past five years, with two resulting in convictions. The other two cases were eventually aborted.

193. **Conclusions:** The following primary themes were identified:

a) Given the nature of how taxation authorities operate (*i.e.,* the differing mandates and jurisdictional approaches) information and lacking statistics obtained indicates that

taxation authorities do not focus on the Money Laundering offence per se and tend to focus more on the tax evasion offences.

b) Furthermore, very little indication was obtained that taxation authorities differentiate between where the illicit income had been derived from. This then meaning that the ITT is not differentiated from other forms of illicit income generation.

TAXATION AUTHORITIES: IMPEDIMENTS ENCOUNTERED

194. It is well known that tax legislation is strict in terms of governing the obtaining and sharing of tax payer information. One of the drawbacks would for instance be the provision of information under civil or administrative auspices which is then subjected to scrutiny by criminal investigators. This and related aspects has been discussed at length within the FATF realm. There are however certain jurisdictions that have relaxed impediments to the aforementioned which have in turn assisted significantly in the countering of organised crime and related activities.

195. Respondent 13's reply is indicative of the aforementioned. The respective revenue authority has a long standing policy and legal obligation to respect the confidentiality provisions of both the Income Tax Act and the Excise Tax Act. This applies to all aspects of the compliance cycle, be it during the intelligence gathering stage or the actual investigation or audit. However, when seeking information from other law enforcement authorities, for the most part the provisions have not significantly limited the agency in its intelligence gathering activities. It is worth noting that data houses in certain police databases is not available to Special Enforcement Program (SEP) auditors and therefore, SEP intelligence gathering of this nature must be relied on through liaison with law enforcement. Once the information is with the agency, the provisions are, however, more restrictive pertaining to disclosures from the agency. In general, the agency cannot share information related to case specifics with external partners. The agency is impeded by legislation in some respects as Section 241 of the Income Tax Act and Section 295 of the Excise Tax Act (GST/HST) restrict the agency's ability to provide external partners with compliance action case specific details that would assist in gaining a better understanding of the characteristics and details of potential tax evasion cases.

196. Respondent 3 indicated that its legislation is applied in the same vein. The tax and customs legislation prohibits the sharing of tax and customs information in terms of section 4 of the Income Tax/Customs and Excise Act. However, if a matter is registered with the National Prosecuting Authority (NPA) in terms of the Prevention of Organised Crime Act (POCA) this legislation supersedes the secrecy provisions in the Tax and Customs legislation allowing for the sharing of information. The Financial Intelligence Centre Act also supersedes the secrecy provisions insofar as placing a reporting obligation (in the form of a suspicious transaction report) on the revenue authority where money laundering is suspected. In recent times the working relations between the various law enforcement structures have improved due to joint prioritisation of investigations.

197. Respondent 12 also mirrors the two prior respondent's approaches. The respective agency experiences several impediments in its attempts to collect intelligence. The agency for instance does not have access to several criminal history databases, and must look to other sources and databases to fulfil its mission of granting permits, as well as to detect and investigate tax evasion. Another primary roadblock to information sharing is the inability of the agency to share tax

information with other law enforcement agencies, which precludes said agency from releasing any information about a taxpayer that was obtained via a tax return or from return information (return information includes a taxpayer's identity and the nature, source, or amount of their income, payments, receipts, deductions, exemptions, credits, assets, liabilities, etc). Although there are exceptions to the non-disclosure provision, the procedures that allow for information to be shared can be arduous and too restrictive. The agency holds some information that would benefit other law enforcement and taxing agencies and vice versa, however without the ability to freely share information in a timely manner among agencies, it is difficult to collect intelligence that portrays the complete picture. We note that the STOP Act S.1706, a bill recently reintroduced in Congress to reduce tobacco smuggling, removes some of the restrictions by allowing information sharing with designated state, federal, and international law enforcement and tax agencies.

198. **Conclusions:** It is therefore clear that these similarities create an environment which could be regarded as conducive towards the illicit trade in tobacco to occur. This lack in ability to share information emanates from law enforcement and from the taxation authorities. It could therefore be argued that the inability to share information pertaining to crimes that are committed predominantly within the taxation and customs domain can be considered as conducive for illicit trade to occur.

199. The primary cause would be the decrease in the risk of detection coupled with lacking criminal procedure and money laundering convictions to stem from the illicit trade.

200. Secondly, not all taxation authorities have investigative powers pertaining to these offences which if seen in the context of lack in sharing of information creates a void from detection, investigation and successful prosecution.

Box 18: **Case study – operation 'Samhna'**

A multi agency operation, code named 'Samhna', headed up by Revenue's Customs Service, is currently underway in Greenore Port, Co Louth, and surrounding area.

The operation, targeting the suspected criminal activities of an organised crime group operating both north and south of the border, involved the surveillance of a general cargo vessel M/V Anne Scan, which sailed from the Philippines on 15/09/2009 for Greenore Port, arriving at approximately 0600 hours on Monday, 26/10/2009, carrying a cargo declared as 'animal feed'. Officers kept the vessel under surveillance, as they suspected that a large consignment of contraband cigarettes was concealed within the cargo.

Following the discharge of part of the cargo from the vessel earlier this morning onto awaiting trucks, which were allowed onwards to the importer's premises, the multi agency task force, involving Officers of Revenues Customs Service and An Garda Siochana, moved in and raided several premises in the Co. Louth area, in addition to mounting an operation on the vessel itself. A large consignment of contraband cigarettes has been confirmed, estimated to be in excess of 120 million cigarettes with a retail value of about EUR50m and a potential revenue at risk of approximately EUR40 million. Several persons have been arrested at various locations by the Gardai for questioning.

The operation in the Republic of Ireland involved Officers of Revenue's Customs Service, An Garda

Siochana, The Criminal Assets Bureau, the Irish Naval Service and Air Corps and in Northern Ireland, Officers of HM Revenue & Customs and the PSNI. In addition the European Anti-Fraud Office (OLAF), which was also involved, will co-ordinate the international enquiries which will form part of the follow-up investigations. It is estimated that in excess of 150 Officers from the various Agencies participated in the field in today's operation.

Two of the vessels that supported the operation were Revenue's Customs cutter RCC Faire and the Navy vessel LE Niamh. Hailing the operation as a great success, Revenue Commissioner Liam Irwin said:*"The success of this operation is a credit to the close working arrangements and cooperation between the various law enforcement agencies both nationally and internationally. Criminals have no respect for national borders and international cooperation is now more essential than ever for law enforcement agencies. This is a shining example of a multi-national, multi-agency response to criminal activity and all the agencies involved should be commended for the part they played in this successful operation".* Garda Commissioner, Fachtna Murphy said:"This is a significant strike against organised crime. The success of the operation illustrates the results and benefits that flow from close interagency cooperation. I want to pay tribute to both our colleagues in Revenue Customs Service and my own members of An Garda Síochána who were involved in this morning's operation. Their hard work and dedication helps us to secure a safer community for everyone."

Defence Forces Chief of Staff, Lieutenant General Dermot Earley congratulated "this joint action by the Revenue Customs Service, Garda Siochana and our LE Niamh which proves the need for this joint co-operation yet again. I know there is a lot of hard work to follow behind the scenes and the Defence Forces will continue to assist in every way it can".

Source: Irish Tax and Customs (2009)

TAX AUTHORITIES: ALTERNATIVE METHODS OF INVESTIGATION

201. This section is to highlight the propensity for tax authorities to offset the negative effects of the aforementioned through the establishment of task teams and the utilisation of a collaborative approach. Once again this differs from jurisdiction to jurisdiction.

202. Unfortunately no significant answers were obtained. The absence of responses could be interpreted as such that collaborative approaches are not being followed to offset the limitations as posed by the ability to share information.

203. **Conclusions:** It is however known that within the taxation arena great effort is being placed on the enhancement of the ability to share information. In the case of taxation authorities that follow an Inland Revenue approach only the utilisation of DTA's with other member countries can assist in obtaining information which may help to curb transnational smuggling. Jurisdictions following a combined approach (*i.e.,* Customs and Revenue Service) can take further advantage of Mutual Administrative Agreements between Customs Authorities.

TAXATION AUTHORITIES: AWARENESS TRAINING ON INVESTIGATING OR REPORTING ML TO STEM FROM ITT

204. The responses received indicated that very little emphasis has been placed on Money Laundering stemming from the illicit trade in tobacco or the tax evasion to be associated with it. The following section then serves to provide an overview of the emphasis that taxation authorities place as a whole on ML investigations and whether this would impact on the ability to associate ITT with ML and TF. This facility will be dependent on whether investigations are conducted internally, are outsourced or performed by other law enforcement agencies. Only five responses were received which all indicate a degree of ML awareness programmes to fully fledged courses. Not one of the respondents indicated whether this was performed with specific reference to the ITT.

TAXATION AUTHORITIES: PREVALENT FORMS OF TAX EVASION TO BE ASSOCIATED WITH THE ILLICIT TRADE IN TOBACCO

205. Respondent 12 stated that a prevalent form of tax evasion associated with the illicit trade in tobacco is the interstate movement of tobacco products from lower taxed jurisdictions to higher taxed ones. It is estimated that states lose several billions of dollars annually to this type of tax evasion. Under the authority of the Contraband Cigarette Trafficking Act (CCTA), and in conjunction with various state agencies, ATF investigates this form of tax evasion. Federal tax dollars are also at stake, and in terms of TTB jurisdiction, diversion schemes vary widely and change in response to targeted enforcement efforts. Schemes include:

a) The illicit manufacture of product,

b) Diversion of "exported" and non-tax paid product, and;

c) Smuggling or misclassification of imported product to evade tax.

d) Another major source of tobacco diversion is the illicit manufacture and sale of tobacco products.

Box 19: **Case study – Tax investigations**

Retailers legally sold tobacco duty free to the reservations of Canadian Natives who then sold to store owners who used 'runners' to deliver the goods to various store owners for resale. Once the tobacco leaves the reserve for sale, it attracts duty and none were paid in these cases.

They both were cases where the Province of Ontario Tobacco Tax investigators performed surveillance and executed the search warrants on the cases. The CIP then obtained the records via a Provincial Offences Act application. The investigations were then conducted via a net worth using both the evidence seized from the province as well as those obtained from 3rd parties via production orders.

Source: Canada

Box 20: **Case study – ITT, tax evasion and terror financing**

Study: Material support to terrorism and cigarette smuggling

In 2002, The Lackawanna Six were identified as an Al-Qaeda Sleeper Cell, living in Lackawanna, NY, USA. They reportedly travelled to Afghanistan in April and May 2001 to join in Islamic jihad and receive military training at the Al Farooq training camp run by al-Qaeda; met with Osama bin Laden; and are believed to have been encouraged to go to Afghanistan by two American veteran mujahidin. They were indicted on two counts of providing material support to terrorism.

In 2004, another subject also of Lackawanna, New York, was convicted of money laundering and cigarette smuggling. An investigation revealed that this subject and more than a dozen co-defendants smuggled millions of cartons of untaxed cigarettes purchased from a Seneca Indian Nation wholesaler and sold them for huge profits in Michigan and in New York.

The operation cost the states millions in lost tax revenue. The members of the Lackawanna Six said that this subject had given them USD 14 000 which they used to travel to the training camp in Afghanistan.

Source: United States

CONCLUSIONS

206. Questions posed focused on whether taxation authorities have the mandate to conduct investigations into ITT and if so whether resulting ML will also be investigated within the realm. Of importance was also to determine whether tax authorities differentiated between tax evasion offences to be derived from ITT as opposed to other predicate offences which may hold tax implications. Questions were also posed in terms of impediments experienced where tax authorities have the mandate to conduct ITT investigations and whether other remedies are sought should such impediments arise. Lastly, taxation authorities had to indicate whether ML investigations forms part of their training curriculum and overall assess how important it is for taxation authorities to link money laundering with tax evasion as predicate offence as arising from the ITT.

8. FINAL REMARKS: MONEY LAUNDERING, TERROR FINANCING AND THE ILLICIT TRADE IN TOBACCO

207. The illicit trade in tobacco accounts for a significant amount of illicitly generated proceeds. These proceeds then emanate not only from the illicit trade in tobacco but also tax and customs offences to be associated with it.

208. The concern that was sighted was that very few Money Laundering or Terror Financing cases could be associated with the Illicit Trade in Tobacco (ITT). The primary purpose of the typology was to determine whether different modus operandi could be ascribed to this specific commodity as well as whether authorities responses to the countering of the predicate offence as well as the associated ML and TF to stem from it, differed from endeavours with respect to other illicitly traded products such as drugs.

209. The purposes of this chapter is to therefore provide an overview of the various conclusions reached as well as ascertain the veracity of the identified research propositions.

A. CHAPTER 3: AN OVERVIEW OF THE ILLICIT TRADE IN TOBACCO

210. A review of existing literature on the subject provided an overview of the nature and extent of ITT. The implications to arise from unabated smuggling activities were:

a) Deprivation of tax revenues to governments.

b) Redirection of limited government resources to address illicit activities associated with this specific commodity.

c) A disproportionate effect and impact on health services. This is exacerbated by decreases in tax revenue and simultaneously fuels debate to increase taxes on the specific commodity which in turns stimulates the incentive to increase smuggling activities.

d) Legitimate brand holders struggle to compete in and against an unfairly created market.

211. The chapter then also provided explanations with respect to differing forms of smuggling to be associated with the product, *i.e.,* bootlegging and/or large scale smuggling. Of importance was also to note the section pertaining to the economics of tobacco smuggling. Here emphasis was placed on the product price and how the price rises as the product moves along the illicit value chain, the effects of transportation and storage costs as well as the nature of illicit distribution points and cash collation. It is only at the lastly mentioned aspect that the propensity for ML to occur was sighted. The tangible risk and vulnerability being the difficulty experienced in identifying a fixed typology to identify cash remitters for instance.

212. Reviewed literature also indicated that a primary difficulty experienced in countering ITT lays in an inability to measure or quantify the extent of this form of illicit trade. A section was devoted to the different measurement tools that governments can employ to assist in policy making.

A lacking coordinated response will, however, continue to hamper the curbing of the phenomenon at a global and national level. This was also cited in the last section that focused on opportunities for an improved investigative response. Here the WCO report states that "where goods are highly taxed, easily portable and penalties remain relatively light for smuggling, transnational criminal organisations will take advantage of any weaknesses in customs, revenue or other border controls to amass profits".[9]

213. The countering of ITT requires a greater sharing of acquired knowledge and understanding of criminal activity and financial business models if enforcement impact is to be improved at domestic and international levels. The international nature of the ITT demands a global response that includes tackling the financial dimensions of the trade and recovering illicitly derived assets.

B. CHAPTER 3: THE JURISDICTIONAL APPROACHES

214. Of importance here was to obtain a broad overview of responding countries approaches to ITT. The primary conclusions were:

a) Most Jurisdictions do see ITT as a criminal offence. This does not, however, imply that they would see or link it as a predicate offence to ML.

b) Other associated offences include tax crimes and transgressions within the trademark environment.

c) The ITT is associated with tax offences which have then also been accepted by the FATF as a predicate offence to Money Laundering.

d) A wide array of penalties is at the disposal of law enforcement entities. These penalties range from transgressions in terms of:

   i) Tax evasion and fraud, customs duty/excise evasion and fraud, smuggling etc.

   ii) The nature of penalties imposed. These range from varying periods of incarceration and fines dependant on other factors such as relations to organised crime as well as the volume and or weight of the illicitly traded product.

e) It became clear that authorities are convicting perpetrators of ITT on varying offences but that ML is very seldom included in the charge sheet.

215. The primary trend to emerge from this chapter is that jurisdictions tend to predominantly investigate and prosecute on the predicate offence only and that very few money laundering and or terror financing cases could be associated with the illicit trade in tobacco.

9 WCO (2011).

C. CHAPTER 4: THE MODUS OPERANDI PERTAINING TO THE PREDICATE OFFENCE

216. This section confirmed the extent of the predicate offence. At first, a summary of the various jurisdictions international bodies' membership was provided. It was clear that most of the jurisdictions belonged to the same bodies but that approaches in terms of addressing ITT differed.

217. In terms of the location of the primary role players involved with ITT it was found that all respondents indicated that tobacco tended to originate from beyond their borders. That would be because their tax rates probably act as an incentive for outside role players to offset their illicit products within their higher duty jurisdiction. Modest support could be found for products being produced and sold within single jurisdictions only. Where investigations had proven to be successful it was due to multiple foreign and domestic agency interaction.

218. The methods identified with the smuggling of illicit goods as sighted were:

- Use of trucks with or without false compartments.
- Use of commercial vehicles
- Use of passenger vehicles
- Planes
- Cargo Vessels
- Passenger and goods trains
- Mules
- Roll on roll off transport
- Abuse of cross border shopping limits
- Postal packets
- False declarations
- Under valuation

219. Various methodologies came to the fore regarding the financing of ITT. This included seed capital obtained from small scale sales which were accompanied by a systematic increase in size of the illicit trade. Also noted was that bigger role players absorbed smaller role players within the OCG environment. Further, maturity cycles as applied to normal business operations were also found to be applicable within this realm *i.e.,* introduction, growth, maturity and decline phases. Of importance was the identification of commingling of funds and or products with linkages between the proceeds of illegal alcohol then used for trade in illicit tobacco, to the eventual bartering for drugs. The ITT then either having its own value chain or making up a part of a more sophisticated/diversified product range.

220. Four case studies were also provided that indicated varying levels of illicit enterprise operations as well as the differing investigative responses. The following chapter then focused on the modus operandi pertaining to the money laundering to be associated with ITT.

D. CHAPTER 5: THE MODUS OPERANDI PERTAINING TO THE MONEY LAUNDERING AND TERROR FINANCING TO BE ASSOCIATED WITH ITT

221. For all purposes this chapter was to be the most important as the responses was supposed to provide an indication of how jurisdictions have linked ML to ITT. The primary methods as sighted was as with other typologies dependant on the levels (nature and size) of operations, the technological and infrastructural tools at the launderers disposal as well as the nature of methods of payment to be associated with the product. This included:

a) The use of cash couriers.

b) Cash couriers using private jets and yachts as methods for transportation of the cash.

c) Bulk cash smuggling

d) Money remittance transactions

e) Cash spent on additions to life styles of the perpetrators and therefore subject to self laundering or not laundering the proceeds at all.

f) Commingling, smurfing, use of professional service providers, casinos and real estate purchases.

222. Four case studies were provided to indicate the actual manifestation of the aforementioned. It can however not be stated that the MO pertaining to ML and TF differed significantly from other typologies. Of importance to note are the amounts involved and the low levels of reporting pertaining to the ML or TF. The next chapter therefore focused on the law enforcement response.

E. CHAPTER 6: THE RESPONSE FROM LAW ENFORCEMENT AND SUPPORTING AGENCIES

223. This chapter focused on the responses from customs, law enforcement, FIUs and taxation authorities.

CUSTOMS

224. The following key themes emerged from the responses from Customs Agencies:

a) A disconnect was identified between the investigation of the predicate offence and any associated money laundering investigation(s). Many of the Customs Authorities do not have the capability to undertake a ML investigation and if a cross-agency platform is not in place, the focus remains on the predicate customs or tax offences.

b) The importance of information collection and sharing, nationally and internationally, which helps develop strategies to respond to the threat. While many of the Respondents collect relevant trade data, their answers do not confirm to what extent this is analysed and trends or patterns identified.

225. The majority of respondents have capability within their Customs authorities to investigate any customs offences perpetrated by tobacco smugglers. However, only around half of these same authorities would also conduct a money laundering investigation, with the remaining respondents

referring the matter to other agencies, such as the Police, the FIU or a specified anti-money laundering agency. In such circumstances, it is possible that cases that could be pursued as money laundering investigations are not due to jurisdiction and enforcement limitations of the Customs Authority concerned. In such cases unless detections are referred for financial investigation elsewhere only predicate customs or taxation offences are likely to be pursued. This may be regarded as the reason for the lack of money laundering investigations associated with the illicit tobacco trade.

226. It is apparent that Customs authorities capture or can access a huge library of information, which could support a robust analysis of the risks to their jurisdiction. A key issue is the extent to which information management systems supports existing investigative work and identifies new risk areas, with appropriate analysis of the data to support the development of strategies and policies to help combat the illicit tobacco trade.

LAW ENFORCEMENT

227. The information as provided by the respondents once again indicates that law enforcement agencies do investigate organised crime activities to be associated with ITT but very few examples were sited where ML was also investigated. In the Customs section strong emphasis was placed on the fact that Customs hand over potential money laundering cases or financial investigations to be associated with ITT. It is however clear that very few of these cases are investigated from a money laundering perspective.

FIUS

228. Various jurisdictions demonstrated that they do have STR's associated with ITT. It was disconcerting to note that several of these STR's cannot be linked to subsequent ML law enforcement investigations. This could be reflective of the method used to obtain information for the purposes of developing this typology or be indicative of STR's related to ITT not being converted to ML investigations.

229. FIU's seem to act in a predominant investigative support function and act as a conduit in terms of obtaining and distributing relevant information. The FIU's therefore are not necessarily part of a task team but through their functioning can support existing task teams. Indications were that STR or SAR's had been obtained and forwarded. As mentioned difficulties are experienced to link reports to successfully concluded ML investigations to stem from ITT.

230. Little information was obtained to indicate that FIU's shared STR's related to ITT. This was disconcerting given the fact that ITT is an offence which occurs in multiple jurisdictions. This could be as result of very few customs authorities or taxation authorities reporting STR's to their respective FIU's. This is a clear area where greater strides can be made.

TAXATION AUTHORITIES

231. Some jurisdictions allow for tax evasion (as derived from the smuggling or illicit trade) and the Money Laundering associated with it to be investigated by the tax authorities. The statistics where provided however revealed that very few Money Laundering cases have been investigated

within these jurisdictions even where they have the mandate to do as such. The emphasis once again remaining with the investigation of the predicate offence.

232. Some jurisdictions indicated that they are responsible for investigating the tax evasion offences but that the ML offence investigation is referred to law enforcement agencies. No statistics were provided to indicate the number of cases provided as well as the success rate when viewed from a prosecution perspective.

233. It can therefore ultimately be summated that the responses indicate that the majority of tax authorities do not single out ITT as a significant tax evasion offence and that very few of the authorities conduct ML investigations or refer possible ML investigations to stem from ITT to law enforcement.

234. The inability to share information pertaining to crimes that are committed predominantly within the taxation and customs domain can almost be considered as an incentive to trade illicitly.

a) The primary cause would be the decrease in the risk of detection coupled to lacking criminal procedure and money laundering convictions to stem from the illicit trade.

b) Secondly, not all taxation authorities have investigative powers pertaining to these offences which if seen in the context of lack in sharing of information creates a void from detection, investigation and successful prosecution.

F. THE RESEARCH PROPOSALS

235. Below follows the initially posed research proposals with the resulting findings.

236. Illicit trade in tobacco is a significant predicate offence to money laundering.

a) ITT can be considered a significant predicate offence if one takes the values of smuggled tobacco into account.

b) Lacking money laundering cases to stem from this could however be regarded as indicative that Law Enforcement can either not establish the connection with the smuggling activity and resulting money laundering investigations, or that other predicate offences enjoy preference where ML cases are pursued.

a) A second predicate offence to be linked with ITT is the tax evasion offence. The FATF has recently added this specific offence as a predicate offence. This study however found it difficult to link the specific income derived from ITT with evaded taxes and resulting money laundering cases.

237. The proceeds of illicit trade in tobacco are used to fund terror.

a) Case studies were provided where linkages could be made between ITT and individuals and organisations identified to be involved with terror activities.

b) Some of these individuals established cigarette smuggling rings where the proceeds were derived for the purposes of providing material support to identified terror organisations.

c) Limited examples were however cited to indicate that ITT could specifically be linked to TF when viewed from a multinational/jurisdictional perspective. This deduction is made due to responses only being received from one jurisdiction. It is however acknowledged that ITT can pose a significant vulnerability to generate proceeds in support of terror organisations. This is based on:

   i) Relatively low risks of detection of the smuggling activity.

   ii) Relatively low likelihood in linking the smuggling activity to terror organisations or suspects.

238. Law Enforcement regards the effect of the illicit trade in tobacco as insignificant when compared to trade in other forms of contraband. Responses obtained did not confirm or refute this proposition. Subjective information does however indicate that lacking coordination between the various law enforcement agencies does show a degree of less importance being placed on ITT as for instance levels of cooperation, which coincides with drug smuggling and offenders. This can therefore be considered an area for further study.

239. FIU STRs will be insignificant in terms of identifying illicit trade in tobacco as predicate to ML or TF.

a) Some jurisdictions were able to provide STRs based on ITT. This was not significant when compared to other predicate offences.

b) A possible explanation for this would be that government reporting institutions are not reporting suspicious or falsely declared proceeds or the suspected tax evasion to their respective FIU's.

c) This also provides some difficulty in linking suspected offenders to other forms of organised crime or previous suspicions pertaining to ML and TF.

d) Institutions with reporting obligations have difficulty in identifying suspicious transactions linked to ITT. This is due to the absence of clear indicators to assist in identifying proceeds from ITT. The requirement would therefore be to provide these indicators and allow internal systems to cross verify said information against third party data. It is foreseen that this problem can also be experienced within other typologies.

240. Despite the threat of civil or criminal investigations and disruption, ITT represents a good opportunity for Organised Crime Groups and / or Terror Groups to generate large sums of criminal profit.

a) Academic study reveals that tens of billions of dollars of illicit proceeds are generated through ITT. This is augmented by figures as provided by the WCO. Limited prosecutions where viewed from a worldwide perspective therefore confirms that an environment exists which may be regarded as conducive for ITT to occur.

b) There were specific jurisdictions whose responses indicated that where ITT was considered serious that strong linkages could be proven with OCG's, that it involved highly organised international role-players, and that where subsequent ML or TF was pursued, significant sentences had been handed down

241. The proceeds of ITT is either laundered or used to fund other crimes and or terror.

a) Obtained information suggests that where OCG's or individuals were identified to be involved with ITT that jurisdictions tended to focus more on prosecuting the predicate offence.

b) Lacking prosecution and convictions within this domain would therefore suggest that:

i) OCG's or criminals do not launder the proceeds of ITT of fund terror, or;

ii) Jurisdictions low conviction rates should not be regarded as the primary indicator whether ITT can be linked to ML and TF.

242. The use of trade in tobacco is significant within the trade based money laundering typology.

a) Information obtained was not significant enough to confirm or refute the proposition.

b) It was however noted that the high taxes on tobacco products could act as a deterrent to TBML.

c) The inverse is also true where tobacco products could be traded in low tax areas as a TBML methodology. One jurisdiction sited an example of this.

243. High taxes on tobacco stimulate illicit trade in tobacco. Most jurisdictions as well as academic research confirmed that high taxes acts as one of the incentives for illicit trade in tobacco to occur.

G. FINAL CONCLUSION

244. The aforementioned coupled with low detection rates, low levels of prosecution for offenders, easy payment of fines (pre determined financial risk), lacking cooperation, coordination and information sharing at national and international levels as well as the lacking of a common strategic impetus at said levels, all act as factors to be regarded as conducive towards ITT and resulting ML and TF to occur.

245. The converse is also true. This is insofar as that where jurisdictions have chosen to pursue ITT and associated ML and TF to stem from it, great successes have been attained. Several of the case studies provided attests to this and can act as an incentive for the FATF to highlight more prominent responses were viewed from a jurisdictional perspective. This is especially so with respect to government agency reporting obligations as well as closer cooperation with international bodies where requested.

246. It is trusted that this document will highlight the need to enhance international cooperation and recognize the illicit trade in tobacco as a significant global money laundering and terror financing threat. Future challenges include the identification of financial pinch points, enhancing ML investigations as well as providing improved standardised data to member countries to assist in the shaping of strategic and tactical responses to the Illicit Trade in Tobacco.

BIBLIOGRAPHY

Barford, M.F. (1993), "New dimensions boost cigarette smuggling", *Tobacco Journal International,* 3, 16–8.

Bowers, S. (2003), "Imps directors resign after customs raid", *The Guardian*, 10 July 2003.

Crimaldi, L. (2011), "4 Charged in 5,7 Million Rhode Island Cigarette ring", Associated Press, published in the *Independent Mail*, 9 November 2011

Ellis, M. (2011), "$33 million contraband cigarette ring rounded up in multi state ATF raids", *Independent Mail*, 3 November 2011. http://m.independentmail.com/news/2011/nov/03/33-million-contraband-cigarette-ring-rounded-multi/, accessed on 23 May 2011.

Irish Tax and Customs (2009), *Irish Authorities make record cigarette seizure* published on http://europa.eu/rapid/pressReleasesAction.do?reference=OLAF/09/15&format=HTML&aged=0&language=EN&guiLanguage=en, accessed on 22 May 2012.

Joossens, L. (n.d.), "The international cigarette trade and smuggling", *The Economics of Tobacco Control in Southern Africa*

Joossens, *et al.* (2000), "Issues in Smuggling of Tobacco Products," in Jha, P. and Chaloupka, F. J. (eds.), *Tobacco Control in Developing Countries*, London, Oxford University Press, pp. 393– 406. http://siteresources.worldbank.org/INTETC/Resources/375990-1089904539172/393TO406.PDF, access on 5 January 2012.

Joossens L., *et al.* (2009), *How eliminating the global illicit cigarette trade would increase tax revenue and save lives* , Paris: International Union Against Tuberculosis and Lung Disease; 2009.

Merriman, D. (n.d.), *Understand, Measure and Combat Tobacco Smuggling*, World Bank, http://siteresources.worldbank.org/INTPH/Resources/7Smuggling.pdf, draft, accessed on 29 June 2012.

OLAF (2009), *Individual indicted as part of a large scale cigarette smuggling and money laundering operation*, as published on United States Attorney's Office for the Southern District of Florida, http://www.justice.gov/usao/fls/PressReleases/090306-02.html

Tobacco Manufacturers Association (n.d.), *EU cigarette prices,* www.the-tma.org.uk/tma-publications-research/facts-figures/eu-cigarette-prices/, accessed on 22 May 2012.

Von Lampe, K., *The Nicotine Racket Trafficking in Untaxed Cigarettes: A Case Study of Organised Crime in Germany,* www.organized-crime.de/zightm01.htm#overview , accessed on 5 January 2012.

WCO (World Customs Organiation) (2011), *Customs and Tobacco Report 2010*, Brussels, Belgium.

Appendix TT:

FATF, *FATF President's Paper: Anti-Money Laundering and Counter Terrorist Financing for Judges and Prosecutors* (Paris: FATF, 2018)

FATF

FATF PRESIDENT'S PAPER

Anti-money laundering and counter terrorist financing for judges & prosecutors

June 2018

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2018), *FATF President's paper: Anti-money laundering and counter terrorist financing for judges and prosecutors*, FATF, Paris, France,
www.fatf-gafi.org/publications/methodandtrends/documents/AML-CFT-judges-prosecutors.html

TABLE OF CONTENTS

Foreword

> “The work of judges, prosecutors and other investigative authorities is crucial for stable institutions, transparency and the rule of law, which are all pillars of an effective AML/CFT system.”

Santiago Otamendi
FATF President 2017-2018

It is a pleasure to introduce the FATF President's Paper "Experience, Challenges and Best Practices" on anti-money laundering and counter terrorist financing (AML/CFT) for judges and prosecutors.

Under the Argentine Presidency, the FATF initiated a global outreach programme to the criminal justice systems given the crucial role it plays in the effective implementation of FATF Standards. The work of judges, prosecutors and other investigative authorities is crucial for stable institutions, transparency and the rule of law, which are all pillars of an effective AML/CFT system. The objective of the outreach programme was to reinforce the effectiveness in the investigation and prosecution of ML and TF offences and in the recovery of the proceeds of crime.

This initiative allowed us to learn about the experiences, challenges and best practices in investigating financial criminality from judges and prosecutor from across the globe. The initiative aimed to improve international co-operation and maintain an up-to-date understanding of the methods that are used to launder money from organised crime or to fund terrorism.

The FATF, in a joint effort with the FATF-Style Regional Bodies (FSRBs) and other international organisations, gathered knowledge through six regional workshops which brought together almost 450 judges and prosecutors from more than 150 jurisdictions and observers organisations.

We invited relevant institutions such as the Organization for Security and Co-operation in Europe (OSCE), the International Prosecutors Association, the International Magistrates Association and Asset Recovery Networks to join the conversation and add value to the project considering their unique perspective.

I would like to express my gratitude to the judges and prosecutors that participated in the project; to Argentina, Ecuador, China, Tunisia and Guyana for hosting the workshops; to the Financial Action Task Force of Latin America (GAFILAT), the Caribbean Financial Action Task Force (CFATF), the Asia/Pacific Group on Money Laundering (APG), the Eurasian Group (EAG), the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the Inter Governmental Action Group against Money Laundering in West Africa (GIABA), the Task Force on Money Laundering in Central Africa (GABAC), the Middle East and North Africa Financial Action Task Force (MENAFATF), the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), the OSCE and FATF Training and Research Institute (FATF TREIN) for co-organising and supporting the events; to FATF Delegations for their input on this paper and to the FATF Secretariat for their assistance.

At the FATF Plenary in June 2018, I presented the conclusions of this exercise, which are outlined in this paper. FATF members supported them and agreed to broadly disseminate and publish them through the FATF Global Network and among relevant institutions and organisations.

This paper identified challenges and highlights useful elements and best practices in the conduct of investigations, prosecutions and convictions of money laundering, terrorist financing, and in confiscations of proceeds of crime. It also highlights the need for international cooperation, a key element when investigating criminal networks and recovering assets that are often spread over multiple countries.

Based on these findings, the US Presidency of FATF will continue this joint effort to enhance the effectiveness of the criminal justice system.

I am glad to deliver this important outcome which I hope will help us to produce results in this global fight against money laundering and terrorist financing.

Santiago Otamendi

Executive Summary

FATF global anti-money laundering and countering terrorist financing efforts are focused both on effective prevention and disruption and on achieving convictions and asset recovery for the benefit of States and victims. Although FATF has had some interaction in recent years with prosecutors and similar experts on various issues, the relationship between the FATF and the criminal justice sector needed to be strengthened. For these reasons, the Argentine Presidency of the FATF initiated a global outreach programme to Criminal Justice Systems.

The main objectives of the project were:

- to prepare a report which identifies the experiences and challenges in relation to money laundering (ML) and terrorist financing (TF) investigations and prosecutions and the confiscation of criminal assets, and the good practices to deal with these issues;
- to enhance the FATF outreach to judges, prosecutors and investigators from different regions, boosting current and potential networks of collaboration, and getting practitioners and relevant actors in close contact to discuss their common challenges and possible solutions, generating a framework to enhance international working relationships; and
- to get FATF and FSRBs countries to work together on these key elements of effectiveness for a successful AML/CFT system.

Through several regional workshops , the FATF in a joint effort with the FSRBs and other international organisations[1] brought together almost 450 judges and prosecutors from more than 150 jurisdictions and observers to share experiences and best practices. This FATF President's paper presents the conclusions from the workshops. Some of the main findings are listed below.

1. Relevant organisations were invited to participate and contribute to the discussions such as the Organisation for Security and Co-operation in Europe, the International Prosecutors Association, the International Magistrates Association and Asset Recovery Networks

Underlying and Supporting Elements

ML and TF investigations and prosecutions and the confiscation of criminal assets are supported by a range of important underlying elements in the wider AML/CFT regime:

- A comprehensive understanding of the jurisdiction's ML and TF risks sets the foundation for an effective AML/CFT regime.
- Effective and timely domestic co-operation and co-ordination is fundamental. Some good practices in this area include setting up a permanent multi-agency coordinating committee on ML/TF and establishing robust inter-agency working relationships based on mutual trust.
- The creation of multidisciplinary agencies/ units that focus on ML/TF and/or on asset confiscation, or at a minimum having expert staffs that are dedicated to this role within larger agencies or public prosecution services.
- Collaborating with the private sector to both provide and obtain information related to ML/TF.
- Provide specialised training for investigators and prosecutors – particularly focusing on building skills in gathering information and evidence, financial investigative techniques, and presenting complex cases to judges or juries.

Money Laundering: Investigation, prosecution and convictions

Investigating and prosecuting money laundering (ML) offences presents a distinct set of challenges for jurisdictions. The overall results of the assessments conducted to date demonstrate the significant challenges that countries face in obtaining convictions. Among the good practices mentioned in the report, some that could be highlighted are:

- Properly criminalising the offence: expand the scope of predicate offences to the broadest list of serious offences or to adopt an all-crimes approach, which may provide clarity and more flexibility for the prosecutors, especially when combined with a system that also incorporates the principle of opportunity.
- Establish, whether through legislation or case precedent, that the predicate offence need not be proven in order to convict for ML, as established in the FATF Recommendations.
- Fixing plea bargaining and deferral prosecution agreements as a legal possibility, subject to judicial control and oversight.
- Having internal guidelines, handbooks, or in-person trainings to teach investigators how to begin and pursue a basic financial inquiry. Also, to have policies or directives which establish the mandatory requirement of opening a parallel financial investigation in every investigation of a predicate offense of ML.

Terrorist Financing: Investigations, prosecutions, and convictions

Investigating and prosecuting terrorist financing (TF) offences presents a distinct set of challenges for jurisdictions. The majority of the reviewed jurisdictions had not prosecuted TF offences or obtained TF convictions at the time of their mutual evaluation. Among the good practices mentioned in the report, some that could be highlighted are:

- Comprehensive criminalisation of TF is directly related to the jurisdiction's ability to investigate and prosecute TF effectively. Drafting the offence to be as broad as possible: for example, structuring the offence in a way that the suspect's intent to finance specific terrorist acts does not need to be proven.

- Ensuring that a TF investigation can be launched without an underlying terrorism case, and that the TF investigation can continue even where the linked terrorism investigation has already been concluded.

- Having legislation or judicial procedures that specifically deals with the use or introduction of classified material or intelligence (e.g. laws or rules may permit judges and/or defence counsel to review information, redactions may be made, information can be "declassified" by the state, etc.).

- Involving the prosecutor at an early stage to determine what pieces of intelligence may be admissible as evidence, or what steps would need to be taken for it to be admissible.

- Having a designated special court to deal with terrorism and terrorist financing cases that often include classified information.

Confiscation: freezing, seizing, and recovering assets

Tracing, freezing and confiscating the proceeds and instrumentalities of crime is fundamental to the effectiveness of measures to combat money laundering and terrorist financing. Serious crime generates a vast amount of proceeds every year. However, the level of implementation of an effective confiscation regime among the assessed countries is modest at best. Some practices particularly useful for asset confiscation are:

- Ensuring that criminal asset confiscation is a policy priority, with a linked strategy that sets out how all relevant authorities can work to achieve the objectives/goals that are set.
- Having a full range of powers to trace, freeze and confiscate criminal proceeds and instrumentalities, including the ability to quickly seize assets of the defendant and associated third parties, confiscation powers that rely on civil standard of proof, or are non-conviction based or where there are appropriate provisions to reverse the burden of proof.
- An effective framework to manage or oversee the management of frozen, seized, and confiscated property, including by competent authorities that are freestanding or part of an LEA, and, as needed, the ability to hire outside vendors or contractors for complex assets.
- Working in co-operation with international partners was seen as a key ingredient of success, especially early outreach to freeze criminal assets subject to confiscation.

International co-operation: mutual legal assistance, extradition & other co-operation

International co-operation is often critical to the success of ML/TF investigations and prosecutions and also for asset recovery. ML and TF networks are often spread over multiple countries and foreign jurisdictions may have the missing pieces of information or evidence which facilitate a successful prosecution.

- Devoting sufficient resources to rapidly process and respond to requests, including having mechanisms and technology that allow authorities to engage in a dialogue with the requesting countries to facilitate case consultations.
- Considering informal methods of international co-operation such as FIU-FIU, police-police or prosecutor-prosecutor co-operation before submitting a formal MLA request.
- Using networks as such as EUROJUST or CARIN and ARINs prior to making a formal request to facilitate international co-operation and target the assistance that will be sought.
- Making contact with overseas authorities and sending a draft copy of a proposed MLA request, so that they can advise on the content and wording of the request.
- Using the Mutual Legal Assistance Request Writer Tool (MLA Tool) that has been developed by UNODC to assist states to draft requests with a view to facilitate and strengthen international co-operation.

FATF/MONEYVAL/OSCE Workshop for Judges and Prosecutors
March 2018, Strasbourg, France

FATF/GAFILAT/CFATF Workshop for Judges and Prosecutors
September 2017, Quito, Ecuador

Introduction

FATF President Santiago Otamendi
FATF/GAFILAT/CFATF Workshop for Judges and Prosecutors
September 2017, Quito, Ecuador

FATF is committed to maintaining a comprehensive understanding of how criminals launder money and how terrorists raise, move, and use funds with the key objective of ensuring up-to-date and effective global standards and their effective implementation.

While the supervisory and regulatory agencies and the private sector play a critical role in preventing money laundering and terrorist and proliferation financing, there is agreement that if global AML/CFT efforts are to be effective, countries must have strong operational authorities to bring prosecutions and obtain convictions, as well as to seize and confiscate the proceeds and instrumentalities of crime for the benefit of states and victims.

As shown through the Mutual Evaluation Reports conducted on the basis of the 2012 FATF standards and 2013 Methodology, many countries have enacted the necessary legislative measures to criminalise money laundering (ML), as well as terrorist financing (TF), however, the results obtained in terms of convictions and confiscations are modest overall. Achieving results in this area of the AML/CFT regime is mainly an issue for prosecutors, judges and investigators, as part of the criminal justice system. From the initiation of an investigation through the sentencing of a defendant, the criminal justice system can involve many governmental actors with different roles who need to coordinate among domestic authorities and international partners to fight ML and TF threats which are increasingly global in nature.

Additionally, financial institutions and DNFBPs covered by the FATF Standards are subject to laws and regulations at the national level. Generally, supervisors ensure compliance with AML/CFT measures, but in exceptional cases, compliance failings may also be dealt in the criminal justice system.

The correct functioning of the criminal justice system must be supported by foundational elements such as stable institutions, accountability, integrity, transparency and the rule of law. These are all pillars of an effective AML/CFT system.

Although FATF has had some interaction in recent years with prosecutors and similar experts on various issues, the relationship between the FATF and the criminal justice sector needed to be strengthened. An enhanced engagement, collaboration and effective communication with the prosecutorial services, investigating judges and some other elements of the criminal justice system is vital given the crucial role they play in the effective implementation of the FATF Standards.

For these reasons, the Argentinean FATF Presidency decided to bring forward an initiative intended to share experiences, and to identify the challenges and good practices which can be critical for improving jurisdictions' effectiveness in terms of ML/TF prosecutions and confiscating criminal proceeds.

Participant at the FATF/MONEYVAL/OSCE Workshop for Judges and Prosecutors
March 2018, Strasbourg, France

Objectives

The main objective of the project is to produce a report that identifies those experiences and challenges, and good practices to deal with them. The paper focuses on the factors that can result in an effective system for prosecution and confiscation, and less on technical legal requirements, although the report also seeks to identify legal powers that appear to lead to effective results.

Also the initiative is designed to enhance the FATF outreach to judges, prosecutors and investigators from different regions. The aim was to, establish networks of collaboration and facilitate discussion among practitioners about common challenges and possible solutions, generating the opportunity to build valuable work relationships. Thus, jurisdictions could learn from each other not just in a theoretical sense as well as make contact with regional and inter-regional counterparts that could be useful in operational matters.

The project also had the benefit of bringing the FATF and FSRB countries together to work more effectively on the investigation and prosecution of ML and TF and the recovery of assets. This is an important element considering that through the mutual evaluation process, it has been observed that most of the countries that are part of the FATF Global Network had had challenges in these particular areas.[2]

Finally, this initiative provided an opportunity for the FATF to extend the outreach and scope of collaboration to other relevant international or inter-governmental organisations.

2 See the analysis of the results of IO7, IO8 and IO9 in each of the dedicated sections.

Methodology

The primary source of information for the exercise was the series of workshops for investigating judges and prosecutors, which were organised by the FATF on a regional basis, in conjunction and with the support of FSRBs and the hosting countries/organisations. These workshops provided a venue to gather experiences and views from a wide perspective of different practitioners on the challenges and difficulties they face in combating ML and TF, and on effective mechanisms and good practices to deal with these.

The information on the experiences drawn from the workshops was supplemented by a desk review of relevant reports and material on these issues and on a horizontal review of all the published Mutual Evaluation Reports, focusing on the country results on the relevant immediate outcomes, as further described below.

Based on the information and views expressed during the workshops, combined with the results of the desk review and the horizontal study, the FATF Secretariat with the support of FATF TREIN, conducted an analysis and identified challenges and good practices, including issues specific to particular regions or type of legal system, and areas for potential further work. That information and analysis is the basis for this report.

FATF President Santiago Otamendi
FATF/MONEYVAL/OSCE Workshop for Judges and Prosecutors
March 2018, Strasbourg, France

FATF President Santiago Otamendi
FATF/GAFILAT/CFATF Workshop for Judges and Prosecutors
September 2017, Quito, Ecuador

The workshops

In order to ensure that experts in all regions had an opportunity to input into the project, and to gather the full range of experiences and views that included a regional perspective, FATF conducted an evolving process of regionally-based workshops in co-ordination with each of the FSRBs:[3]

- Americas - GAFILAT and CFATF
  September 2017
- Asia/Pacific - APG and EAG
  January 2018
- Africa/Middle East - ESAAMLG, GIABA, GABAC and MENAFATF
  February 2018
- Europe - MONEYVAL and the Organization for Security and Co-operation in Europe (OSCE)
  March 2018
- FATF wrap up workshop
  May 2018[4]

Through workshops in different regions, the FATF brought together almost 450 judges and prosecutors from more than 150 jurisdictions to share experiences and best practices. In addition to the FATF and FSRB Secretariats and FATF TREIN, relevant international organisations such as the OSCE, the International Prosecutors Association, the International Magistrate Association and the various Asset Recovery Networks participated and contributed to the discussions.

3 There were another two workshops conducted by CFATF (May 2018) and by GAFILAT (April 2018). Both FSRBs sent a report setting out the topics discussed, the participation and conclusions, which were considered for this report.

4 With the support of FATF TREIN.

Scope

The topics for discussion during the workshops were generally the challenges and good practices around:

- investigating and prosecuting money laundering cases,
- investigating and prosecuting terrorist financing cases,
- seizing and confiscating criminal proceeds and instrumentalities and
- providing international co-operation and mutual legal assistance.

Participants in each of the workshops included investigating judges and magistrates, prosecutors, and investigators with experience and expertise in investigating and prosecuting ML and TF, or seizing and confiscating assets. Participants from FATF members attended various workshops, while those from the FSRBs were involved with the workshop in their region.

Participant at the FATF/ GAFILAT/CFATF Workshop for Judges and Prosecutors
September 2017, Quito, Ecuador

Underlying and Supporting Elements

Identifying risks, strategic policies and priorities

A comprehensive understanding of the jurisdiction's ML and TF risks sets the foundation for an effective AML/CFT regime. Properly identifying the risks and common ML/TF methods also assists investigators and prosecutors in detecting and ultimately proving criminal activities. The workshops for judges and prosecutors highlighted the good practice of involving investigators and prosecutors in the risk assessment process. These actors can provide information that feeds into the countries' overall understanding of risk by participating in the process.

In addition to helping authorities identify criminal threats, a good understanding of ML and TF risks contributes to the setting of national strategies and priorities for combatting ML and TF. Knowing the level and type of risks in the country helps to allocate resources for agencies charged with investigation and prosecution, including resources that can be used to hire personnel, train them, and build specialised capacity. In the case of TF, the jurisdiction should integrate counter-terrorism and CFT strategies, to the extent possible.

The strategies should clearly articulate why criminal prosecutions and asset confiscation are desirable outcomes. They should also be used to incentivise investigations, prosecutions, and confiscation of assets. For example, many jurisdictions have set up asset forfeiture funds which can be used to fight crime, benefit society, or compensate the victims of crime. If appropriately used, these mechanisms can provide useful incentives for action. Strategies can also inform the budgetary process and ensure adequate resources for the law enforcement authorities (LEAs), including prosecutorial authorities and asset confiscation units. Finally, the involvement of the criminal justice sector in the risk assessment or even strategy-making process can promote legislative change, as those who work with the law most closely are in a good position to identify loopholes or areas for potential changes and updates.

ML and TF investigations and prosecutions and the confiscation of criminal assets are supported by a range of underlying elements in the wider AML/CFT regime. This section explores the FATF and FSRB jurisdictions' experiences related to certain aspects of the wider framework surrounding the work of investigators, prosecutors and judges. It also highlights specific challenges and good practices.

Institutional framework

Investigating and prosecuting ML/TF cases often involves broad set agencies with differing skills. It is therefore important to ensure that the institutional framework to investigate and prosecute these offences incorporates the appropriate range of agencies and facilitates the use of specialist expertise where necessary.

One of the key good practices discussed in the workshops is the "task force" model of investigation. This may include setting up multi-disciplinary teams to conduct ML or TF investigations and collaborate on the development of cases. Effective task forces can consist of a mix of investigators, specialised LEAs (such as drug, tax, anti-corruption, or customs agencies), prosecutorial offices, intelligence authorities, and financial analysts, to include the FIU. The exact composition of the task force depends on national practice, but the intention of the task force model is to leverage expertise, resources, tools and authorities in an interagency setting to achieve the best results. Such models also help avoid operational conflicts and bring all relevant authorities together, potentially with the effect of speeding up the completion of cases and simplifying tasks.

Another good practice is setting up specialised ML/TF investigation units and designating specialised prosecutors to focus on ML/TF and asset confiscation cases. The task forces and special units should be sufficiently resourced, including staff with the requisite skill-sets. A good practice is to use special expertise such as forensic accountants, financial analysts and experts in computer forensics in investigations. If necessary, this expertise can be employed from external sources outside of the unit or task force.

Domestic co-operation and information sharing

The workshops highlighted the importance of effective and timely domestic co-operation and co-ordination. This is particularly critical in TF cases. Some good practices in this area include setting up a permanent multi-agency coordinating committee on ML/TF and building up trust between domestic agencies. [5]

Involving multiple agencies in the investigative process also increases the need to share information across institutional borders. This can be acute where the investigative and prosecutorial authorities are separated – such as in common law jurisdictions. Where the authorities are separated, involving the prosecutor in the investigation at an early stage has proven to be a useful practice. Practitioners mentioned that such early involvement can guide investigators to develop useful, admissible evidence that can prove the elements of the offense and that prosecutors may be necessary in seeking the authority to use certain investigative techniques. Additionally, in jurisdictions where authorities have prosecutorial discretion, working hand-in-hand with investigators can increase the chances that the police "referral" will result in charges.

In 2017, the FATF finalised a guidance paper to improve co-operation and exchange of information within jurisdictions: Inter-agency CT/CFT information sharing: good practices and practical tools. While not publicly available, the guidance is accessible to agencies involved in combatting terrorism and its financing, as well as agencies not traditionally involved in CFT activities.

5. In terms of TF, the MER of the United States notes that the task force environment in that country is particularly useful for enhancing information-sharing and expertise and helping the authorities to conduct financial investigations effectively. The U.S. approach consists of 104 multi-jurisdictional (i.e. federal, state, and local) Joint Terrorism Task Forces (JTTFs) led by the Federal Bureau of Investigation.

Engagement with the private sector

Many jurisdictions participating in the workshops highlighted the importance of collaboration with the private sector to both provide and obtain information related to ML/TF. Some good practices include:

- Setting up public-private partnerships to facilitate information sharing, and producing typologies together with the private sector[6].
- Sharing sanitised information about real cases and other contextual data.
- Supporting the private sector in identifying ML/TF cases by providing red flags, risk indicators and feedback on suspicious transaction reports.
- Particularly for TF, engaging with a broad range of private sector entities beyond the financial sector, such as airline and rental car companies and retail stores.

Capacity and experience

Many of the practitioners noted the lack of capacity and experience to investigate and prosecute ML/TF cases and confiscate assets in their jurisdictions. Jurisdictions have found it beneficial to provide specialised training for investigators and prosecutors – particularly focusing on building skills in gathering information and evidence, financial investigative techniques, and presenting complex cases to judges or juries. The capacity building was often triggered by a risk assessment, or when ML/TF issues were prioritised at a national level.

It was noted during the workshop that many jurisdictions with only a few TF investigations and often no TF prosecutions face particular challenges in building expertise and capacity in the TF field. This can be problematic because when TF expertise is required, it is usually at a very short notice. Joint investigations, if the facts permit partnering with a foreign LEA, could partly alleviate this issue through "case mentoring". The workshops also highlighted the importance of having capacity to not only respond to TF cases, but to proactively look for and identify potential TF activity, especially in jurisdictions where there is a low risk of terrorist attacks.

6 The joint typologies work completed by authorities in the Netherlands with the private sector was noted as a useful example.

Money Laundering
Investigation, prosecution and convictions

Results of the FATF/FSRB Mutual Evaluations

Immediate Outcome 7

Immediate Outcome 7 of the FATF Methodology measures the extent to which ML offences and activities are investigated, prosecuted and subject to effective, proportionate and dissuasive sanctions. In line with the FATF Methodology, the jurisdictions' effectiveness is determined by considering five core issues[7]:

- How well and in what circumstances potential cases of ML are identified and investigated;
- Whether the types of ML activity being investigated and prosecuted are consistent with the country's threats and risk profile and national AM/CFT policies;
- Whether different types of ML cases are prosecuted (e.g. foreign predicate offences, third-party laundering, stand-alone offence) and offenders convicted;
- Whether the sanctions applied against natural or legal persons convicted of ML offences are effective, proportionate and dissuasive;
- Whether countries apply other criminal justice measured in cases where an ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure an ML conviction.

Of the 50 country assessments completed in the current round of mutual evaluations, only 7 countries achieved a substantial level of effectiveness while none were able to demonstrate a high level of effectiveness.

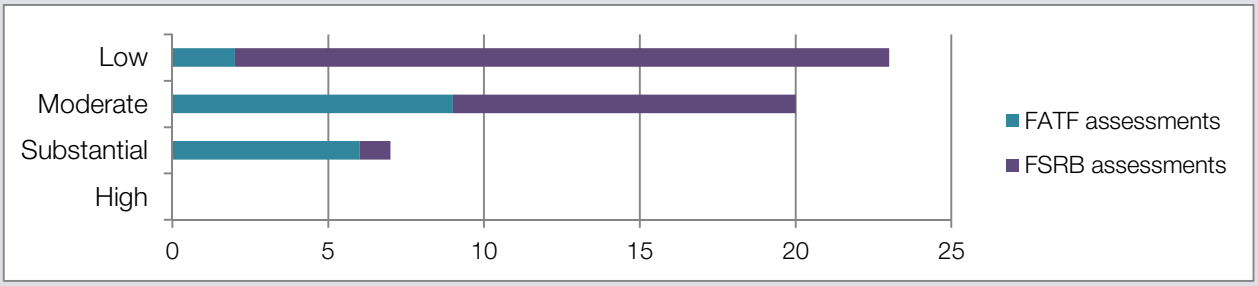
This section is intended to provide targeted analysis regarding the implementation of an effective criminal system response to money laundering offences. It is based on the findings of the discussions conducted during the workshops and on the horizontal and the literature reviews done by the FATF Secretariat with the support of FATF TREIN. It also discusses the legislative basis and of other core elements of effectiveness, such as the proper use of parallel financial investigations, the production and use of evidence and the specific investigative powers and techniques that could be useful to obtain successful results in this area.

7. The full text of the core issues can be found in the FATF Methodology, as well as examples of information and specific factors that a country may use to demonstrate effectiveness. See http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

Table 1. Effectiveness results under Immediate Outcome 7

	Number	High		Substantial		Moderate		Low	
		Number	%	Number	%	Number	%	Number	%
FATF assessments	17	0	0%	6	33%	9	53%	2%	12%
FSRB assessments	33	0	0%	1	3%	11	33%	21	64%
All assessments	50	0	0%	7	14%	20	40%	23%	40%

Figure 1. Comparison between FATF and FSRB member countries on effectiveness with Immediate Outcome 7



Note Table 1 and Figure 1: Results from the 4th Round of Mutual Evaluations as at 15 May 2018
Source Table 1 and Figure 1: Published assessment reports and the consolidated assessment ratings, available on www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

While FATF countries obtained better results on effective implementation, the overall results demonstrate the significant challenges that countries faces. Also, where jurisdictions had obtained convictions, the sanctions were often not considered effective, proportionate or dissuasive. This is another indication of the challenges that countries are facing in investigating and prosecuting ML offences.

Overall, these very modest results across the Global Network demonstrate the significant challenges that countries around the global network have experienced in effectively combatting ML activity through investigation and prosecution. These results suggest that countries could improve how they investigate and prosecute ML offences. The results may also signify a variety of other realities and country circumstances, such as a lack of data and statistics, an insufficient priority placed on ML, inadequate resources or weak institution, corruption that impacts the criminal justice system, or even poor preparation or presentation in connection with the mutual evaluation process.

Technical compliance

On the technical compliance side, the assessments of Recommendations 3, 30 and 31 show that countries generally had established the necessary legal and institutional frameworks for investigating and prosecuting ML in their national system.

Recommendation 3 requires countries to criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (Palermo Convention). It also establishes that countries should apply the crime of ML to all serious offences, with a view to including the widest range of predicate offences.

The level of compliance with Recommendation 3, throughout the Global Network, is substantial.

Figure 2. Technical compliance with Recommendation 3 (money laundering offence)

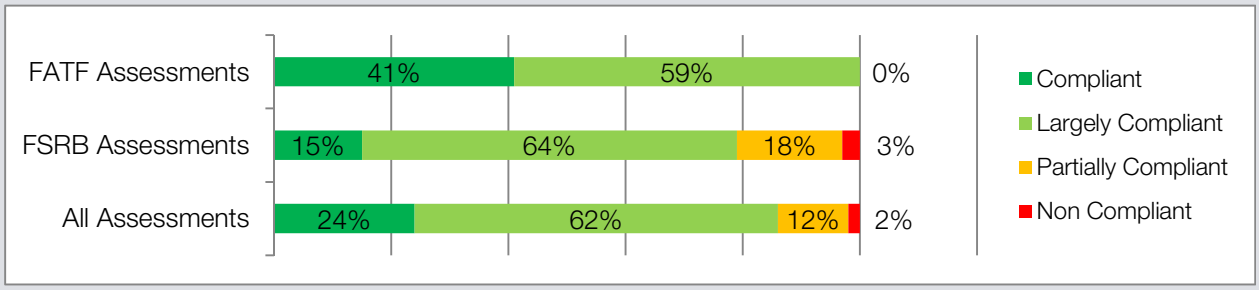


Figure 3. Technical compliance with Recommendation 30 (responsibilities of law enforcement and investigative authorities)

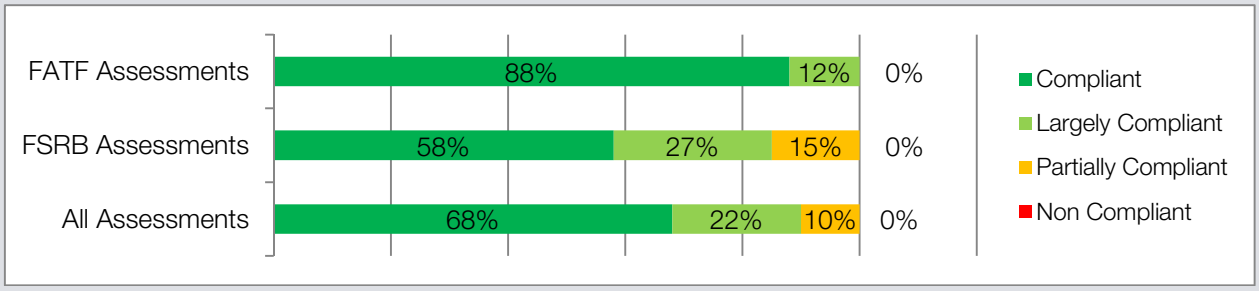
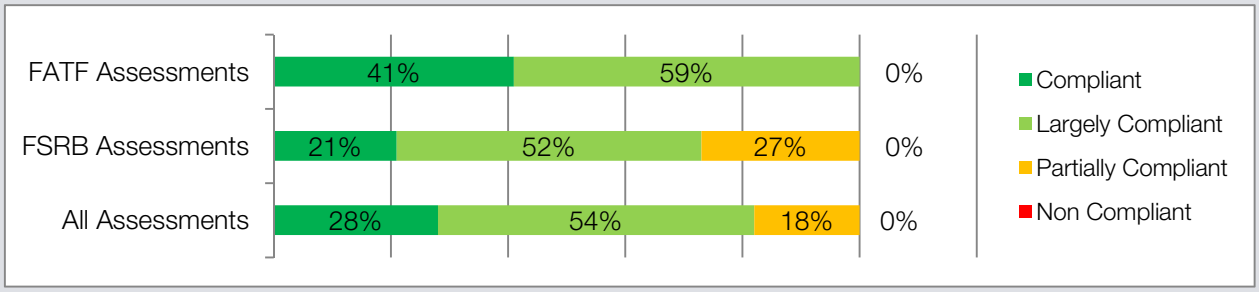


Figure 4. Technical compliance with Recommendation 31 (powers of law enforcement and investigative authorities)



Note Figures 2-4: Results from the 4th Round of Mutual Evaluations as at 15 May 2018
Source Figures 2-4: Published assessment reports and the consolidated assessment ratings, available on www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

Around 86% of the assessed countries have no shortcomings or minor shortcomings. This demonstrates that there is a good technical implementation of this standard.

Recommendation 30 sets the responsibilities of law enforcement and investigative authorities, demanding that countries should ensure that designated law enforcement authorities have responsibility for ML and TF investigations within the framework of national AML/CFT policies.

The level of compliance with recommendation 30, throughout the Global Network, is very positive. Around 90% of the assessments revealed that countries have no shortcomings or minor shortcomings. This demonstrates that most countries have clearly designated authorities that are responsible for investigating ML/TF offences.

Finally, recommendation 31 establishes the basis of the powers that law enforcement and investigative authorities should have in order to carry out their missions. This includes the possibility to: access all documents and information needed during an investigation; compel the production of records held by financial institutions, DNFBPs, and other natural or legal persons; search persons and premises; take witness statements; and seize and obtain evidence. It also establishes that competent authorities need to be able to use a wide range of investigative techniques, including special techniques that are suitable for the investigation of ML, associated predicate offences, and terrorist financing.

The level of compliance with recommendation 31, throughout the Global Network, is largely good. Around 82% of assessments reveal that countries have no shortcomings or minor shortcomings. This demonstrates that generally most countries have the necessary investigative powers and tools to pursue ML/TF offences.

Legislative basis

To effectively investigate and prosecute money laundering, countries must start with properly criminalising the offence. FATF recommendation 3 (R.3) sets out the specific elements required to comply with the obligation to criminalise money laundering based on the Vienna and the Palermo conventions. In addition, R.3 contains other elements which go beyond the various obligations in the international conventions.

- Experts from several jurisdictions highlighted challenges they face in utilising their domestic ML offences.

- Some participants reported that their national legislation still contains a requirement to prove the predicate offence beyond reasonable doubt in order to be able to convict for ML.

- Other participants from countries without an "all crimes" approach to predicate offenses expressed a desire for simpler legislation that clearly defined the crimes which can be the basis for money laundering charges.

- Also, participants signalled that it could be problematic when legislation does not define properly the extent of subjective knowledge that is sufficient to prove the offence, considering that an unclear standard of proof can cause difficulties in relation to the principle of presumption of innocence and how the defendant can use that to his advantage.

- Finally, it was mentioned that in several countries, the criminalisation of self-laundering is not possible due to constitutional issues and that limits the capacity to investigate and prosecute those types of cases. It should be noted though that in all FATF evaluations where jurisdictions have argued that criminalising self-laundering is contrary to fundamental principles of domestic law, this has been rejected by the Plenary.

It is a common practice in many jurisdictions to focus on the prosecution of the predicate offence and to ignore or deprioritise the prosecution of related ML. This is reportedly done for various reasons: the evidentiary thresholds under other legislation may be easier to meet, or the prosecutors may be more familiar with prosecuting predicate offences and have not been sufficiently trained on the benefit or importance of pursuing ML charges. In some cases, it might be easier to convict on the predicate offence, as the prosecutor has already accumulated enough evidence to proceed with predicate charges but has not fully developed the financial evidence needed to bring ML charges. There are many justifications for the pursuit of predicate offenses at the exclusion of ML related to convenience. Prosecuting ML in addition to a predicate offence is often resource-intensive and time-consuming. In some countries, the laws did not properly incentivise ML charges because the sentence would be essentially the same if the defendant were only prosecuted for the predicate offense.

While there are differences in legal traditions and the way legislation is drafted in jurisdictions, some good practices related to criminalising ML can be identified:

- It was recommended during the workshops to expand the scope of predicate offences to the broader list of serious offences or to adopt an all-crimes approach, which may provide clarity and more flexibility to the prosecutors, especially when combined with a system that also incorporates the principle of opportunity. It should be noted that Recommendation 3 does require coverage of all serious crimes as predicate offenses, to include, at a minimum, those listed in the Glossary to the FATF Recommendations (i.e. a range of crimes within 21 different categories).

- It was also stated as a good practice to elaborate the definition of subjective knowledge, either in the law establishing the ML offense or through case law.

Practitioners felt it was better to work with a lower threshold on the mens rea element, such that they would only need to demonstrate that the defendant had a belief or suspicion of the possible illicit origin of the funds. The ability to show "willful blindness" or that the defendant should have known that the funds or assets were criminally derived, was also deemed useful.

- Several practitioners agreed that it was helpful to establish, whether through legislation or case precedent, that the predicate offence need not be proven in order to convict for ML, as established in the FATF Recommendations. Some practitioners noted that their domestic laws have removed the obligation to prove that money laundered comes from a criminal act altogether.

- Some participants mentioned that it is sufficient for the prosecutor to demonstrate that the defendant has unexplained wealth, which then places the burden on the defendant to provide an objectively reasonable explanation for why he has or dealt with funds under investigation. This was presented by the Dutch delegation as the consistent approach they take for ML cases; being this one of what they call the "6 steps approach."[8] This means that building on unexplained wealth or a tax inconsistency, investigators are able to start an investigation for ML even though they do not have direct evidence of a specific predicate offence. After an initial showing by the state, the Dutch system reserves the burden of proof to the indicted, requiring him to explain the licit origin of the funds. Other delegations noted that while prosecutors must show that the proceeds have derived from some criminal offense, they need not show which specific act generated them, or, in other words, a crime committed on a certain day, by a certain person.

The European Court of Human Rights in a recent decision[9] found that reversing the burden of proof after a prima facie showing is in line with the conventional law. The Court agreed that the practice is respectful of the principles of innocence and of fair trail, as long as the defendant has the possibility defend against the ML charges.

A good practice which has proven useful in some jurisdictions is plea bargaining, or the process of settling a criminal case with a defendant in exchange for him pleading guilty to some crime in addition to providing co-operation. Often, this can result in the defendant admitting guilt to less serious or fewer offenses than those alleged in the indictment. Thus, the defendant may receive a lower sentence than would have been otherwise possible.

The "bargain" benefits the defendant because, if he had gone to trial, he could have been found guilty of all charges against him (particularly in a country with a high conviction rate) and/or faced a much stiffer sentence. The government benefits from economy of not putting on a full trial, and, more importantly, the government could stand to gain valuable co-operation from the defendant, who may provide evidence or testimony which can be used against other, higher-level targets in the criminal organisation or conspiracy.

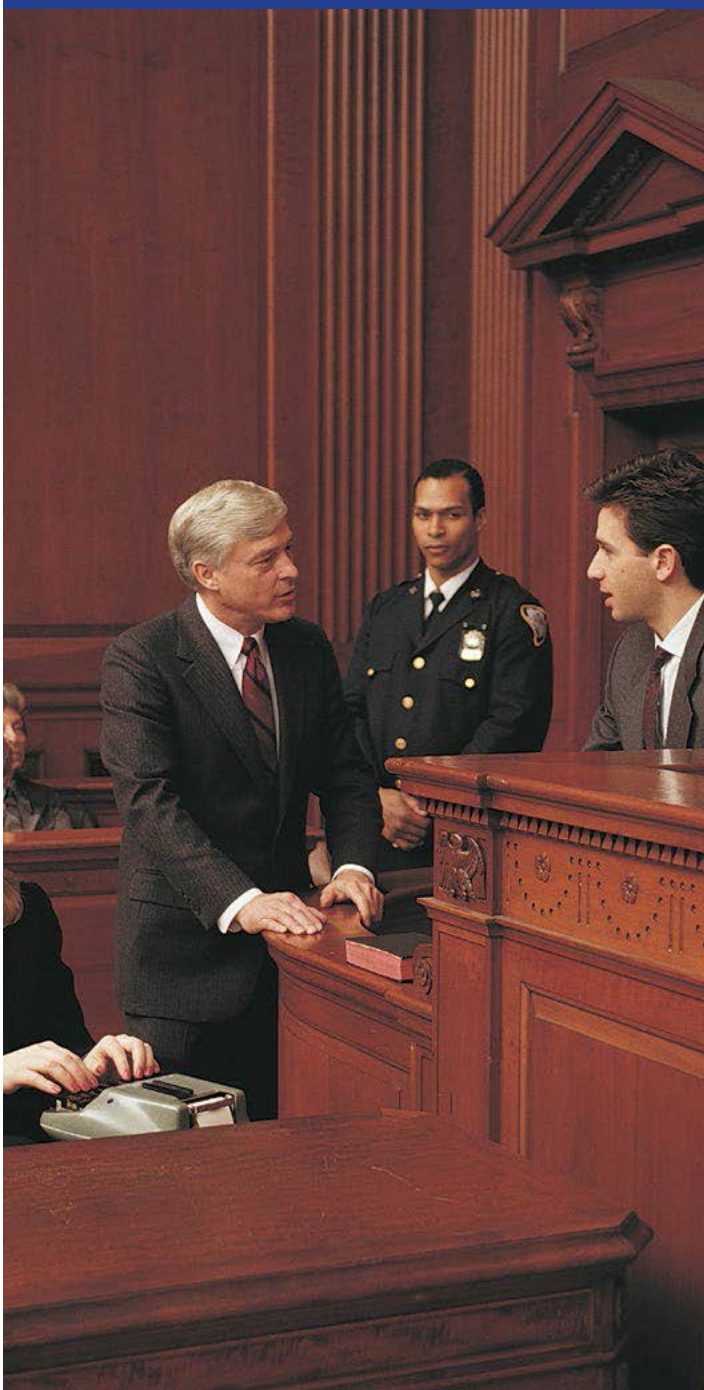
Another similar legal power is a deferred prosecution agreement, which is an agreement reached between a prosecutor and an organisation which could be prosecuted, permitting a prosecution to be suspended for a defined period provided that the organisation meets certain specified conditions. Both legal powers should be subject to judicial control and oversight.

8. The 6 steps are: 1) no direct evidence of a specific predicate offence; 2) a suspicion of ML; 3) obtaining the statement of the suspect; 4) abiding by the requirements for a suspect's statement; 5) investigation by the Public Prosecution Service; 6) drawing a conclusion.

9. Zschüschen v. Belgium (application no. 23572/07)

However, it was also mentioned that the practice of plea bargaining or deferred prosecution agreement would be challenging or impossible in those criminal systems that rely on the principle of legality and do not give the prosecutor the power to negotiate.

Furthermore, it was also stated that the principle of opportunity is a very important tool considering the primary importance of choosing the best or most impactful cases to investigate and prosecute and not having to prosecute all crimes, which can be very resource intensive. Prosecutorial discretion was widely regarded as a good feature, especially in light of the risk of setting bad judicial precedents or prosecuting those not truly worthy of punishment.



Burden and standard of proof

The issue of the burden of proof was discussed during the workshops as a potential challenging area for the prosecution of the ML offence. While several countries' laws permit a reversal or shifting of the burden of proof, other countries' laws or constitutions contain a principle or presumption of innocence. This means that the prosecution has the responsibility to prove that the defendant committed the crime beyond reasonable doubt. In the context of ML, it also means that the "proceeds" element must be proven as well: the funds involved must be shown to be derived from an illicit source. Countries that permit a shifting, or dynamic, burden of proof have expressed that this has proven to be very useful.

Evidence

One of the biggest challenges in ML cases is gathering the evidence linking the assets to the criminal activities or proving that assets/ funds that were laundered were derived from an offence (either committed by the accused or a third party). It is not uncommon for this element to be required to be proven at trial, and it is also, ordinarily, the element requiring the deepest investigation.

To establish this link, practitioners must identify and trace assets or "follow the money" until the connection between the predicate offense and the assets can be determined.

Establishing this nexus between a financial transaction and a predicate offence may be essential for certain investigative measures in some countries (e.g. production orders, search warrants, wire-tapping orders, and surveillance orders). Other legal systems may require a lesser showing (e.g. probable cause or relevance), but investigators and/or prosecutors in many countries must seek judicial authorisation when obtaining evidence via more intrusive methods.

Furthermore, competent authorities expressed that they may have difficulty showing that the defendant knew he or she was dealing with criminal proceeds or that he intended to conceal or disguise them, depending on national requirements.

During the workshops, participants agreed that, in line with the FATF Standards, it is imperative to be able to use circumstantial evidence, especially with regard to the knowledge or intent of the defendant and the showing that the money laundered, was, in fact, dirty. Also, it was noted as a good practice to have legislation admitting a test of reasonable grounds to prove that proceeds have a criminal source.

ML investigations are often driven or reliant on financial intelligence provided by the FIU. Workshop attendees discussed how prosecutors could be tempted to utilise that information directly in the process instead of obtaining the underlying evidence upon which the financial intelligence report was based. This temptation could be especially strong when the case has cross-border elements (i.e. in situations where information is exchanged through the Egmont Group channels). In this regard, it was noted as a good practice to train practitioners on the characteristics of the information-sharing system, the powers and capacities of the FIUs, and on the guidelines and limitations on use for information obtained through the Egmont Group.[10] Also, close engagement between the investigators and the FIU may help to have a clear understanding of the possibilities and the limits of the financial intelligence that the FIU can provide.

It was mentioned that financial intelligence is an excellent source of lead information, but in many countries, it should not be used as evidence. In some countries, the FIU may be able to participate as a party to the prosecution, and in rare cases, the defendant may be able to access financial intelligence if it contains evidence tending to exculpate him.

10. https://www.egmontgroup.org/en/document-library

Powers and techniques

Recommendation 31 provides a framework for the powers that law enforcement and investigative authorities should have. Experts stressed the importance of competent authorities conducting investigations of ML, associated predicate offences, or TF should be able to access all necessary documents and information for use in those investigations and prosecutions. This should include available compulsory measures to: obtain records held by financial institutions, DNFBPs and other natural or legal persons; search of persons and premises; take witness statements; and seize and obtain evidence.

The FATF Standards also requires jurisdictions to be able to use a wide range of other investigative techniques, some of which entail more specialised expertise, such as undercover operations, intercepting communications, accessing computer systems, and conducting controlled deliveries. Participants from certain regions stated that the use of particular investigative techniques was more or less common, but their use, generally, seemed to be on the rise. Some challenges were mentioned with regard to a lack of capacity to conduct forensic investigations (e.g. of computer hard drives), accessing evidence held by foreign service providers, or limited technical tools to intercept communications. Some practitioners mentioned successful experiences in co-ordinating controlled deliveries with international partners.

Other tools and techniques emerged the workshops discussions as being effective for combatting ML were: the capacity to conduct electronic surveillance or location tracking, phone geolocation and communication trends analysis, and having the capacity to do audio or video recordings in public spaces. Also mentioned were several new tech-related tools such as monitoring internet use and gathering forensic information from the dark web (e.g. block-chain analysis technologies). Finally, it was signalled that being able to access and intercept social media communications and to monitor other web-based chats and chat rooms could potentially provide important inputs to the investigations. Encrypted communication channels were deemed problematic by the participants.

It was noted during the workshops that investigators should ensure that the tools and techniques are not a substitute for conducting financial analysis, which can often be thought as difficult to conduct, but which can be aided by technology such as automated bank record scanning systems or intelligent link software.

It was mentioned that some techniques are resource intensive and in that regard it is important to undertake their use with a defined purpose, knowing exactly what evidence can be produced and how that evidence can go towards proving the case. Finally, the importance of good co-ordination between law enforcement and prosecutors was stressed so as to avoid possible defence strategies, the unlawful obtaining or retaining of evidence, and collection of information belonging to non-suspects.

Finally, as noted in the FATF's 2012 financial investigations guidance, ongoing law enforcement collaboration and exchange of information with FIUs should play an important role in investigations. This can lead to the FIU providing additional financial intelligence to the investigative team, thus contributing to a fuller picture of the financial modus operandi of an organised criminal group. In doing so, care should be taken to ensure that any action by the FIU does not unduly jeopardise or hinder the criminal investigation.


Agreement

Terrorist Financing:

Investigations, prosecutions, and convictions

Investigating and prosecuting terrorist financing (TF) offences presents a distinct set of challenges for jurisdictions. TF cases often involve classified intelligence, can span multiple jurisdictions, and require rapid responses from the investigative and prosecutorial authorities. The authorities may also need to find a balance between gathering sufficient evidence to obtain TF convictions and disrupting the activity to prevent a terrorist act from occurring. As an initial matter, participants in the workshops noted that TF investigations can be initiated in many ways, and that TF investigations do not simply pre-date or post-date a terrorist act or require a link to an attack. Donor networks operate constantly and shift methods; states sponsor and fund terrorist organisations; terrorist organisations generate revenue from the territory they control; and individuals may be inspired to provide material, resources, or other support, including themselves.

This section draws from FATF and FSRB members' experiences in conducting TF investigations and prosecutions. It identifies common challenges as well as good practices from jurisdictions that have successfully dealt with TF cases.

Results of the FATF/FSRB Mutual Evaluations – Immediate Outcome 9

Immediate Outcome 9

Immediate Outcome 9 of the FATF Methodology measures the extent to which TF offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions. In line with the FATF Methodology, jurisdictions' effectiveness is determined by considering five core issues[12]:

- The extent to which different types of TF activity are prosecuted and offenders are convicted, and whether this is consistent with the country's risk profile.
- How well cases of TF are identified and investigated.
- Integration of the investigation of TF with national counter-terrorism strategies and investigations.
- The effectiveness of sanctions or measures applied against natural and legal persons convicted of TF offences.
- Whether other criminal justice, regulatory or other measures to disrupt TF activities where it is not practicable to secure a TF conviction.

The review of MERs highlighted the nearly direct correlation between the jurisdiction's understanding of TF risk and its level of effectiveness under IO 9. This illustrates the importance of understanding TF risks: for example, whether the country experiences activity such as collecting, transferring or using funds intended for terrorist purposes.

12. The full text of the core issues can be found in the FATF Methodology (http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf)

Table 2. Effectiveness results under Immediate Outcome 9

	Number	High		Substantial		Moderate		Low	
		Number	%	Number	%	Number	%	Number	%
FATF assessments	17	1	6%	11	65%	4	23%	1	6%
FSRB assessments	33	0	0%	7	21%	14	43%	12	36%
All assessments	50	1	2%	18	36%	18	40%	13	26%

Note: Results from the 4th Round of Mutual Evaluations as at 15 May 2018
Source: Published assessment reports and the consolidated assessment ratings, available on www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

Relevant data from the mutual evaluations

The majority of the reviewed jurisdictions had not prosecuted TF offences or obtained TF convictions at the time of their mutual evaluation. Only 14 (29%) of the reviewed jurisdictions had prosecuted any TF offences, and only 10 (20%) had obtained convictions. For a large majority of countries that reported charging or convicting for TF, the numbers are in the single figures and sanctions were often not considered effective, proportionate or dissuasive.

To some extent, these numbers highlight the challenges that countries are facing in investigating and prosecuting TF offences. However, they do not necessarily fully reflect the rate of TF prosecutions and convictions because:

- Many jurisdictions had prosecuted TF conduct by using alternative offences in addition to, or instead of TF charges. These included association with a terrorist organisation or aiding and abetting a terrorist act.
- In some cases, the TF charges formed a part of a wider terrorism case, but these cases did not contribute to the total number of TF prosecutions in the country.
- In some cases, the low numbers were simply indicative of the lower TF risk profile of certain jurisdictions.

Technical compliance

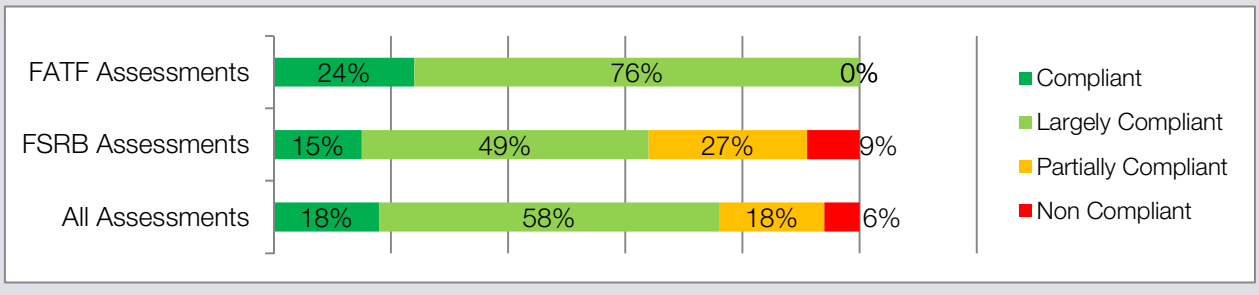
A foundational aspect for effective investigation and prosecution of TF activity is the criminalisation of TF as a separate offence.

FATF Recommendation 5 (R.5) provides measures to assist countries in fulfilling the legal requirements of the International Convention for the Suppression of the Financing of Terrorism (1999) (The Terrorist Financing Convention), and, indeed, contains elements which deliberately go beyond the existing international legal obligations.

The level of compliance with R.5 was reasonably high across the assessed jurisdictions, particularly after the FATF's global review of compliance with recommendations 5 and 6 (relating to targeted financing sanctions) after the terrorist attacks in Paris in November 2015. Globally, 76% of the reviewed jurisdictions were either compliant or largely compliant with the R.5, to include all the FATF members and 64% of the FSRB members. Common deficiencies included the lack of criminalisation of the funding of an individual terrorist without a link to a terrorist act and the low level of available sanctions. Other deficiencies range from exemptions to the definition of terrorism or a list of terrorist acts which is too narrow in scope and which, in turns, narrows the scope of the TF offense.

Figure 5 shows the technical compliance ratings on R.5 from the 50 MERs conducted to date.

Figure 5. Technical Compliance Recommendation 5 (Terrorist financing offence)



Note: Results from the 4th Round of Mutual Evaluations as at 15 May 2018
Source: Published assessment reports and the consolidated assessment ratings, available on www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

Legislative basis to investigate and prosecute TF

Comprehensive criminalisation of TF is directly related to the jurisdiction's ability to investigate and prosecute TF effectively. For example, the lack of criminalising the financing of an individual terrorist without a link to a terrorist act can prevent a jurisdiction from prosecuting the financing of travel of a foreign terrorist fighter.

The FATF has focused on improving the global level of criminalisation of TF in recent years. For example, in 2015 the FATF launched a fact-finding initiative to determine whether 194 jurisdictions around the world had implemented measures to cut off terrorism-related financial flows, including adequately criminalising TF[13]. The results of the initiative prompted the FATF to design a follow-up process to ensure countries were making the required changes. In 2016, the FATF also issued Guidance on the criminalisation of terrorist financing – a guidance paper aiming to assist countries in implementing the requirements of R.5[14].

In the various workshops, practitioners noted that the key challenges related to the criminalisation of TF and self-financing and the difficulties in defining terms such as "terrorism", "terrorist" or "terrorist organisation" in legislation. In many jurisdictions TF offences are also relatively new compared to money-laundering offences, some of which have been set in law for decades. The good practices discussed and identified in the workshops included:

- Drafting the offence to be as broad as possible: for example, structuring the offence in a way that the suspect's intent to finance specific terrorist acts does not need to be proved[15].

- Involving prosecutors in the drafting of the offence to ensure the provisions are workable in practice.

13. The FATF's report to G20 leaders with the results of the review can be found at www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-financing-actions-taken-by-FATF.pdf

14. www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Criminalising-Terrorist-Financing.pdf

15. For example, the MER of the United States notes that the offence of knowingly providing material support or resources to a designated Foreign Terrorist Organisation is the most often charged TF offence. Specialist prosecutors confirmed that this is because this offence allows for effective TF prosecution and conviction without needing to prove any specific intent on behalf of the defendant to fund terrorist activity/acts.

Core elements of effectiveness

Parallel financial investigations

Practically speaking, counterterrorism and TF investigations are often linked (however, it is important to note that they do not need to be). To ensure that all the relevant actors in the network are discovered, it is important to conduct systematic parallel financial investigations in every terrorism-related case. The investigation can either be a standalone TF investigation, or where applicable, form a part of a wider terrorism investigation.

Many jurisdictions face challenges with the investigative capacity and capability to conduct parallel financial investigations. Experts at the workshops reported that often, financial investigations are not pursued if the underlying terrorist activity appears to be primarily self-funded or if the sums involved are very small.

The workshop identified good practices, which include ensuring that a TF investigation can be launched without an underlying terrorism case, and that the TF investigation can continue even where the linked terrorism investigation has already been concluded. Another useful practice is to issue manuals and procedures for identifying and investigating TF.

In addition, the FATF Guidance on the criminalisation of terrorist financing has a specific section on terrorist financing investigations, providing further information on good practices. For example, it notes that financial investigations should be viewed not only from a prosecution-oriented perspective, but also from an intelligence standpoint.

Evidence

Many of the challenges in TF cases relate to the availability and admissibility of evidence. Some particular challenges related to proving the elements of the TF offence include:

- Proving mens rea, i.e. that the defendant intended or knew that the funds were to be used by a terrorist, a terrorist group, or for a terrorist act – especially where the defence claims the funds were meant for personal expenses such as rent or food or charitable purposes.

- Proving that the recipient of the funds or assets is a terrorist or a terrorist organisation, especially where they have not been designated by the United Nations Security Council or national authorities as such or before a terrorist attack is planned or committed.

- Proving TF when the funds are sent oversees or may not ever actually be used to finance an attack.

TF cases may be initiated by or rely on classified pieces of intelligence. The defendant may also know from personal experience information that is classified and thus pose a disclosure risk to the national authorities. There are particular challenges related to "converting" classified intelligence into admissible evidence:

- The prosecution may have to find a way to recreate or corroborate information that is otherwise only found in classified material.

- The prosecution may find itself in a position where it would have to reveal secret information if it intended to prosecute, and therefore, it may decline to pursue the charges or dismiss the case.
- Sentences may be lower as not all elements of the TF activity can be taken into account due to the inadmissibility of evidence.
- Additional, burdensome steps may need to be taken to keep the sources and methods of intelligence gathering confidential.
- Different levels of intelligence may be accessible to different people – such as the intelligence service, police, or the prosecutors – which can complicate co-operation among agencies.

While gathering and using evidence is one of the most challenging areas in TF prosecutions, there are also some good practices in the area:

- Having legislation or judicial procedures that specifically deal with the use or introduction of classified material or intelligence (e.g. laws or rules may permit judges and/or defence counsel to review information, redactions may be made, information can be "declassified" by the state, etc.).
- Involving the prosecutor at an early stage to determine what pieces of intelligence may be admissible as evidence, or what steps would need to be taken for it to be admissible.
- Steering the investigation in a way that the confidential intelligence is supplemented or supplanted with admissible evidence, such as financial records or records of communications obtained through judicial authorisation.
- Developing jurisprudence to enable the use of circumstantial and indirect evidence to prove knowledge and intent.
- Using the defendant's own words and activities, such as on social media, to help prove intent or finding witnesses who can testify to the defendant's behaviour or beliefs and changes thereto.
- Implementing all UN-required terrorism and related designations and establishing a system of domestic designations to help prove that an individual is a terrorist or an organisation is a terrorist organisation, or developing jurisprudence which gives weight to foreign designations[16].
- Using the 24/7 electronic evidence system under Article 35 of the Budapest Convention to obtain and offer immediate assistance concerning the collection of electronic evidence. [17]
- Having a designated special court to deal with terrorism and terrorist financing cases that often include classified information.
- Using administrative powers to freeze or seize assets based on confidential intelligence that could not be used to support a prosecution.

16. In particular, many workshop participants noted that they monitored closely the Specially Designated Nationals and Blocked Persons List of the U.S. Office of Foreign Assets Control (OFAC).

17. Article 35 of the Budapest Convention on Cybercrime (24/7 Network) states that Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Powers and techniques

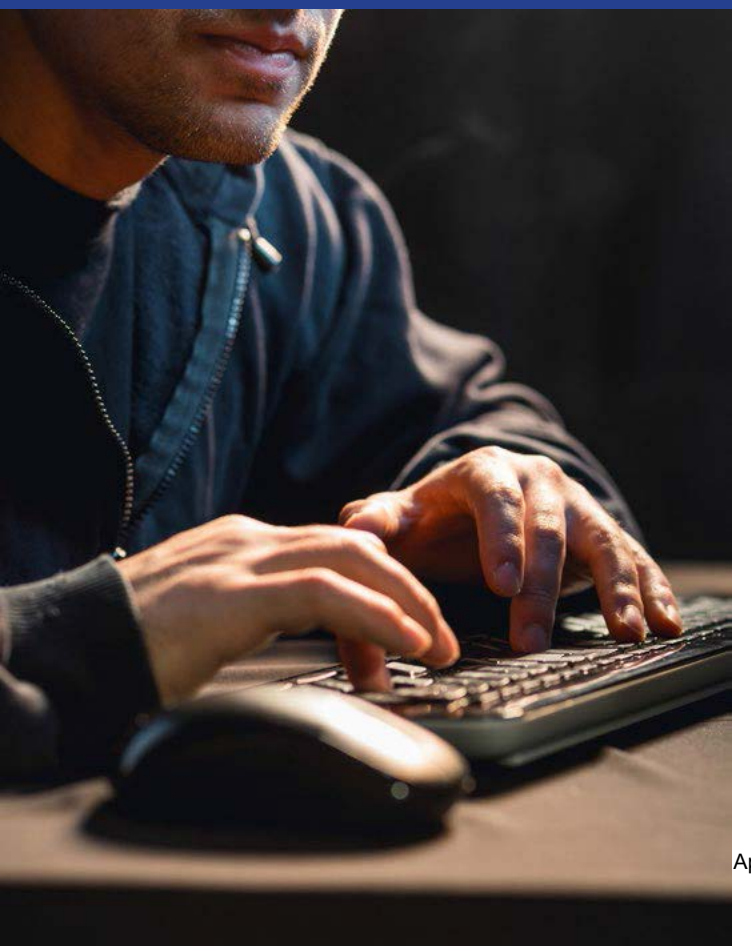
Special investigative techniques, such as the use of wiretaps, monitoring internet use, intercepting social media communications, or using confidential human sources (informants) or undercover agents, are often important sources of evidence in TF cases. It is imperative that competent authorities have a wide variety of techniques available to them.

In terms of confidential informants, jurisdictions have experienced challenges in trying to protect the identity of the informant. Further, it is often necessary to change the sources and find new informants.

Social media can often be an important source of evidence in TF cases. There can, however, be challenges in obtaining evidence from social media platforms: intercepting communications may require a pre-authorisation from the court or it can be challenging to obtain social media content from overseas. Social media content may also not be admissible as evidence.

Some good practices related to using social media content as evidence include:

- LEAs might create profiles on social media platforms, enter into closed groups, and communicate with suspects to produce direct evidence (i.e. screen shots)
- Using the law enforcement agent who participated in the communications with suspects as a witness.
- Communicating with the social media platforms and their law enforcement sections directly. Early engagement – even before a TF investigation is opened – can be useful to find out what type of information or evidence is available and how it can be obtained. One example is to use preservation orders to ensure the social media content is not routinely deleted while the investigation is ongoing.



Prevention & Disruption

TF cases are often time-sensitive and there is a difficult balance between allowing the TF activity to continue to gather further evidence and disrupting the activity to prevent a possible terrorist attack. Many jurisdictions have opted for disrupting the activities early instead of pursuing a TF prosecution. This is often done in the interest of public safety, or where it has been clear that the available evidence would not be able to support a TF prosecution.

The need to disrupt TF activities is also reflected in the FATF Methodology. In addition to prosecuting TF offences, IO 9 takes into account jurisdictions' use of the other criminal justice, regulatory or other measures to disrupt TF activities where it is not practicable to secure a TF conviction.

It should be noted that disrupting the terrorist or supporting network fully can be very challenging. This is particularly true in cases where the identity of the recipient is not known, and the funds have been sent to an unstable conflict zone. Authorities may be able to cut off one part of the network but other financiers are able to continue their activity and keep transferring funds to the same recipient.

Common methods to disrupt TF activity identified in the workshops include:

- Targeted financial sanctions to freeze the funds of designated terrorists and terrorist organisations – the burden of proof to designate is often lower than to prosecute, yet the desired disruptive impact can often be reached [18].
- Non-conviction-based asset seizure and confiscation.
- Withdrawal of passports, extradition, and deportation; although such measures should be coordinated or coupled with advanced notice to the country where the suspect is sent.
- Taking a broader view, the workshop participants also highlighted the importance of de-radicalisation efforts in jurisdictions both to prevent TF activity and prevent recidivism.

18. See 2013 FATF International Best Practices on Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6) which outlines the importance of an effective freezing regime.

Investigating and prosecuting terrorism offences vs. TF offences

It is a common practice in many jurisdictions to prosecute alternative offences such as association with a terrorist organisation, money laundering or fraud instead of prosecuting TF offences. Common justifications for doing so included: the evidentiary thresholds under other legislation can be easier to meet or the prosecutors may be more familiar with other legislation. In some cases, there may be an urgent need to disrupt the activity, and the prosecutor has enough evidence already to charge another offence instead of TF.

Discussions during workshops highlighted that prosecuting TF cases can often be labour-intensive and time-consuming and add to the workload of the prosecutors without necessarily increasing the sentence. In some cases, TF prosecutions are not pursued because the suspect has been self-funding their terrorist activities and a terrorism prosecution is pursued instead. Still, prosecuting non-terrorism related offences can lead to lower sentences because these other offences do not fully reflect the gravity of terrorism-related charges. Some experts reported that, in fact, the inclusion of TF charges as part of a larger prosecution might be the only charge of conviction if the direct participation of the accused in terrorist acts is not proven.

However, despite the challenges, seeking TF prosecutions is important, especially where there is any suspicion of TF activity, for example, based on a suspicious transaction report or information provided from another country. Investigating and eventually prosecuting TF offences can lead to discovering and disrupting a wider network financing the same terrorist organisation. It may also uncover criminal activity that generated funds used for TF or the laundering of assets derived from TF. Finally, although TF can occur in formal financial systems and through informal channels, and may be accomplished in comparatively small amounts, the ultimate impact of the financing can be hugely detrimental. While the political will to prosecute persons that commit acts of terrorism is strong, those who financially facilitate and support terrorism are just as critical to the terrorist ecosystem as those who carry out heinous acts. Prosecuting TF was also recognised for its deterrence value, as national financial systems can be vulnerable origin or transit points for TF even if terrorism does not occur within particular countries' borders.

Confiscation:

freezing, seizing, and recovering assets

Tracing, freezing and confiscating the proceeds and instrumentalities of crime is fundamental to the effectiveness of measures to combat money laundering and terrorist financing. Serious crime generates a vast amount of proceeds every year. Some of the main reasons that criminals launder their proceeds are to prevent competent authorities from detecting their illegal conduct, prevent authorities from depriving them of their ill-gotten gains, and to use these ill-gotten gains to promote ongoing criminal activity. Confiscation strangles the operational budgets of criminal organisations, ensures that crime does not pay, and recovers value which can be used to compensate the victims of crime.

This section draws from FATF and FSRB members' experiences in identifying and tracing, seizing and freezing, and ultimately, confiscating and recovering, criminal assets. It identifies common challenges and good practices from FATF and FSRB jurisdictions.

Results of the FATF/FSRB Mutual Evaluations – IO 8 & R.4/R. 38

Immediate Outcome 8 of the FATF Methodology measures effectiveness of the confiscation regime - the extent to which proceeds and instrumentalities of crime are confiscated. This can be contrasted with the legislative and other measures that are required pursuant to Recommendation 4 (domestic confiscation and provisional measures) and Recommendation 38 (mutual legal assistance for freezing and confiscation), which set out several elements that underpin for an effective confiscation (or forfeiture) regime.

These ratings demonstrate that, to date, the level of implementation of an effective confiscation regime among the assessed countries is modest at best. According to all assessments, almost three-quarters of jurisdictions are not succeeding in this area. Although the Methodology for the current round of assessments dates from 2013, the concept that criminals should be deprived of their proceeds is one that has been a core element of the FATF Recommendations since the original 1990 Recommendations.

In line with the FATF Methodology, jurisdictions' effectiveness in depriving criminals of the proceeds and instrumentalities of ML, TF, and predicate offences (or their equivalent value), is determined by considering five core issues:

- Whether confiscation is a policy objective in the country.
- If the country is confiscating proceeds/ instrumentalities/equivalent value related to both domestic and foreign predicate offenses and where assets are located overseas.
- Whether falsely or non-declared currency or bearer negotiable instruments moved across the border are confiscated.
- How well confiscation results align with ML/TF risks and national AML/CFT priorities.

Many of the assessments reviewed cited deficiencies in the way that the jurisdiction addressed these following issues:

- Confiscation was only occasionally laid out as a policy priority, and this was mostly found in jurisdictions having specialised agencies or units dedicated to confiscations.
- Actions taken on false or non-declaration of physical cross-border transportation of cash and bearer negotiable instruments were limited and inconsistent. Not many cases were linked to ML/TF and many countries applied a small fine to these cases. It also appears that in many cases the cash declarations or disclosures are not used to their fullest extent as part of the AML/CFT system, due often to technical limitations.

Table 3. Effectiveness results under Immediate Outcome 8

	Number	High		Substantial		Moderate		Low	
		Number	%	Number	%	Number	%	Number	%
FATF assessments	17	1	6%	4	23%	11	65%	1	6%
FSRB assessments	33	1	3%	5	15%	9	27%	18	55%
All assessments	50	2	4%	9	18%	20	40%	19	38%

Note: Results from the 4th Round of Mutual Evaluations as at 15 May 2018
Source: Published assessment reports and the consolidated assessment ratings, available on www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

- With respect to the linkage between confiscation and the risks faced by jurisdictions, MERs frequently noted that the results obtained were not in line with the risks faced, whether as regards the amount confiscated, or the nature of the results (e.g. limited confiscation in relation to predicates generating the most proceeds of foreign predicate offences).

- A misalignment between amounts subject to provisional measures (freezing, seizing) and amounts confiscated, or between amounts *ordered* confiscated and *actually* recovered.

Overall, too small an amount of money was confiscated considering the risks and contexts of the country or a lack of focus on parallel financial investigations such that assets which could be confiscated were not identified or traced.

Although both qualitative and quantitative information is important in determining effectiveness under IO 8, the amount of criminal proceeds and instrumentalities that are ultimately confiscated and recovered by the government (or where there is restitution to victims), is an important overall element. In an ideal world, competent authorities are able to identify and trace a significant proportion of the proceeds of crime located or generated within the jurisdiction, freeze or seize those assets, then confiscate and recover them. This is a significant challenge. Experts referred to a number of complications in the workshops, most often the inability to follow the money trail; the criminals' use of webs of companies, accounts, and nominees to hold assets; or the movement of assets abroad, potentially to non-cooperative countries.

Reliable or comprehensive data and statistics on confiscation, such as the number of cases and the value of the assets that were frozen, confiscated, and recovered, is variable or lacking across the MER reports. Furthermore, that data is not always consistent across agencies within one country, and thus is difficult to interpret. Similarly, there are few estimates of the size of the criminal economy for jurisdictions, and any such estimates that do exist have to be treated very cautiously, thus making it more challenging to determine how well a country is doing in terms of the amount it confiscates. The lack of data also often makes it hard to identify the nature of the deficiencies or weaknesses that lead to results that defy expectations. Qualitative information, such as case examples, is presented across the MERs as well.

In terms of the amounts ordered to be confiscated, there are two FATF members that confiscate noticeably larger amounts (i.e. reaching into the low billions of USD/EUR annually). The amounts confiscated by other countries range from minimal amounts (less than a million) to 100-200 million. As regards the numbers of cases, this varies also from 0-20 cases a year (annual average) to several thousand. With respect to the number of cases and the value of the amounts confiscated, there can often be significant variations between jurisdictions (even ones of a similar size in terms of population or economy, legal systems etc.), with the reasons for this being less apparent.

Technical Compliance

There appears to be a large degree of technical compliance, with all FATF members being Compliant (C) or Largely Compliant (LC) on both Recommendation 4 and Recommendation 38, to date. For FSRBs members, the results show more than 80% are C or LC on R.4 and 70% C or LC on recommendation 38.

The most frequently cited deficiencies are:

(a) Recommendation 4 – inadequate mechanisms to manage property, lack of equivalent value confiscation, gaps regarding instrumentalities and limitations in the range of offences where confiscation can be pursued.

(b) Recommendation 38 – similar deficiencies as for R.4, inability to enforce non-conviction based orders, lack of mechanisms to share confiscated assets or to co-ordinate actions with other countries.

In general it appears that though there are a mix of deficiencies under both R.4 and 38, these are relatively minor, taking into account the requirements laid out in the FATF Standards.

Figure 6. Technical Compliance Recommendation 4 (Confiscation and provisional measures)

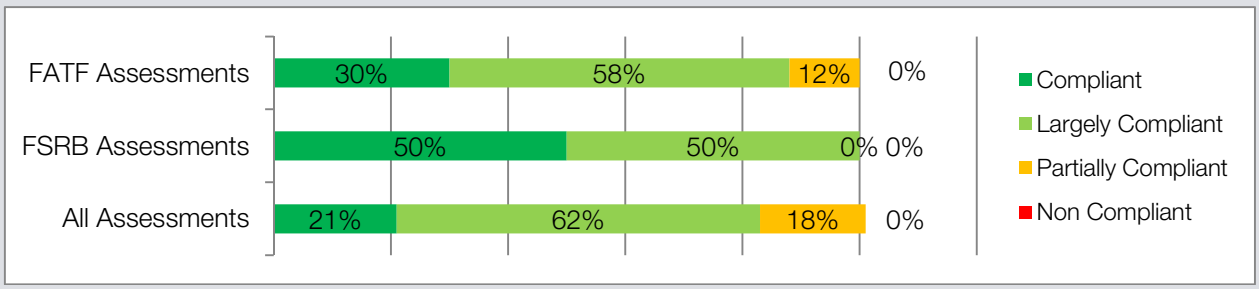
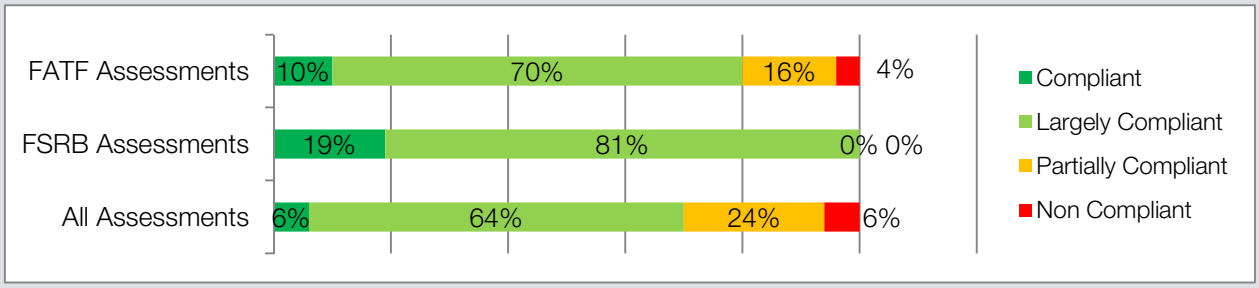


Figure 7. Technical Compliance Recommendation 38 (MLA: freezing and confiscation)



Note Figures 6 and 7: Results from the 4th Round of Mutual Evaluations as at 15 May 2018
Source Figures 6 and 7: Published assessment reports and the consolidated assessment ratings, available on www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

Core elements of effectiveness

The effectiveness of any confiscation regime (all aspects thereof) is based on a number of factors, which include the underpinning laws and regulations that provide a full range of powers, the institutional framework and competent authorities that have responsibility for taking action, and the mechanisms, processes and tools that are used. Some practices particularly useful and effective practices for asset confiscation are:

- Ensuring that criminal asset confiscation is a policy priority, with a linked strategy that sets out how all relevant authorities can work to achieve the objectives/goals that are set.

- The creation of multidisciplinary agencies/ units that focus on asset confiscation, or at a minimum having expert staff that is dedicated to this role within larger agencies or public prosecution services. There is a need for expert lawyers, investigators, forensic accountants, financial analysts, and increasingly, IT experts.

- A framework to manage or oversee the management of frozen, seized, and confiscated property[19], including by competent authorities that are freestanding or part of an LEA, and, as needed, the ability to hire outside vendors or contractors for complex assets. Judges were not seen by participants in the workshops as generally able to manage seized assets or dispose of them effectively in addition to their other duties.

- Unlike other aspects of the criminal justice system, confiscation can result in revenue for governments; this provides an opportunity for confiscation offices to be self-sustaining.

- Working in co-operation with international partners was seen as a key ingredient of success, especially the early outreach seeking the imposition of provisional measures against assets subject to confiscation. Furthermore, the legal ability to domesticate or enforce foreign confiscation orders was regarded positively by practitioners.

Financial investigation and Asset tracing

As noted above, parallel financial investigations should be a routine part of any investigation into crimes that generate proceeds or where money or assets are being used for criminal or terrorist purposes. If effective action is to be taken against the proceeds of crime, it is critical that investigators can, in a timely way, identify all parties (whether natural or legal persons) involved in or linked to the criminal activity and/ or the criminal, as well as identify all assets (and the persons holding or controlling those assets) which might be subject to confiscation or be an asset that could be used to meet a value-based confiscation judgment. As the practitioners in the workshops emphasised, where possible, as much financial investigation as possible of the criminal should occur before the arrest or before the point in time at which the criminal becomes aware he is being investigated, to include the tracing of assets and liabilities, net worth analysis, and understanding of income and expenditures, as appropriate. This will allow more effective results in terms of freezing/seizing. If there is more than one agency or body involved in the criminal investigation and the confiscation, then this requires a well-coordinated approach. It could also be effective to employ a task-force approach for certain types of investigations

Investigative powers - It is essential that authorities have a full set of investigative powers available to them to investigate the financial activity of criminals.

- At the most basic level, participants in the workshops mentioned this means that law enforcement/prosecutors should have the power issue to production orders or subpoenas (commonly used to require

19. FATF Best Practices Paper Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery.

financial institutions to produce financial records) or to conduct searches that allow documents, assets, or other items to be seized as evidence or even in view of confiscation. Such powers should have a purpose that extends beyond the traditional gathering of evidence for a criminal offence to the tracing and/or analysis of criminal proceeds.

- It is important that these powers, if used at a pre-arrest stage, are linked to provisions that prevent third parties from tipping-off the criminals or the owners of the assets. Experts noted that such authorities would normally be obtainable on relatively lower factual showing or such as "reasonable grounds to suspect".

- Some of the other techniques and powers set out in R.31 such as undercover operations, intercepting communications, and accessing IT systems could also be useful for asset tracing.

- One power that exists in some common law jurisdictions and which was noted as useful in certain cases is a monitoring order power, whereby a court order requires persons (usually financial institutions) to report any transactions with the suspected criminals for a future period. This in effect provides real-time financial intelligence.

- With respect to accessing records, investigative authorities may use judicial processes to request a warrant to compel a search or seizure, or a subpoena to require testimony be given or records produced.

- The attendance of witnesses and the production of records may be required from any place or in any territory or other place subject to the jurisdiction where the investigation is taking place. In some cases, the prosecutor may also apply to a court for the issue of a search warrant to be executed upon a legal person. For example, an agent of the court may "serve" the subpoena upon the recipient (e.g. bank, title company, registered agent, trustee, etc.).

- Standard investigative techniques can also be used to overcome investigative difficulties or impediments to understanding trusts, which may be used to hold or conceal criminal assets. Once the trustee is located, law enforcement may use compulsory measures to obtain records and identify those who exercise control over the trust such as a protector or a person with a general power of appointment. Competent authorities are able to "follow the money" to the non-trustee individual (if any) who ultimately benefits from the trust or similar structure.

- Various tools were cited in the workshops as useful in "following the money," such as using records to trace funds through numerous accounts or institutions, developing informants or key witnesses; executing search warrants to obtain relevant documents including financial records and business records; cross-referencing business or travel records; the power to ask financial institutions to confirm whether they hold an account in a particular name; and utilising special investigative techniques such as electronic surveillance or monitored undercover operations to pierce the veil of legal entities to their true owners.

Timely access to databases and other sources of information regarding assets – it is often essential to obtain information about a criminal's assets very quickly, and an important issue in this regard is the capacity to search against a database(s) for different types of assets to know whether assets that may be subject to confiscation are held by the criminal, an associate or third party. For example all police forces would have access to registers of motor vehicles. There is currently also considerable debate about timely access to beneficial ownership records for legal

persons and arrangements, with an increasing amount of information being held within company registries.

- Many countries have one or more government registries for real property, and some countries maintain a central database of all bank accounts held in that country or have some capacity to query all reporting entities for relationships or transactions with specified individuals or entities [20]. Such databases or any rapidly accessible record keeping system showing assets and owner for important types of assets appears to be a very useful tool for authorities to trace assets in a timely way. However, any such systems should have measures to verify the accuracy and authenticity of the information it holds.

- Direct or indirect access to taxation records it also very important as a way to cross-check what a defendant or associate declared as legitimate income, assets etc. It is important that all databases are searchable in an effective way.

20. In the European Union the Fifth Anti-Money Laundering Directive requires EU members to create a database of all bank accounts held in the country.

Seizing/freezing

Attendees at the workshops noted that it was essential that competent authorities are able to take action to freeze or seize assets that may ultimately be subject to confiscation. Depending on national law or procedure, or the facts of the case, this may entail measures affecting all assets of a defendant (e.g. a global prohibition on dealing with assets owned or controlled by the defendant, even if held by third parties) or only specifically enumerated assets (often those that are directly traceable to crime). Also, depending on the legal system, the power to order restraint or seizure may rest only with a court or judge, or the prosecutor or investigating judge may have certain powers. Important elements in an effective regime include:

- **Ability to take timely action** - As noted, it is important that there is the legal possibility and practical mechanism in place to freeze/seize most or all relevant assets before or at the same time as arrest. In jurisdictions where investigations can be conducted covertly, the seizures might be timed to the moment when the investigation becomes overt. Preferably, freezing and seizing this can occur after assets have been traced and some amount of financial analysis carried out, but this may not always be possible. Participants at the workshops agreed that the ability to act on an ex parte basis, without notice to the suspect, even for just a short period, was helpful to ensure the efficacy of provisional measures so that the suspect did not have a chance to move or dissipate assets. Practitioners agreed that an evidentiary requirement on the government to prove a risk of dissipation before it is possible to obtain an order was burdensome. Such a requirement is often difficult to prove in practice and would negatively impact the ability to freeze assets. With respect to practical mechanisms, action can be taken more swiftly if prosecutors are involved in the case at an early stage and either have appropriate powers themselves or can apply rapidly for a court order. It is also helpful for courts to have procedures permitting emergency or urgent applications.

- **Evidence and burden of proof** – Experts expressed the view that the evidentiary requirements and burden of proof should not be unduly onerous at the freezing/seizing stage of proceedings. Authorities were comfortable with standards such as reasonable grounds to suspect the defendant has assets derived from crime or probable cause to believe that there is property that would be subject to confiscation in the event of a conviction.

- **Third party property** – Frequently, the criminals that commit the predicate offences will seek to launder the proceeds and place the proceeds in the hands of third parties (family, associates, or legal persons or arrangements) that were not directly involved in the crimes. Prosecutors need to be able to trace and have the power to freeze such property, including in cases where equivalent value confiscation that will be sought because the proceeds are unavailable or have been spent. Countries

use different legal powers in this regard, and three mechanisms that were cited were: (a) directly tracing the criminal proceeds through any transactions/ transfers into the property that is to be restrained; (b) producing evidence to show that the third party received a gift of property from the defendant or was not a bona fide purchaser of the asset; and (c) showing that the defendant has effective control of the property even if it is held in the name of a nominee. Of course, the rights of bona fide third parties should be appropriately protected.

- **Extent and nature of the provisional order** – Whichever authority is competent to issue preliminary orders should ensure that property will be preserved and available to satisfy any confiscation order that is subsequently made. Practitioners agreed that the scope of the order should be broad, and, if possible, include income derived from property that can be confiscated and equivalent value or substitute assets. The nature of proceedings giving rise to the order will vary. Depending on the legal system, they could be in rem or in personam, orders could be made against specific assets or all assets of a defendant, and they may have extraterritorial reach. According to the FATF Standards, courts or other authorities should be able to issue provisional measures covering assets located abroad, but of course mutual legal assistance would be required to give effect to the order in the foreign country. Practically, property could be: (a) restrained in place (e.g. a financial institution may be ordered to simply freeze accounts) (b) subjected to conditions (e.g. a prohibition on the sale of real property may be ordered which does not evict occupants before conviction), or (c) seized and taken under the control of a law enforcement, the court, or other authorised body, if there is a concern that the nature of the property might lead to it being dissipated or hidden regardless of the court order, such as with cash, personal property, vessels, vehicles, or other movable assets.

- **Ancillary powers/orders** – Following the legal developments that have occurred around Mareva injunctions in a civil law context, many countries have also provided prosecutors with additional powers that can assist in ensuring that assets are located, effectively frozen and then available to meet any confiscation order. One such power is the possibility for a court to order that a defendant make a sworn declaration about all his assets. If obtained at an early stage of proceedings this can potentially provide useful additional information regarding assets, and place an onus on a defendant to be truthful about all the assets he owns or controls, or run the risk later of being shown to have perjured himself. Another option, available in some jurisdictions is that the government has the power to ask the defendant questions about things such as finances which the defendant is required to answer. Such a power must be carefully used, and should not negatively impact the defendant's basic right to not

be forced to incriminate himself, i.e. the answers could not be forced and also used as evidence of a criminal offence. A third mechanism that is used is for the defendant to agree, or for the court to order, that a defendant repatriate assets that are located in another jurisdiction.

- **FIU power to freeze** – A number of FIUs have the power to temporarily place a hold on (freeze) assets involved in suspicious transactions. Another similar mechanism is a "no consent" order whereby the FIU refuses to consent to a reporting entity's processing of a suspicious transaction. Such administrative holds can be useful to expeditiously prevent monies from being transferred abroad, for example in fraud cases, where it can then be difficult to recover them. Freezes may only be available for certain types of transactions/assets and they are temporary—some lasting a matter of hours or days—but they give the prosecution sufficient time to gather evidence to seek stronger judicial orders.

Confiscation/forfeiture

Consistent with Recommendation 4, and various international Conventions, countries should have a full range of powers to confiscate (a) property laundered; (b) proceeds from, or instrumentalities used or intended for use in ML or predicate offenses; (c) proceeds or instrumentalities linked to TF; and (d) property of corresponding value. These are long-standing norms, and as noted above, most countries have the basic authorities in place in their laws. Surprisingly, quite a number of countries do not have adequate powers to ensure confiscation of equivalent value. Experts noted that it is important that the defendant is not incentivised to benefit from his criminality by spending proceeds first while retaining other property that was legally acquired.

Evidence and standard of proof - The nature of the evidentiary requirements and the burden of proof varies according to the type of confiscation (criminal, civil, administrative) and the jurisdiction and its legal system. The issue is not one that is discussed in many MERs, but is important in terms of the ultimate effectiveness of the regime.

- In all jurisdictions, there are laws allowing confiscation of proceeds and instrumentalities post-conviction, in particular for the offences of conviction. This is often viewed as part of the criminal sentence, and the procedural rules that apply for that purpose will also apply to confiscation; however, some jurisdictions apply a lesser standard of proof than the normal criminal standard (beyond reasonable doubt) to confiscation.

- Experts surmised that it could be effective if the burden were the normal civil standard of balance of probabilities or something similar.

- One issue where broader sentencing considerations are relevant relates to confiscation of instrumentalities, and the need to ensure that the nature and value of the property being confiscated is somehow proportionate to the scale of the criminality involved.

- Workshop attendees also considered the issue of how the court will take into account the proceeds gained in circumstances where the prosecution does not include all possible charges, but a representative set, such as when additional offences are believed to have been committed, but it would not be cost-efficient to proceed with all charges. The benefits from this unindicted conduct might also be taken into account for confiscation purposes.

Non-conviction based (NCB) confiscation – An increasing number of countries have adopted NCB confiscation regimes in addition to their conviction-based laws. In such proceedings—which are sometimes also referred to as civil confiscation, civil forfeiture, or extinction of dominion—assets can be declared forfeited to the state without the condition precedent that the defendant has been convicted of a crime. The nature of the proceedings is in rem (against the asset itself rather than against a person).

- Some participants described situations where NCB is available in limited circumstances, such as when the accused has died or absconded, while other workshop participants discussed fuller NCB regimes in which the state proceeds on the legal fiction that the property is "standing in" for the defendant and is forfeitable due to its involvement in crime is separate from any criminal proceeding and the standard of proof is usually the same as or similar to the civil standard (e.g. the state must show by a preponderance of the evidence or on balance of probabilities that the property constitutes the proceeds or an instrumentality of crime).

- In some jurisdictions, Ireland, for example, NCB is the main mechanism used to confiscate criminal proceeds and

instrumentalities and is integrally linked to efforts to combat serious organised crime. Experts noted that the civil confiscation can backstop a criminal prosecution, or even succeed in the event of acquittal.

- A variation on NCB that is used in some jurisdictions is administrative confiscation/ forfeiture or abandonment. This is usually conducted by LEAs and authorised only for certain types of assets, e.g. assets under a certain value or amount or cash that is seized at the border. Assets can be forfeited by administrative notice if uncontested or can be heard in civil proceedings, if contested. The standard of proof in such cases is also lower.

Unexplained wealth orders, unjust enrichment offenses, and burden-shifting provisions – Many countries have introduced additional powers, in both criminal and civil proceedings, that require the government to produce sufficient evidence that a person has assets that cannot be explained by his known legitimate income or legitimately acquired assets, and then place the burden on the defendant to show otherwise.

- Thus, for serious offences such as drug trafficking, where the convicted person does not have known legitimate income to explain his wealth, the prosecution present evidence of net worth or similar accounting evidence.

- There are also certain presumptions that may be triggered by the defendant's "criminal lifestyle" or lack of legitimate income over a period of time where he committed multiple offences. Similarly, unexplained wealth orders, originally conceived as useful in combatting corruption, are being used more broadly to attack criminal assets in civil proceedings. Practitioners at the workshops expressed a desire to learn more about these tools.

Other remedies, including tax and civil restitution – Countries are also adapting their responses to profit-generating crime by looking to use the broadest possible range of powers. Increasingly, using tax collections, penalties, and assessments to recover assets is seen as an avenue of last resort. Tax recovery can be an option when prosecutors lack the evidence to show that the property is criminal proceeds that would meet a civil or criminal burden of proof, but they do have evidence that the defendant has engaged in tax evasion or fraud. While it is preferable to be able to obtain a criminal conviction and also deprive the person of their proceeds, having an option to impose a tax assessment, combined with penalties and interest, can have a similar punitive impact on the defendant in terms of the amount he must disgorge. Proving that assets came from legitimate income may be a much more difficult task for the defendant.

Also, many experts cited restitution as a worthy objective which can, depending on the legal system, be a complimentary power to and work in tandem with confiscation. Many financial crimes have victims, and persons that have been defrauded should receive full restitution, if at all possible. Experts discussed how their legal traditions encompass both restitution and confiscations; depending on the circumstances, it may even be possible to provisionally restrain assets and confiscate them, at which point the state can use the resulting funds to satisfy a restitution order. Some experts said that a combination of confiscation proceedings combined with a civil claim by the victim may accomplish the dual objective of depriving criminals of proceeds while also ensuring victims receive compensation. However, other jurisdictions noted that communication with potential victims is key, as legal claims filed by victims can slow or complicate confiscation where the prosecution intends to ultimately distribute money to victims who can demonstrate their pecuniary losses.

Asset management and recovery

Assessments to date demonstrate that many countries have inadequate legal powers, and lack the institutional frameworks and skill sets needed to effectively manage and/or realise assets that are frozen, seized, or confiscated.

The objective and intention in both Recommendations 4 and 38 is that counties should have mechanisms for managing and disposing of assets domestically and when the confiscation is co-ordinated with another jurisdiction. Assets, depending on the type, require preservation and safeguarding; some require active management; yet others should be sold on an interlocutory basis to maximise the value that can be obtained (or make sure that the defendant's value is maintained if he prevails and the property is not confiscated). Best practices in this area were identified as having dedicated agencies for asset management or else persons who can be charged with such tasks as part of their official duties. Some experts mentioned that they have found it effective to outsource this work to contractors or vendors through government contracting mechanisms, especially when specific expertise is necessary (e.g. to run an ongoing business operation or manage tenants, etc.).

Additionally, in many countries, the value of property realised to satisfy confiscation orders is often considerably less than the value of the property ordered confiscated, or the property has depreciated considerably in value since it was first seized due to lack of maintenance. The issue of asset management and recovery has been looked at previously by FATF and other organisations/bodies, and good practices are detailed, as in the FATF Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for On-going Work on Asset Recovery (2012), or the study by the UNODC Open-ended Intergovernmental Working Group on Asset Recovery (2017)[21].

21. https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2017-August-24-25/V1705952e.pdf

Institutional mechanisms – It is important that there is an effective and cost-efficient mechanism to manage assets and that there are professionals who can appraise and sell assets in a way that maximises the return to the state. In considering which mechanism could be most appropriate, there are numerous considerations such as the likely value and type of assets at issue, whether there are existing bodies that carry out similar functions, cost efficiency of a model, and the need for adequate transparency and accountability. Many different approaches exist, for example:

- In some countries there is no specialised agency or body that has this function, and it is left to general law enforcement or individual judges to manage seized assets, with court services being left responsible for realisation or recovery of assets. Neither entity is usually well equipped with the necessary powers and skills to handle this role for anything other than the most straightforward case.

- Another option which is used is that the Asset Recovery Office in a jurisdiction is not only responsible for asset tracing but also asset management, sometimes with support of other government agencies, as in Belgium and the Netherlands. There are also specialised law enforcement agencies responsible for managing and selling seized assets such as the U.S. Marshals Service, which also handles assets seized by other LEAs.

- There are free-standing government agencies that either solely manage seized/confiscated assets or do that along with other asset management functions.

- Receivers, trustees, or asset managers may be appointed by the court, such as private sector accountants or specialists in bankruptcy or liquidation; some experts cautioned that, fees and charges can sometimes raise issues.

- Additionally, specialised private sector firms have entered the market which can offer asset management and auctioneering services. Some have a particular focus on asset recovery, and many work on a commission basis.

Ultimately, the model or mechanism that is chosen should be cost-effective, with the maximum possible amount being paid into central revenue or specialised asset forfeiture funds, after costs for management and realisation are met. Whether confiscated funds enter the general treasury, budgetary process, or a special fund, practitioners noted at the workshop that it is advisable to use confiscated assets in a responsible, transparent, and accountable way, such as to finance crime-fighting efforts and initiatives or on projects which benefit the general public. Participants recounted the unique and lawful uses for confiscated assets in their jurisdictions and some explained the benefits of having a fund subject to auditing and other controls. Asset sharing with countries whose assistance has made the confiscation or return of assets possible should also be considered where appropriate and is encouraged by the FATF Standards.


auction

International cooperation:
mutual legal assistance, extradition and other cooperation

Appendix H

FATF/MENAFATF/GIABA/GABAC/ESAAMLG Workshop for Judges and Prosecutors
February 2018, Tunis, Tunisia

International co-operation can be critical for the success of ML/TF investigations and prosecutions and also for asset recovery. ML and TF networks are often spread over multiple countries, and foreign jurisdictions may have the missing pieces of information or evidence which facilitate a successful prosecution. Where there are financial or other records located abroad, foreign witnesses whose testimony is critical, or suspects present in another jurisdiction, timely co-operation can be outcome determinative.

The FATF Standards deal with international co-operation in a holistic manner. As a baseline for co-operation, countries should become a party to and fully implement four important multilateral instruments[22]. Countries should also be able to execute extradition requests in relation to ML and TF[23], have mechanisms in place for the rapid provision of a wide range of mutual legal assistance for ML/TF and associated predicate offences investigations, prosecutions and related proceedings; and be able to take expeditious action in response to requests for freezing and confiscation[24]. Finally, Recommendation 40 states that countries should ensure that their competent authorities (to include FIUs and financial supervisors, and LEAs) can rapidly, constructively and effectively provide the widest range of international co-operation and exchange information in relation to ML associated predicate offences and terrorist financing.

22 See Recommendation 36. From an AML/CFT perspective, the most important international agreements are the Vienna Convention (1988), Palermo Convention (2000), Merida Convention (2003), and the TF Convention (1999).

23. See Recommendation 39.

24. See Recommendations 37 and 38.

Other forms of co-operation and information exchange

During the workshops, practitioners emphasised the need for international co-operation that is less formalistic. This may be conducted at an investigator-to-investigator level, among counterpart agencies, or even between agencies that are not direct counterparts (i.e. diagonally). Such informal co-operation—outside of MLA or diplomatic channels—was widely promoted as a beneficial first step to pursue international co-operation. Considering that formal mutual legal assistance is considered to be a slow and resource-intensive mechanism, it was agreed that this could be done more effectively having preliminary direct contacts between counterpart law enforcement agencies and financial intelligence units or from liaison magistrates or law enforcement/judicial attachés posted locally or regionally (agency-to-agency assistance).

As mentioned in the FATF operational guidance for financial investigations, such assistance could lead investigators into a rapid identification of evidence and assets, confirm the assistance needed and even more importantly provide the proper foundation for a formal MLA request (government-to-government assistance). Such contacts also offer an opportunity to learn about the procedures and systems of the foreign jurisdiction and to assess various options for conducting investigations, prosecutions and confiscation.

Workshop attendees also stressed the importance of forming personal connections with foreign colleagues and having close contact through different networks, such as those provided by Interpol or Europol or utilising the contact points of the Camden Asset Recovery Interagency Network (CARIN) and the other regional ARINs.

Finally, the FATF's financial investigations guidance highlighted that it is essential for financial investigators to discuss issues and strategy with foreign counterparts, and this should involve consideration of conducting a joint investigative team or providing information to foreign authorities so that they can conduct a parallel investigation.

Mutual legal assistance

Mutual legal assistance is one of the most decisive weapons states have to fight serious international crime. The need for a mutual legal assistance requests may arise quickly, but they need to be drafted in such a way that complies with treaty requirements and makes it easier for the requested state to comply with the request. Challenges to executing requests can arise when criminal justice practitioners from different legal systems attempt to work together.

Practitioners noted that central authorities should be proactive, communicative, and arrange for direct consultation between operational authorities if required. Countries noted that they had better results seeking co-operation when they shared draft requests before sending final versions, actively followed up on requests, answered questions from the requested state, and engaged in a dialogue instead of blindly mailing documents back and forth. Participants noted that the system of treaty-based assistance can be speeded up using technological aids, such as video-teleconferencing and emailing advanced copies of MLA requests.

There are, however, some particular challenges related to international co-operation. A jurisdiction may choose not to seek formal co-operation such as mutual legal assistance (MLA) where they consider it is unlikely to receive a response. Some obstacles to co-operation included a lack of bilateral or multilateral treaty basis, not having the knowledge or guidance to draft a quality, actionable request, or having very rigid standards for seeking international co-operation. Finally, during the workshops, one major challenge to effective international co-operation was the lack of a clear political commitment to co-operate, especially when one country's nationals are being investigated in another country.

International co-operation in a TF case may also be difficult where one of the cooperating jurisdictions may be seeking capital punishment in the case. There have also been issues with dual

criminality, especially in situations where the funding an individual terrorist is not adequately criminalised.

As detailed, good practices in this area include:

- Considering informal methods of international co-operation such as FIU-FIU, police-police or prosecutor-prosecutor co-operation before submitting a formal MLA request.
- Prioritising MLA requests that have a ML or a TF element or seek urgent action to seize assets.
- Providing assurances about the penalties that are being sought by the prosecution in certain cases to facilitate extradition (e.g., assurances that the death penalty will not be sought in a terrorism-related prosecution).
- Using networks as such as EUROJUST or CARIN and ARINs prior to making a formal request to facilitate international co-operation and target the assistance that will be sought.
- Making contact with overseas authorities and arrange to send a draft copy of a proposed MLA request, so that they can advise on the content and wording of the request.
- Demand to keep the fact or the contents of a MLA request remain confidential.
- If countries utilised central authorities, the secondment of confiscation, ML, and/or TF specialists to such a central authority was seen as advantageous.
- Using regional tools such as European Investigation Orders and Council of Europe Convention no. 198 ("Warsaw Convention").
- Building trust and informal connections between jurisdictions to facilitate MLA and more informal channels of international co-operation and information exchange.
- Using the Mutual Legal Assistance Request Writer Tool (MLA Tool) that has been developed by UNODC to assist states to draft requests with a view to facilitate and strengthen international co-operation.

FATF/APG/EAG Workshop for Judges and Prosecutors
January 2018, Shenzhen, China

Potential next steps

The criminal justice system is a crucial component of effective anti-money laundering and countering terrorist financing systems (AML/CFT), and FATF places considerable importance on countries ensuring that criminals and terrorists are convicted and given dissuasive sentences, and deprived of their proceeds.

The findings from the process initiated by FATF President Santiago Otamendi to thoroughly examine the experiences, challenges and best practices in investigating and prosecuting money laundering (ML) and terrorist financing (TF), and in confiscating assets linked to criminal activity are laid out in this President's paper. The findings are laid out in detail above, with key points mentioned in the Executive Summary, and draw on both the experiences of national experts, but also on the review of mutual evaluation reports and other research.

The exercise has reinforced the FATF's focus on achieving effective results as regards the investigation and prosecution of ML and TF offences and on the recovery of the proceeds of crime.

The FATF programme of several regional workshops, carried out jointly with the FSRBs and other international organisations, has brought together almost 450 judges and prosecutors from more than 150 jurisdictions to share their experiences and best practices. This by itself has already provided real benefits with strengthened contacts and informal networking by the judges and prosecutors attending.

The FATF can follow up in a range of ways on the strong progress made under this Presidency initiative:

- **Dissemination**
  The paper will be broadly disseminated, not only through the FATF and FSRB delegations, but also to other relevant international organizations such as the Organization for Security and Co-operation in Europe, the World Bank, the International Monetary Fund, the International Prosecutors Association, the International Magistrates Association and various Asset Recovery Networks, among others.

- **Training needs**
  The FATF may consider how further training and capacity building for investigators, prosecutors, and judges on ML/TF investigation and prosecution and asset confiscation can be provided. This could also involve increased action to effectively coordinate the efforts of countries and other donors and match the technical assistance provided with the specific needs observed.

- **Networks for judges, prosecutors and investigators**
  The value of international cooperation networks were highlighted during the regional workshops. Workshop participants considered that a network for judges and prosecutors focusing on ML/TF cases and asset confiscation would be very useful, and FATF may consider how to better ensure that adequate channels promoting informal information sharing are put in place.

- **Enhanced participation and collaboration**
  The expert input of judges, prosecutors, and investigators is vital to ensuring a good understanding of ML/TF risks and threats, and to the development of standards, policies, and new tools to effectively investigate and prosecute ML and TF. Strengthening this input will also provide an opportunity to have better informed policy decision making. FATF already works closely with many international partners, and will work to strengthen even further its engagement with relevant bodies and networks such as CARIN and the ARINs, EUROJUST, the International Association of Prosecutors, and the International Association of Magistrates.

- **Further products**
  FATF can also consider how it can work with partner organisations to create further products that will also be useful for practitioners. Workshop participants already identified potential value from products such as handbooks, checklists, investigative guides, and a model MLA request database.

The work undertaken over the year has reinvigorated and refocussed FATF's attention on the criminal justice system, which is a fundamental underpinning to all national and international efforts to combat money laundering and terrorist financing. Based on these findings, the US Presidency of FATF will continue this joint effort to enhance the effectiveness of the Criminal Justice System.

ACRONYMS

AML	Anti-Money Laundering
ARIN	American Registry for Internet Numbers
CARIN	Camden Asset Recovery Inter-Agency Network
CFT	Countering the Financing of Terrorism
DNFBP	Designated Non-Financial Business and Profession
IO	Immediate Outcome
LEA	Law Enforcement Authority
MER	Mutual Evaluation Report
ML	Money Laundering
MLA	Mutual Legal Assistance
NCB	Non-conviction based Confiscation
OSCE	Organization for Security and Co-operation in Europe
R.	Recommendation (FATF 40 Recommendations)
TF	Terrorist Financing
UNODC	United Nations Office on Drugs and Crime

FATF

FATF President's Paper: Anti-money laundering and counter terrorist financing for judges & prosecutors

This report presents the findings from the process initiated by FATF President Santiago Otamendi (2017-2018) to thoroughly examine the experiences, challenges and best practices in investigating and prosecuting money laundering (ML) and terrorist financing (TF), and in confiscating assets linked to criminal activity.

www.fatf-gafi.org

June 2018

Appendix UU:

FATF, *FATF Guidance: Private Sector Information Sharing* (Paris: FATF, 2017)

FATF

FATF GUIDANCE

PRIVATE SECTOR INFORMATION SHARING

NOVEMBER 2017

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2017), *Guidance on private sector information sharing,* FATF, Paris
www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-information-sharing.html

CONTENTS

INTRODUCTION

BACKGROUND AND CONTEXT

1. Effective information sharing is one of the cornerstones of a well-functioning AML/CFT framework. Constructive and timely exchange of information is a key requirement of the FATF standards and cuts across a number of Recommendations and Immediate Outcomes. Financial institutions should not be unduly prevented from sharing information for the purpose of ML/TF risk management.

2. Information sharing for AML/CFT purposes in financial institutions such as banks can occur at different levels within the same group. Other financial institutions such as money and value transfer service providers (which operate mostly through agents or other distribution channels) may have different business models and structures. The underlying objective of effective information sharing applies to all such financial institutions operating through various structures.

3. Information sharing also takes place between different entities and sectors for example between financial institutions not part of the same group and public sectors, and vice versa. Such information flow can take place within the domestic context or it can be across borders. Public-to-public sharing of information is equally critical and is an important element for the effectiveness of the domestic co-ordination and co-operation regime.

4. Information sharing is critical for combatting money laundering, terrorist financing and financing of proliferation. Multinational money laundering schemes do not respect national boundaries. Barriers to information sharing may negatively impact the effectiveness of AML/CFT efforts and conversely, inadvertently facilitate operations of such criminal networks. This underscores the importance of having rapid, meaningful and comprehensive sharing of information from a wide variety of sources, across the national and global scale.

5. Sharing information is key to promoting financial transparency and protecting the integrity of the financial system by providing financial institutions, and relevant competent authorities the intelligence, analysis and data necessary to prevent and combat ML/TF. Similarly, financial institutions look to the public sector to share information on trend analysis, patterns of behaviour, targeted suspects or geographical vulnerabilities in order to better manage their risk exposure, monitor their transaction flows and provide a more useful input to law enforcement. Public and private sector institutions can be source as well as target of information flow. The use of data in this manner highlights the importance of a continuous dialogue between the public and private sectors. The reliance on shared information also underlines the increased focus of international efforts towards identifying potential barriers to information sharing which might impinge on the effectiveness of the system and exploring possible policy and operational solutions to overcome them.

6. In June 2016, FATF issued Consolidated Standards on Information sharing[1] containing relevant excerpts from the FATF Recommendations and Interpretive Notes which relate to information sharing. The consolidation of existing Standards without any amendments was done in order to add value and to help to clarify the requirements with respect to information sharing, which are spread across 25 of the FATF Recommendations, and which impact 7 Immediate Outcomes in the FATF Methodology for assessing effectiveness. These are a starting point for the issues considered in this paper.

[1] Consolidated FATF Standards on Information Sharing.

PURPOSE OF THIS GUIDANCE, TARGET AUDIENCE, CONTENT AND THE STATUS OF THIS GUIDANCE

7. The purpose of this Guidance is to:

i. Highlight the usefulness of information sharing among entities of the private sector (particularly financial institutions) to increase the effectiveness of their ML/TF prevention efforts.

ii. Identify key challenges that inhibit sharing of information group-wide and between financial institutions not part of the same group;

iii. Clarify the FATF Standards on information sharing regarding: a) group-wide AML/CFT programmes and within its context, sharing of information on suspicious transactions within the group, and how STR confidentiality and tipping-off provisions interact with such sharing; and b) between financial institutions not part of the same group;

iv. Highlight country examples of collaboration between data protection and privacy and AML/CFT authorities to serve mutually inclusive objectives;

v. Provide country examples to facilitate sharing of information within group, between financial institutions not part of the same group; and of constructive engagement between the public and the private sectors;

vi. Support the effective implementation of the AML/CFT regime, through sharing of information, both in the national and international context.

8. The target audiences of this Guidance are:

i. Countries and their national competent authorities with responsibility for AML/CFT;

ii. Practitioners in the private sector, including financial institutions that have group-wide AML/CFT programme obligations to fulfil or that process customer transactions with other institutions; and

iii. National and supra-national data protection and privacy (DPP) authorities.

9. The paper sets out the challenges to information sharing and provides guidance both in the context of group wide and between financial institutions not part of the same group. Annex-1 articulates how differences in DPP regimes or their application can affect the information flow. Annex-2 includes country examples and approaches on addressing some of these challenges, including of national DPP and AML authorities working together to meet their respective objective. It also sets out innovative practices adopted by countries to promote group-wide information sharing and between financial institutions which are not part of the same group. The section further contains examples of established mechanisms and processes to ensure guidance and feedback for the private sector, which helps facilitate better information sharing among all stakeholders. It should be noted that these examples are presented for information only. These examples are illustrative in nature and not to be construed as FATF recommended approaches. These examples are also cross-referred with respective sections of the guidance. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the legal framework. This Guidance is non-binding and it draws on the experiences of countries and of the private sector and may assist competent authorities and financial institutions to effectively implement some of the Recommendations.

GENERAL INFORMATION SHARING ISSUES

10. Information sharing plays a vital role in allowing financial institutions and supervisory and law enforcement authorities to better deploy resources on a risk based approach, and develop innovative techniques to combat ML/TF. The size and geographical scope of the international financial system makes it imperative to improve coordination and collaboration between all the stakeholders if the measures to identify and prevent ML/TF are to succeed. Enabling greater information sharing is a key element of collaboration whether it involves sharing across borders, between entities of the same financial group, between different financial groups or between private and public sector or vice versa.

11. Improvements in information sharing are also critical to enabling the full exploitation of the potential improvements to AML/CFT safeguards, and access to financial services, promised by new technologies and evolving business models. However, there remain obstacles to effective information sharing which can obstruct this progress and create legal and regulatory uncertainty. Challenges which have been identified are discussed below:

A. Legal Issues

12. Legal constraints may inhibit availability, access, sharing and processing of information for AML/CFT purposes. This may be on account of different policy objectives, customer confidentiality concerns and record retention requirements. In some instances, regulated entities are uncertain as to the sharing permitted under these legal regimes, and this clear lack of understanding inhibits effective information sharing. Countries should therefore overcome the challenges and implement an effective information sharing regime concerning application of different legal provisions in this context by providing appropriate clarifying guidance of their laws and regulations to eliminate ambiguity regarding sharing.

13. In particular, these challenges may emerge due to following concerns:

i. Different legal frameworks of Data Protection and Privacy (DPP) and their implementation

14. AML/CFT laws and regulations of a jurisdiction are designed to prevent, detect, disrupt, investigate and prosecute ML/TF. Individuals have the right to privacy and to protect their personal data[2]. This is a fundamental right in many jurisdictions. This right represents an important policy objective in accordance with the fundamental principles of domestic law. AML/CFT goals also serve significant national security and public interest objectives and should be pursued vigorously, in a way that is balances an individual's rights to protection of personal data and privacy. AML/CFT and DPP public policy goals are not mutually exclusive and should recognise support and be balanced.

15. Differences in DPP laws across jurisdictions may create implementation challenges, particularly for the private sector in sharing information. The issue may be further compounded if there is a lack of regulatory guidance, or an inconsistent approach towards AML/CFT requirements and DPP obligations. The perceived conflict between AML/CFT and DPP objectives may be due to lack of adequate coordination between different authorities at the rule making stage, leading to lack

[2] Personal data could mean any information relating to a natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

of the proper balance between data protection on one hand and prevention or combating of crimes on the other hand. The apparent complexity of different DPP approaches and the fear of penalties and risk avoidance have a significant impact on availability, access, processing or sharing of information by the private sector, even when such sharing is permitted.

16. While there are some situations where DP authorities try to provide support to public authorities and private stakeholders, there are many cases where, more clarity from national regulators and public authorities on how to effectively manage differing regulatory requirements may be helpful in this regard. For example, global financial institutions operating in multiple jurisdictions would benefit from data protection authorities issuing clarifying interpretation and guidance on the extent to which sharing personal data across borders for AML/CFT purposes is permissible under the public interest or other derogation(s) contained in different data protection regulations on data transfers (*e.g.* the extent to which transfers of data made for the purpose of complying with AML/CFT is permissible).

17. Countries should examine and if needed, amend and/or clarify the national legislations in order to ensure the proper balance. A dialogue between national authorities responsible for data protection and privacy and AML/CFT is useful, to adopt compatible and coherent policies such that financial institutions are able to meet legal requirements. National authorities could also consider developing and sharing, where necessary, an analysis of national laws and regulations to support effective information sharing (Paragraphs 3-7 of Annex-2).

ii. Financial institution secrecy provisions

18. Financial institution secrecy laws can inhibit information sharing. For example, financial institution secrecy can sometimes not be invalidated by "legitimate interest" or security concerns, depending on national legislation. In this respect, it should be noted that under Recommendation 9, countries are required to ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

B. Operational Challenges

19. Operational challenges may occur at an institutional and/or national level. IT capability of the financial institutions and their record-maintenance procedures may hinder effective sharing of information in a timely manner. For example, some customer information that might be useful for CDD purposes may not be integrated into financial institutions' AML/CFT systems because it was collected for a different purpose. Outsourcing rules which place a restriction on how much work can be centralised offshore and conversely data or onshoring rules which mandate that data, IT system and operational process remain onshore can create limitations leading to operational complexity and process fragmentation.

20. Inadequate IT tools, different data formats, lack of policies and procedures on how to deal with the information available and a general lack of appreciation of the value of information available both on the part of the public and private sector may act as barriers to information sharing, even when it is available. Issues of IT capability and IT integration may also arise when financial institutions grow a global footprint through acquisition, necessitating the integration of different IT systems into those of the acquiring institutions.

21. In certain cases, information exchange between the public and private sector as well as among private entities relies on predefined templates that allow for automatic analysis and

aggregation of information. These templates should be flexible enough to take into account other relevant information (such as IP addresses, phone numbers, usernames, job title and organisation etc.) that is available to financial institutions. Standardisation of data formats may also promote data sharing by enabling integration.

C. Challenges for Supervisors

22. From the perspective of supervisors, lack of information sharing may inhibit implementation of consolidated supervision for AML/CFT purposes (e.g., as required under Recommendation 26). For example, in case of financial institutions operating through a network of branches/subsidiaries in a number of countries, host country laws (applicable to such branches/subsidiaries) may not permit the home supervisor of the parent bank to have access to, and examine all the customer's information maintained by such branch/subsidiary. This may necessitate separate arrangements between the home and host supervisor whereby the home supervisors examine such customer files on behalf of the parent (home) supervisor. This may hinder the timely and comprehensive review of records and also adversely impact the effective application of the consolidated group supervision for AML/CFT purposes.[3]

23. Supervisors should thus promote bilateral or multilateral agreements that efficiently support information sharing for AML/CFT purposes, specifying the information to be exchanged when exercising consolidated or group-wide supervision, along with the definition of timelines for the provision of that information. While these arrangements cannot overcome legal impediments that hinder information sharing, in case the consolidated supervision of the group is hindered due to any reasons (including lack of access to relevant information), or if the group is exposed to excessive risks that are not properly managed, home supervisor may limit the range of activities that the group may conduct and subject it to escalating supervisory measures, including directing the financial group to close the foreign offices in extreme cases.

[3] Essential Criteria 8 of the BCBS Core Principle 13 (home-host relationships) requires that the home supervisor is given on-site access to local offices and subsidiaries of a banking group in order to facilitate their assessment of the group's safety and soundness and compliance with customer due diligence requirements.

INFORMATION SHARING UNDER FATF RECOMMENDATIONS

24. This section sets out key FATF Recommendations (R.18, R.20 and R.21) and their expectations in the context of information sharing within financial group. The section also covers information sharing between financial institutions not belonging to the same group, as provided under FATF Recommendations.

A. Information sharing within financial groups

Recommendation 18- Internal controls and foreign branches and subsidiaries

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

i. Meaning of 'financial group' or 'group-wide' in the context of information sharing

25. A financial group's programmes against ML/TF should be applicable to all branches and majority owned subsidiaries of the financial group.[4] These programmes should include policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management. Group-level compliance, audit, AML/CFT and other functions with a role in oversight/management of group-level ML/TF risks should also be provided with customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes.[5] This should be subject to safeguards sufficient to ensure confidentiality of information and its use for the intended purposes only.

26. The term "Group wide" (or "enterprise-wide") used in the context of AML/CFT Programme requirements for the financial group under FATF Recommendation 18 includes all the entities (in domestic and cross border environments) comprised by the definition of financial group laid down in the FATF Glossary. This is in line with the principle that a financial group as a whole may be exposed to ML/TF risk due to activities of its group entities, which are covered under FATF Recommendations, and hence such risk should be identified, managed and mitigated at the group level.

27. As per the FATF Glossary, "Financial Group means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level."

[4] Interpretive Note to Recommendation 18, paragraph 4.
[5] Interpretive Note to Recommendation 18, paragraph 4.

ii. Information required to be shared for group-wide programmes

28. Information sharing in the financial group is meant to effectively identify, manage and mitigate ML/TF risks by the group. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management (see paragraphs 50-54 below for further details). This should be in accordance with the legislative framework (both of home and host countries), determining the scope, extent and mechanism of such information sharing.

29. The table below explains the broad AML/CFT purposes that such sharing seeks to achieve. This is to reinforce the point that sharing of information for group compliance is meant to ensure comprehensive and effective ML/TF risk management and compliance. All the information as indicated in the below table may not be available, collected or needed in each and every case. This would depend upon the products and services being provided to the customers, geographical location, the existing legal framework as well as risk and context. Nevertheless, intra group information sharing may lead to an effective group-wide compliance programme.

Table 1. **AML/CFT Purposes for Information Sharing**

Types of Information	Examples of information elements (as available, when necessary)	AML/CFT purposes for sharing information within the group
Customer Information	Customer identification and contact information (name and identifier), in case of legal persons and arrangements: information on nature of its business and its ownership and control structure; legal form and proof of existence; address of registered office and principal place of business; Legal Entity Identifier (LEI) information, financial assets records, tax records, real estate holdings, information on source of funds and wealth, economic/professional activity, and account files, whether the customer is a PEP (including close associates or family members) or not and other relevant elements from documents collected while on-boarding the customer or updating records, targeted financial sanction information and any other information, whether identified from public sources or through internal investigation relating to ML/TF, risk categorisation of customer etc.	Manage customer and geographical risks, identify global risk exposure as a result of on-boarding of the same customer by multiple entities within the group, more efficient record-keeping of customer information.
Beneficial Owner Information	Beneficial owner identification and contact information, real estate holdings, information on source of funds and wealth, economic/professional activity, and account files, whether the beneficial owner is a PEP or not and other relevant elements from documents collected while on-boarding a customer or updating records.	Manage beneficial owner and geographical risks, identify the same beneficial owner for multiple entities within the group, more efficient record-keeping of beneficial owner information.

Types of Information	Examples of information elements (as available, when necessary)	AML/CFT purposes for sharing information within the group
Account Information	Bank/other account details, including the intended purpose of the account, expected location of transactions/activity as expressed by the customer and business correspondence etc.	Effective due diligence and transaction monitoring at group level, justification of transaction pattern vis à vis financial profile, follow-up on any alerts or abnormal trading pattern across the group.
Transaction Information	Transaction records, credit and debit card records and usage, past credit history, digital footprints (IP address, ATM usage information etc.), attempted/failed transaction information, currency transaction reports, information on closure of account or termination of business relationship due to suspicion, analysis made to detect unusual or suspicious transactions etc.	Global transaction monitoring, alert processing and identifying suspicious transactions, flagging and checking the existence of similar behaviour across business lines within the group.

iii. Importance of sharing of information for group-wide programmes

30. In the broader context, sharing of information for group-wide compliance is important for effective identification, mitigation and management of ML/TF risk by the financial group. It will also allow the group to exercise better internal controls and improve the quality of decision-making on due diligence, transaction monitoring and suspicious transaction reporting. The sharing of information by group entities, including subsidiaries and branches with the head office allows the group compliance to put in place comprehensive risk management processes. Consolidated screening and monitoring of customers and transactions to identify potential breaches of targeted financial sanctions also depends on the availability of information about listed entities and customer's activities with different entities of a group.

31. The BCBS's 2017 Guidelines[6] on *"Sound management of risk related to money laundering and financing of terrorism"* also provides comprehensive guidance to banks on the effective management of ML/TF risk in a group-wide and cross-border context. It explains the rationale behind and principles of consolidated risk management; how group-wide AML/CFT policies and procedures should be consistently applied across the group, and, where reflecting local business considerations and the requirements of the host jurisdiction, should still be consistent with and supportive of the broader policies and procedures of the group; and how banks should address differences in home/host requirements. It also provides detail on how banks that are part of a group should share information with members of the same group with a view to informing and

[6] See BCBS Guidelines on Sound Management of Risks Related to Money Laundering and financing of Terrorism.

strengthening group-wide risk assessment and the implementation of effective group-wide AML/CFT policies and procedures.[7]

32. The following are the main outcomes expected of information sharing for group-wide programmes:

a) Global risk assessment

33. For an effective group-wide compliance programme, financial institutions should understand the ML/TF risks they are exposed to on a global basis. Such risks may be due to customers, products, geographical profile of their operations, transaction pattern or other factors from each entity belonging to the same group. A comprehensive understanding and identification of these risks will allow the financial institutions to better structure its risk profile and take commensurate measures. Information from branches, subsidiaries and other parts of its business should feed into overall risk assessment. It will help identify and determine the nature and level of ML/TF risk of each entity belonging to the group and the level of ML/TF risk of the group on a global basis, particularly where the shared information relates to cross border relationships. Thus, it is important that the group compliance is able to obtain and has access to such information, including from its overseas operations, where required. For example, if Bank A, located in Country X, identifies a money launderer and closes his accounts, but that same money launderer has an account with Bank A's subsidiary in Country Y, that subsidiary will continue to provide banking services to the money launderer as it will be unaware of the activity and bank actions in Country X. Financial institutions should also, when assessing the ML/TF risks they are exposed to on a global basis, take into consideration the barriers to required information sharing, which may inhibit effective implementation of FATF Recommendations, as an autonomous risk and consider mitigation measures accordingly.

34. Sharing of information with group compliance (i.e. at a head office level) does not assume that the ML/TF risks should be assessed only by the group compliance for the whole group in all the locations where it operates. Each operation in a given location should be responsible in its own right for assessing its ML/TF risk and should have information relevant for its own risk assessment. For this purpose a local operation of a multi-national group in a given jurisdiction would equally require access to information from group compliance or from other parts of the group that is relevant to its own risk assessment. A multi-national group should, therefore include in its risk assessment and management framework a mechanism to determine when its local operations are required to assess multi-jurisdictional risk in relation to a customer relationship and when it would be justified, or indeed required, to share customer or transaction information across more than one geographic location.

35. Furthermore, centralised storage of records should not be equated with group-wide sharing of the information contained in records. Access to electronically/centrally stored records should be managed in accordance with confidentiality and other obligations. Global transaction monitoring must always be done in a manner that enhances compliance with risk management and reporting obligations in all the locations where a multi-national group operates. Thus, monitoring in one location should not weaken compliance with these obligations in other locations where the group operates. Consideration should be given to local legal constraints on access to confidential

[7] "Regardless of its location, each office should establish and maintain effective monitoring policies and procedures that are appropriate to the risks present in the jurisdiction and in the bank. This local monitoring should be complemented by a robust process of information sharing with the head office." (Paragraph 72).

information and addressed in the global risk assessment with commensurate measures implemented by the financial group.

b) Effective mitigation of customer, product, services and geographical risks

36. Developing appropriate measures to mitigate customer, products and services and geographical risks requires having adequate information on customers, their transaction patterns, expected location of transactions/activity as expressed by the customer, products and services used and, where necessary, on the source and/or destination of funds. Information so obtained by the financial groups will help in devising appropriate solutions to manage and mitigate risks. For example, based on an overall assessment of customers or customers' categories, financial institutions may devise policies on additional or enhanced due diligence measures, stricter transaction monitoring procedures, face-to-face interaction with certain customers, more frequent review of customer information etc.

37. Similarly, information shared by a financial institution with group compliance on identified misuse of new or existing products or services and measures taken to mitigate the risks may help the group take a consistent approach in a multi-national environment. Such mitigation procedures at a group level can be implemented effectively only if the group compliance has adequate information about its customers, their transactions and activity level and any abnormal pattern based on available customer information. For example, a politically exposed person (PEP), located in Country X, a high risk jurisdiction for corruption, sends one high-value wire inconsistent with their profile, without an explanation in response to bank's inquiries, which leads the bank to close the PEP's account. The same PEP uses another account in Country Y with the same banking group to send structured wire transfer and lies about the source and purpose. The subsidiary in Country Y will not be aware of the account closure in Country X by its subsidiary which will prevent them from properly risk managing the customer. This may also prevent detection of potential STRs in the cross border context based on information gathered from various sources within a group.

c) Consistent application of controls

38. Local operations of a global firm have to be in line with local laws and regulations. At the same time, these should also be subject to its group wide compliance programmes to ensure consistent application of controls across the group level. Enforcement of group wide controls and procedures requires sharing of relevant information with the financial institution's group compliance. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of internal controls (including sharing of information, as required under FATF Recommendations), financial groups should apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including as appropriate, requesting the financial group to close down its relationships with the host country.[8] This may be required, for example, when the risks outweigh the institution's ability to manage the risk through commensurate measures.

[8] INR 18.5.

39. Information on customers' identification and acceptance policies, internal and external audit reports, supervisors' on-site inspection reports and sanctions and remedial actions imposed as well as sample records evidencing due diligence measures undertaken, reporting done and record-keeping requirements complied with, where appropriate shared with the group compliance may help enable assessment of implementation. This will allow the firm to enforce its global controls, taking into account the specificities of each country and location. For example, lack of CDD and record-keeping measures undertaken by bank A's subsidiary in country X may weaken the overall effectiveness of group controls of the bank. Financial institution at a global level may verify the implementation of these measures if its group compliance has access to such records on a sample basis.

d) Common approach by financial conglomerates having multiple businesses

40. Quite often, financial groups have their operations across multiple line of business (bank, securities, insurance, commodities etc.). Group-wide compliance means that such financial conglomerates should be in a position to monitor and share information on their customers' identities, their transaction and account activities across the entire group. While some adjustments may be needed due to different AML/CFT requirements for each sector, sharing of information would enable a comprehensive risk management approach on a consolidated basis. For example, if financial group A has presence in banking, securities and insurance sector under the same group, unexplained cash deposits by a high-risk customer X in his bank account should trigger an alert about his transactions across other business lines. Absence of such information will allow the customer to continue his transactions in other sectors without similar monitoring or additional due diligence.

B. Sharing of information on suspicions that funds are the proceeds of crime or related to terrorist financing within the financial group

Recommendation 20- Reporting of suspicious transactions

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

41. FATF Recommendation 20 requires financial institutions to report suspicious transactions if it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing. Recommendation 20 only requires the reporting of suspicious activity in good faith and that does not equate to criminal liability. That is a determination for the national authorities (e.g. law enforcement) to make.

42. Technological advances in recent years have improved the analytic and processing capacity of financial institutions, and their ability to dig deeper in transactions and to identify trends and typologies based on information-flow from multiple locations, products and services and sectors. Advances in data science techniques and analytics enable financial institutions to sift through large amounts of structured and unstructured data to identify patterns and trends. Harnessing of this potential requires as much information as possible to be brought together, often in a centralised pool, and is in the interest of both the public and the private sectors.

43. Sharing of information and analysis of transactions or activities which appear unusual (if such analysis was done); including an STR, its underlying information, or the fact that an STR has been submitted by branches and subsidiaries with group compliance promotes effective implementation of group-wide compliance programmes.[9] Similarly, branches and subsidiaries should receive such information from group-level functions when relevant and appropriate to risk management. This applies both to domestic and cross-border environment where customers may have exposure across a group's operations and across more than one geographic location. It allows financial institutions to identify higher risk customers across the group's business and deploy specific monitoring mechanisms or enhanced measures. It also enables emergence of a global picture of the risk exposure of the financial institution to such customers, thereby promoting implementation of an effective risk-based approach. Such sharing, which may occur before or after filing of an actual STR by the financial institutions, where required will enable the group compliance to look at the suspect customer's activities or transactions across different verticals, lines of business and jurisdictions. This will also allow them to conduct sophisticated analyses of suspicious activities, assess these analyses against the client database and build the scenario across its global operations (paragraph 8 of Annex-2).

44. In the context of terrorist financing, timeliness of information sharing is critical. The instant sharing of relevant information within a financial group could be crucial, particularly where customers that were assessed as higher risk (due to their transaction history and/or country of origin) are involved. An initial suspicion by a financial institution that a transaction may involve TF may further be corroborated or confirmed if information on transactions involving the same customer or recipient of funds across the financial group is available. Such a chain of transactions would likely only be picked up if the initial suspicion was shared across the financial group and the customer or recipient was flagged for further attention. The process of sharing the information relating to a suspicion of TF and obtaining further corroborating information should, however, not cause a delay in the timely submitting of an STR in the host jurisdiction where the suspicion first arose or where the transactions in question have taken place.

45. The inability to lawfully share such information may potentially lead to inconsistent application of the group-wide compliance programme within the same corporate umbrella. As an example, it may result in a situation where one subsidiary has filed an STR about a particular client or transaction, but another group entity which is not aware, may fail to notice suspicious behaviour based on similar facts, warranting further scrutiny or an STR filing as needed. This inhibits the effectiveness of global group-wide compliance programmes. Furthermore, there may be cases in which such a scenario might render the group entity as a whole not compliant with STR requirements in the second jurisdiction, as knowledge of potential suspicious behaviour by the first subsidiary could be imputed to the entity. However this does not imply that intentional non-compliance to a financial group is imputed when the inability to communicate effectively is the result of the inability to lawfully share such information in the first instance. It is also incumbent upon the financial institutions to document appropriate criteria for the sharing of information (in accordance with laws and regulations in the host country) in support of a group-wide risk management compliance program and to ensure that safeguards are in place for the protection of the confidentiality of the information and its restricted use for the intended purpose of AML/CFT. Where there are challenges to the effective implementation of group-wide risk management, financial

[9] The Egmont group of FIUs issued a 'white paper on enterprise-wide STR sharing: issues and approaches' in February 2011. It sets out key issues for a cross border STR sharing regime and also presents possible approaches to facilitate enterprise STR sharing. The paper concludes that the cross-border element of enterprise-wide STR sharing necessitates that jurisdictions coordinate their actions in this field.

institutions should apply appropriate additional measures to manage the ML/TF risks and inform their home supervisors, as appropriate.

C. Confidentiality of STR and tipping-off and how it interacts with group-wide sharing

Recommendation 21 - Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

(a) …

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

i. Concerns on sharing of information on suspicious transactions within the group and potential solutions

46. One of the main concerns that relates to sharing of STRs (or sharing the fact that a STR has been filed or the underlying STR information) is ensuring their confidentiality, which is critical to the effective functioning of the reporting regime. Confidentiality of STRs is needed so that the subject of STR and third parties are not tipped-off, as this can adversely affect intelligence gathering and investigation, and can enable persons to abscond or dispose of assets. Confidentiality also protects the reputation of the person who is the subject of an STR. Finally, confidentiality protects the safety and security of the person filing the report, and breaches of confidentiality have the potential to undermine the entire suspicious transaction reporting regime. Unauthorised disclosure of STRs could also result in a financial institution facing criminal liability in many jurisdictions. These concerns necessarily place limits on the sharing of STRs.

47. The issue of STR confidentiality can get more complex if such sharing occurs across borders, where different national laws come into play. These may include, for example, national provisions relating to discoverability and production of available records (including STRs filed in host country and shared with group-compliance in home country) in home country's judicial proceedings, access to databases of financial institutions by national authorities etc.

48. Another concern that relates to sharing of STRs relates to how information can be shared domestically and internationally. Concerns also exist on the treatment of foreign STRs or information that reveals the existence of a foreign STR in legal proceedings. This is unclear and varies considerably in both civil and criminal cases across countries. While some countries have regulations which require regulator notification of judicial requests and subpoenas concerning domestic STRs so that the regulators can intervene to ensure STR confidentiality in the legal proceedings, these regulations may not protect foreign STRs submitted to a foreign FIU. Quite often, concerns also exist regarding the confidentiality of STRs once these are shared cross border, including their potential misuse for unrelated purposes, leakage to media for political gains, and sharing without due process of law. From an FIU's perspective, one of the key concerns is to avoid situations where third parties (including authorities in third countries) may have unjustifiable access to the relevant information especially if STRs are shared across jurisdictions systematically rather than because they have a multi-jurisdictional element to them. In order to ensure the confidentiality of STRs which are shared across jurisdictions, countries should consider extending

the same legal protections to foreign STRs which are given to domestic STRs within their legal system.

49. Finally, there are concerns that group-wide suspicious information sharing could potentially lead financial groups to systematically submit STRs only in their home jurisdiction, rather than in the jurisdictions in which the relevant financial institutions of the group are located. A related concern is that even if the STR is submitted in the relevant jurisdictions, the financial group's internal investigation may take place only in one jurisdiction (of the parent company), leaving some relevant information outside the reach of the host FIU's powers to request additional information from the financial institution. Such coordination and internal investigation across the group should be handled expeditiously so as to not lead to delay in the timely filing of the STR with the financial intelligence unit in the host jurisdiction. To allay these concerns, it is emphasised that financial institutions are required to file suspicious transaction reports with the financial intelligence unit of the host jurisdiction[10] where they are operating promptly, regardless of any sharing.

ii. Possible mechanisms for sharing of suspicious information within financial group

50. There are different ways in which information relating to unusual or suspicious activity can be shared within a financial group, based on the domestic or supra-national legal framework of jurisdictions concerned. This does not necessarily have to be by sharing an STR itself, which is prohibited in certain jurisdictions. This can be achieved, for example through: (a) sharing of information and analysis of transactions or activities which appear unusual, if such analysis was done (e.g. facts, transactions, circumstances and documents, including personal information). These information elements are illustrative and not meant to provide an exhaustive list. Sharing of relevant information in such cases could be without disclosing the fact that an STR is filed; or (b) disclosing the fact that a STR has been filed; or (c) disclosing the fact that an STR has been filed and sharing underlying information (e.g. information on suspicions and the results of any internal analysis or examination, (but not the STR itself); or (d) sharing of STRs and underlying information. This can be depicted as follows:

Table 2. **Possible ways for sharing suspicious information within financial group**

Possible ways	Information on suspicions, internal analysis or examination	Fact that an STR is filed	The STR itself
(a)	✓		
(b)		✓	
(c)	✓	✓	
(d)	✓	✓	✓

[10] Under the EU framework, financial institutions have to report suspicious transactions to the FIU of the Member State in whose territory the obliged entity transmitting the information is established. This means that in situations of free provision of cross-border services, STRs must always be submitted to the home FIU; if financial institutions operate establishments in another Member State, they must submit STRs to the host FIU. In some specific circumstances and subject to limitative criteria, national laws may go beyond EU passporting rules. The European Court of Justice confirmed that, subject to the conditions that no effective mechanism ensuring full and complete cooperation between the Member States exists which would allow AML/CFT crimes to be combated effectively, and on condition that the legislation is proportionate, EU law would not preclude Member State's national legislation which requires credit institutions operating in that Member State without being established there, to forward directly to these Member State's authorities information necessary for combatting ML/TF (see C-212/11 - Judgment of the Court (Third Chamber) of 25 April 2013 - Jyske Bank Gibraltar Ltd v Administración del Estado)

51. One of the key objectives of information sharing in this respect is to improve compliance with risk management and reporting obligations in all the locations where a multi-national group may operate. The overarching principle should be that the shared information may be found relevant by group compliance for an overall analysis and ML/TF risk management across the group or for some entities belonging to the group. There should, therefore, be a cross-jurisdictional element to the shared information such as a customer that has exposure to operations of the group in more than one location or aspects of the flow of transactions or funds that affect operations in the relevant jurisdictions. Such sharing should be subject to adequate controls and monitoring by the group compliance to protect confidentiality of information and ensure its use only for ML/TF risk management.

iii. Criteria for sharing information within financial group

52. Financial institutions should determine appropriate criteria for sharing such information for the purpose of group compliance. This need not be the same criteria as for reporting of STR. For example, in some cases, there may still not be sufficient grounds to convert triggered red flags into to an STR, though sharing of information on any further analysis carried out in such cases to group compliance, may reveal additional information which may help making a filing decision. Depending on the circumstances, a financial institution may reach the STR reporting threshold at the same time as the unusual or potentially suspicious activity is initially detected (including prior to the execution of the transaction for attempted transactions). Or, in many cases, further analysis will be needed in order to determine whether the threshold for suspicion is met. This analysis may or may not result into filing a STR. Further, the very nature of transaction or business relationship of customer with financial institution may make some information irrelevant for the purpose of group compliance. This may happen if the transactions are localised, without any potential for them to extend to other branches, subsidiaries or sectors. Financial institutions should make appropriate decisions in such instances based on the context, complexity and materiality of identified cases.

53. Systematic sharing of such information on a group-wide basis in each and every case may not be necessary or conducive to improved compliance with risk management and reporting obligations. Financial institutions should expressly address in their risk assessment and management framework where it should lay the basis for identifying the instances and the types of information that will be shared for group compliance. Criteria for reporting suspicions for the purpose of group compliance should be under periodical reassessment to take into account relevant events (such as group-wide audits or reviews) and be subject to supervisory scrutiny.

iv. Safeguards to protect information shared

54. Financial institutions should establish sufficient safeguards concerning the information shared to ensure that (a) confidentiality of information so shared is protected (including against tipping-off) and (b) information is used only for AML/CFT purposes and not for any other purpose. These should include policies, protocols and procedures for such sharing and setting up of access controls and firewalls, including conditions of information flows between the different entities of the group when needed (e.g. when different entities of the group have the same client) so that such information is ring-fenced, and accessible only by AML/CFT staff and only for specific AML/CFT purposes. Furthermore, the existence of suspicion on a client from an entity of the group does not imply automatically/systematically filing an STR by other entities of the group concerned, though it may be an important element for the risk analysis and the risk profile of the business relationship and may require enhanced CDD measures, where needed.

v. Resolving legal barriers and engagement with private sector

55. Countries should seek to address any legal and regulatory barriers which impede the flow of information within the financial group, thereby inhibiting effective implementation of FATF Recommendations. This may require a thorough assessment of the existing provisions (DPP, financial secrecy, AML/CFT or any other legislation) restricting information sharing. A proactive engagement with the private sector can also identify areas where there is a divergent view between the public sector and private sector on expectations of the existing requirements. This may be followed by issuing appropriate guidance and clarifications to create an enabling environment for sharing of information.

INFORMATION SHARING BETWEEN FINANCIAL INSTITUTIONS NOT IN THE SAME GROUP

56. Effective AML/CFT systems at national and international level also require information sharing between different financial institutions, which are not part of the same financial group. This includes information sharing between different institutions both within a single country, and internationally, and is affected by all the constraints and obstacles noted above. Key FATF Recommendations requiring information sharing between financial institutions which are not part of the same financial group are R.13 (correspondent banking), R.14 (MVTS), R.16 (wire transfer) and R.17 (Third party reliance). Each of these requires specific information to be provided or available, in order to implement essential preventive measures.

57. Sections III and IV set out information sharing between different financial institutions based on key FATF Recommendations, and also describe the benefits of voluntarily sharing additional information, and how this can be facilitated.

A. Information sharing under FATF Recommendations

i. In the context of correspondent banking relationships (R.13)

58. Financial institutions are required to gather sufficient information about a respondent institution to fully understand the nature of its business and to assess respondent institution's AML/CFT controls and be satisfied with the mode of use of payable-through accounts. This would include an understanding of types of customers the respondent institutions intends to service through such relationship, the expected nature of transactions, their value etc. In some specific cases the correspondent institution may require additional information from respondents to effectively monitor respondent's transactions. Such monitoring may require the respondent banks to provide specific transaction and customer information to correspondent banks to allow them to dispose the alerts generated by their transaction monitoring systems. However, this review of information by the correspondent bank should not be triggered by and does not amount to a requirement to conduct CDD on the customer of the respondent but as a consequence of the monitoring of the transactions to or from the respondent bank.[11]

59. Respondent institutions should be able to provide additional targeted information requested by correspondent in some specific cases on specific customers and transactions. Due to absence of such information on account of information sharing restrictions, correspondent banks may not be able to apply appropriate AML/CFT controls to manage the risks associated such relationships.[12] In such cases, without further information, correspondents may have no alternative but to suspend the business relationship. This could eventually lead to a delay in processing or even the termination of correspondent banking relationships, thereby exacerbating the de-risking phenomenon (paragraph 12 of Annex-2).

60. To avoid such a scenario, appropriate mechanisms should exist to allow respondent financial institutions to share the requested information with correspondents. For this purpose, authorities of the respondent institutions should understand and clarify the cases in which correspondent institutions may request information and the type of information they may request, so that an appropriate sharing mechanism is put in place by respondent financial institutions to

[11] See FATF Guidance on Correspondent Banking Services (in particular, paragraphs 3, 4, 5 and 18).
[12] See FATF Guidance on Correspondent Banking Services (in particular, paragraphs 32, 33 and 41).

enable such information-flow. Countries could also consider encouraging responsiveness from respondent banks and expressly set out their obligations to share information with their correspondent.

61. Where warranted, countries should consider conducting evaluation of their existing legal framework to address challenges to information sharing in this respect, to ensure their own data protection, financial secrecy provisions or other related regulations are not causing their financial institutions to lose access to correspondent banking services. A dialogue and engagement between public and private sector may also further help identify specific areas or issues where guidance may be needed.

ii. In the context of Money or Value Transfer Services (MVTS) (R.14)

62. Under R.14, MVTS providers working through agents (regardless of their location) are required to include them in their AML/CFT programmes and monitor them for compliance with these programmes. This would require sharing of information from agents to their MVTS providers to enable them to effectively monitor their transactions. This would enable the MVTS providers to not only fulfil their oversight responsibility but also add value to the transaction monitoring and reporting mechanisms put in place by agents through sharing of feedback and further information.

63. In appropriate cases, targeted sharing of information on suspicious transactions may also help MVTS providers better manage their ML/TF risk, and ensure compliance with existing risk management and reporting obligations. Countries could consider issuing necessary guidance in this respect and identify and address any specific barriers that prevent sharing of such information.

iii. In the context of wire transfer (R.16)

64. FATF Recommendation 16 requires countries to ensure that financial institutions include required and accurate originator information, and required beneficiary information, on all domestic and cross-border wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. The objective of R.16 is to ensure that the basic information on originator and beneficiary of wire transfers should be immediately available to FIU/LEAs and also to ordering, intermediary and beneficiary financial institutions for transaction monitoring and filing STRs, sanctions screening, freezing and tracing of wire transfers.[13]

65. In case the relevant information is missing, intermediary and beneficiary financial institutions are required to have risk based policies and procedures for determining (a) when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and (b) the appropriate follow-up action. This could, for example, include asking the previous financial institution in the payment chain for providing the missing or incomplete information as soon as possible. More fundamentally, such basic information about the originator and beneficiary is necessary for financial institutions to effectively execute wire transfers, and the transmission of such information would accordingly generally be authorised by non-AML legal frameworks.

66. Information sharing restrictions which impede financial institutions from sharing such information may lead to a considerable delay in processing. Countries should create enabling regulatory framework that removes barriers to information sharing in this respect. Appropriate guidance and feedback may further clarify regulatory expectations from financial institutions.

[13] FATF Interpretive Note to Recommendation 16, paragraph 1 and 2.

67. Further, consistent with paragraph 22 of the INR 16, MVTS providers are required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a funds transfer, the MVTS provider: (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether this gives rise to suspicion; and (b) where necessary should file an STR with the appropriate FIU, and make relevant transaction information available to the FIU.[14] This would also require information flow in respect of cross border transactions executed by an MVTS provider. Countries should remove any existing barriers to information sharing and consider issuing appropriate guidance so that MVTS providers are able to comply with these requirements.

iv. In the context of third party reliance (R.17)

68. Under Recommendation 17, financial institutions may be allowed to rely on third parties (whether domestic or cross-border), to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business. These elements are: (a) identification of customer, (b) identification of beneficial owner, and (c) purpose and intended nature of business relationship. The relying financial institution is required to immediately obtain necessary information concerning such elements, and to take adequate steps to be satisfied that copies of identification data and other CDD documents will be made available from the third party without delay, when so requested.

69. Use of third party reliance procedures is thus pre-conditioned on the ability of the financial institutions to be able to obtain relevant information from third parties. The need to understand the purpose and intended nature of business relationship may also necessitate sharing of additional information such as financial position of customers. This may help determine if the transactions being conducted are consistent with the financial institution's knowledge of customer, their business and risk profile. Information sharing restrictions or regulatory uncertainty may impede the ability of financial institutions to rely on third parties, especially in a cross border context. This may require intervention from host authorities of third parties to address any existing challenges, which prevent third parties from sharing information with financial institutions of the home countries, where permitted for reliance purposes.

v. In the context of regulation and supervision of financial institutions (R.26)

70. In the context of effective implementation of FATF Recommendations, for cross-border supervision, supervisors of the home jurisdiction should have access to the customer, account and transaction information maintained by the financial institution in the host jurisdiction, to the extent permissible under the legal frameworks of both jurisdictions. This should include STR and related information, where this is necessary to assess compliance with AML/CFT obligations and the robustness of risk management procedures. While host supervisors will be assessing compliance with local laws and obligations, home supervisors should have the ability to assess compliance with group-wide AML/CFT policies and procedures. Lack of such access may inhibit the ability of the home supervisor to effectively assess group compliance, thereby impacting the effective implementation of FATF Recommendations. If impediments to information sharing prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisors should make it clear to the host supervisor that the financial institution may be subject to additional

[14] See paragraph 67 of FATF Guidance on RBA for MVTS, February 2016.

supervisory actions, such as enhanced supervisory measures on the group, including, as appropriate, requesting the parent group to close down its operations in the host jurisdiction.[15]

[15] See BCBS Guidelines on Sound Management of Risks Related to Money Laundering and financing of Terrorism, June 2017: Section IV

INNOVATIONS IN INFORMATION SHARING

Information sharing beyond the FATF Recommendations

71. Sharing of additional information between financial institutions - beyond the required information noted above that is required by the FATF Recommendations - can have wider benefits by strengthening the understanding of risks and vulnerabilities. It can also ensure better compliance and leveraging of capacities by the private sector and preventing criminals from exploiting individual financial institutions' lack of awareness of their activity with other institutions.

72. For example, some jurisdictions have found that sharing alerts or information about customers who are refused or exited due to ML/TF concerns can prevent arbitrage of the financial system by criminals, who may attempt to engage with many different institutions. Consolidating information on payments by multiple institutions can identify criminals structuring payments using multiple institutions to avoid detection by other means.

73. However, such information sharing can also raise a range of public policy concerns about how the information will be used (or misused), including unfair commercial practices, encouraging de-risking and financial exclusion, potentially breaching STR confidentiality and increased risk of tipping-off, customer confidentiality, data protection and privacy, financial institution secrecy, as well as the general information sharing challenges described in the earlier part of this guidance.

74. For example, sharing of customer information between financial institutions could potentially raise competition concerns resulting from selective sharing of information with only a small group of participants. De-risking and defensive STR filing behaviour may be exacerbated, e.g. if financial institutions feel obliged to file an STR on a customer simply because they have learnt that other financial institutions have done so (and without conducting their own internal investigations). Overreliance on a system of sharing of suspicious information or a common platform could potentially lead to moral hazard where a financial institution would regard a potentially suspicious customer as suspicious before proper due diligence is done, and hence preventing the customer from accessing the entire financial system.

75. Countries should carefully consider the legal, policy and operational concerns noted above, and design means of mitigating them. This would for example, include consideration of measures to avoid abuse of the sharing mechanism, unauthorised use of the information obtained and violation of the underlying principles of such sharing arrangements, as well as potential implications of such behaviour.

76. Countries should also provide clarity on what types of information can be shared, with whom, under what circumstances, for what purposes, and subject to which restrictions, depending on the sensitivity involved and the need to ensure confidentiality of information. This understanding could be documented and be supported by information security guidelines and access protocols. This would avoid varied interpretation, ambiguity in understanding and inconsistency in implementation, all of which can impede information sharing under these provisions. Suitable oversight mechanism and transparency would also ensure the confidence in and accountability of all stakeholders.

77. Nonetheless, in recent years, countries and the private sector have made great strides in data analytics that aid in the detection of ML/TF activities and trends. In order to share such information, sufficient safeguards and mechanisms within existing legal frameworks are permitting

information sharing that provides improved and more real time and actionable information, leading to positive outcomes. Some such mechanism and processes are described below and in Annex-2.

A. Types of information sharing

78. A range of information can be shared in this context, and in a number of different ways. This is set out below:

i. Information on risks, crime trends and typologies

79. Financial institutions can collaborate to share analytical and strategic information on recent risk and crime trends, methods, techniques, common typologies and modus operandi identified to abuse the financial system. Such information, stripped of personal data, would accordingly not implicate data protection and privacy, tipping off, or other protections for personally identifiable information. Such information sharing may provide good insights which can be used by participating financial institutions in their operations. This promotes a greater collaborative environment among participants and can also help keep the risk assessment up-to-date based on current trends and methods.

80. Often law enforcement authorities are also part of these initiatives and can provide a more comprehensive update on these crime trends and typologies, including through case examples and specific information on ML/TF risks. This can raise general awareness of the current financial crime scenario, strategic and operational risks derived from such crimes and their possible impact on the financial industry as a whole.

ii. Information on transactions and customer information

81. Some countries under their own domestic legal framework specifically allow sharing of certain transaction information, and other information on suspicious transactions (but not necessarily of the STR itself) between financial institutions which are not part of the same group. This may include information on customers, representatives and/or beneficial owners associated with two or more financial institutions or covered entities, including information on individuals or entities suspected of ML/TF. This applies, for instance, in cases where financial institutions share or have the same customers (paragraphs 10-14 of Annex-2).

82. Such information sharing may provide additional elements to asses customers' risk more effectively or may also facilitate confirmation of initial suspicion for example, when a newly opened account with some activity for a few months suddenly receives a huge wire transfer and it becomes necessary to request information from the remitting bank to confirm the source of funds and other related details. Countries could consider encouraging financial institutions to share specific threat information and high risk customer information with one another. This facilitates sharing of intelligence and assists in decision-making by authorities and the private sector, wherever relevant.

B. Mechanisms for information sharing

83. A number of possible models are currently being developed which may encourage such voluntary sharing of information. It could include include bilateral information exchange between financial institutions and/or **shared KYC utilities and/or centralized data repositories**, which capture key elements of customer and transaction information and disseminate such information to participating financial institutions with appropriate protocols and access controls. Such utilities can contain different types of information for AML/CFT purposes. It includes identification information on customer and/or beneficial owner and additional information to support risk assessment and risk profiling of customer by financial institutions. These utilities can be used at the time of on boarding a customer, to access customer information, as well as on an ongoing basis, to perform further customer due diligence measures. Such utilities can also contain updated information on respondent institutions, which can facilitate their risk assessment and ongoing due diligence by correspondents. In all such cases, the ultimate responsibility for due diligence remains with the financial institution using such utilities.

84. These utilities and databases can be hosted by the authorities or the private sector or both through a public private partnership. For example, in some countries databases to share information on international wire transfers conducted or either the fact that STRs have been filed and/or the content itself of STRs and related information have been created to facilitate information sharing in appropriate cases among reporting entities, as well as administrative and law enforcement authorities. However, such utilities and/or repositories, whoever hosted by, could give rise to questions on where the ultimate responsibility for monitoring lies, and who should be held accountable for failures – another form of moral hazard.

85. In some cases, **specific information sharing arrangements** to facilitate information sharing among financial institutions for AML/CFT purposes have been reached between jurisdictions. This can provide statutory gateway to facilitate information sharing between financial institutions in a cross border environment for AML/CFT purposes.

86. **Public private partnerships** for information sharing are also being developed in a number of jurisdictions and have achieved positive outcomes. Through such partnerships, information is shared across law enforcement, FIU, vetted participants from the private sector as well as international partners in some cases, to facilitate a more comprehensive view of transactions and customers' behaviour. Such sharing often happens in a secured environment in order to facilitate further data-mining, operational analysis and scanning by the private sector to fill potential intelligence gaps.

87. **Industry forums or platforms-** Initiative can also be steered by financial institutions by creating structures such as inter- bank forum or through their banking/industry associations to share information on recent crime trends, modus operandi and typologies across participants. Representatives of law enforcement and supervisors could also collaborate in such initiatives to further support the work.

88. Information sharing on customers and suspicious transactions may be facilitated by safe harbour provisions for financial institutions, provided that the safe harbour is not abused, and they have established and maintained adequate procedures to protect the security and confidentiality of the information. Such safe harbours can carve out specific legal protection to enable information sharing between financial institutions for AML/CFT purposes.

89. Annex-2 of the guidance provides information on the approaches taken by a number of countries to facilitate such information sharing. These are set out in detail in particular, in paragraphs 10-22, 29-30 and 32-34 of the Annex. These examples are presented for information only and their inclusion in this guidance does not amount to their endorsement by the FATF. Further, the Annex is only illustrative and does not contain an exhaustive list of all the examples, which may be leading to diverse outcomes. It, however highlights how different types of information (strategic as well as operational and customer related) can be shared following different models or mechanisms in different contexts for AML/CFT purposes.

90. There are significant benefits of information sharing between financial institutions and at the same time, there are potential risks that need to first be addressed or mitigated. It is also affected by the same challenges as noted above. Countries are encouraged to assess how such voluntary information sharing which is beyond what is required by the FATF Standards can improve their AML/CFT system, and to develop their legislative framework to enable such sharing of information.

GUIDANCE AND FEEDBACK

91. Lack of guidance and feedback by public sector authorities on information shared by the private sector may hinder private sector's ability to effectively monitor transactions and provide well-developed reports to FIUs. In appropriate cases, countries could consider putting in place enhanced "feedback loop", whereby more consistent and more fully explained feedback is provided to the private sector on suspicious transactions reports. Further developing communications channels where the private sector receives feedback on thematic cases or information on targeted areas of focus would help provide clarity on regulatory expectations (paragraphs 23-28 of Annex-2). Countries could also consider developing specific engagement programmes with sectors that appear vulnerable to ML/TF threats (paragraph 31 of Annex-2).

92. Lack of guidance and feedback by public sector authorities may also impede or discourage information sharing between different private sector entities, or between private and public sectors, and vice versa, e.g. because regulatory expectations are unclear or because there is insufficient information available about risks. The public sector should clearly communicate via guidance and feedback the mechanisms that should be put in place to share information in this context. Countries should also consider publishing information on the existing legal mechanisms, gateways and permissions, which permit financial institutions to share information, both group-wide and across financial institutions. This will provide greater clarity and assurance, and promote a consistent understanding across the private sector.

CONCLUSIONS

93. An effective system of national coordination and cooperation and international cooperation hinges on how well different stakeholders, both in the public and private sector interact and engage with one another and exchange information, intelligence and analysis.

94. Legal constraints such as different legal frameworks of data protection and privacy and their implementation, financial institution secrecy provisions and operational challenges may impede information sharing in group wide context as well between financial institutions not part of the same group. With the rapidly evolving threat and risk scenario, especially regarding terrorism financing, it is vital that appropriate solutions to barriers to information are devised by national authorities and also the private sector in a coherent manner. These measures may include authorities (for example, AML/CFT authorities and data protection and privacy authorities) engaging with one other, wherever appropriate to arrive at a shared ground. This engagement can also identify areas where there is a lack of clarity or divergent views between the public sector and private sector. Clarity and guidance on such issues may help facilitate an efficient application of obligations.

95. AML/CFT and data protection and privacy, are both significant public interests. National legal regimes should facilitate both, so as to prevent money laundering, terrorist and proliferation financing, and other financial crimes in a way that pays sufficient regard to individuals' rights to privacy and data protection, while providing a legally certain regime for financial institutions which ensures that AML/CFT and data protection laws do not cut across one another. It is incumbent that national authorities responsible for AML/CFT and data protection recognize derogations in law when necessary to prevent conflicts, and provide clear and consistent guidance to the private sector to prevent misunderstandings or conservative approaches to information sharing for AML/CFT purposes.

96. The private sector is an important partner in combatting ML/TF and holds valuable information which is of critical importance to law enforcement and other competent authorities. Effective and timely exchange of such information helps law enforcement in pursuing its objectives. Furthermore, it is a two-way relationship between the public and the private sector, and this can be achieved if there are appropriate mechanisms for sharing of strategic, operational, tactical and targeted information by law enforcement with the private sector as well. Building of networks, an environment of trust and ongoing dialogue between authorities and the private sector may help achieve a positive outcome in this regard.

ANNEX-1 – DIFFERENCE IN DPP REGIMES AND THEIR APPLICATION

1. As stated in section 1 of this guidance, the differences in legal frameworks of DPP laws across jurisdictions, may create implementation challenges, particularly for the private sector, both in the group-wide and inter-institutional context of information sharing. These challenges can emerge due to following specific factors:

i. **Barriers to group-wide sharing of information.** Some jurisdictions treat group-wide sharing of information containing personal data the same as information sharing with third parties. This is because some data protection legislation considers other subsidiaries or branches as third parties resulting in sharing restrictions. This may also apply to group-wide offices across jurisdictions where such transfer is also made subject to sharing restrictions. This impacts group-level information sharing for AML/CFT risk mitigation purposes among subsidiaries and their head office and parent companies. For global firms, different regional and jurisdictional levels of data protection requirements are often cited as being significant as they limit the free flow of information within the firm.

ii. Principle of data minimisation under DPP framework requires that an organisation should only process the personal data that it actually needs to process in order to achieve its processing purposes, which are not defined in sufficiently clear and specific manner. It often leads to ambiguity on legality of information sharing. When personal data processing is required under domestic AML/CFT framework, ambiguity arises when the law does not prescribe the obligation to process personal data in sufficiently clear way, more particularly due to lack of regulatory guidance on the purposes for which such data can be collected, processed and shared. National data authorities in some instances are currently working on developing a compliance framework that will take into account the issue of group-wide data sharing.

iii. **Processing of personal data** occurs at all financial institutions at account opening for customer due diligence purposes and thereafter as customers engage in transactions for business accounting and risk mitigation purposes, including AML/CFT. In certain jurisdictions, the processing of personal data requires specific and explicit consent of customers, depending on the type of information concerned. In such cases, it is required that consent should be freely given, specific, informed and explicit indication of the individual's wish to agree to the processing of his or her personal data, as expressed either by a statement or by a clear affirmative action. Consent, where required, also applies to transfer of data. It leads to uncertainty, whether there can be a general consent obtained by the financial institutions at the time of on boarding customers or a more specific consent is needed each time the data is processed by the financial institutions. Furthermore, there may also be an absolute prohibition in certain jurisdictions on transfer of personal data (or some of such data) even in situations where the customer consents. It can be challenging for financial institutions to rely upon general consents or public interest exemptions to transfer customer data for the purposes of combatting financial crime. Express legislative provisions or guidance defining the circumstances in which customer data can be transferred across jurisdictions for such purposes can help facilitate information sharing.

iv. **In some cases, transfer of personal data to third countries is prohibited** unless the data protection authorities of the home country confirms that information sent to the third

country will be subject to satisfactory levels of data protection, using some safeguards (for instance, for transfers of data within the group, the use of Binding Corporate Rules may be approved by such authority). The absence of such a determination may affect the information exchange. While such legislation provides the derogations on grounds of public interest, often these grounds are stated to be available only for case-by-case data transfer and not for systematic transfers of information, which may require a specific legal framework. The timely flow of information in a seamless manner may be impeded by requirements to give prior notification to national data protection authorities and obtain multiple authorisations, which has an impact on information sharing.

v. **When beneficial owners are included in the business relationship of financial institutions, the access to information concerning beneficial owners may be hindered when the financial institution or affiliates may be located in jurisdictions which do not allow processing such information.** Therefore, in such cases, the financial institution may be unable to obtain the beneficial owner's consent, where required, to the collection, processing, or sharing of their personal information. This may lead to conflicts between DPP and AML/CFT requirements, and in practice means financial institutions face additional problems sharing beneficial ownership information. At a group -wide level, this may impede the ability of financial institutions to detect any abnormal patterns by establishing linkages and connections (e.g. transactions between two or more companies with the same beneficial owner), and hinder identification of suspicious patterns of activity. This may pose additional problems in many cases as the beneficial owner's identity is generally disclosed by a third party (representative of a legal entity), or is obtained and held by the financial institution itself, without the beneficial owner coming into the picture. Obtaining specific consent in these cases is often stated to be challenging.

vi. **Implementation of the requirement to apply additional measures to family members and close associates of PEPs** in a way that is compatible with data protection principles is not easy. Gathering identification details from various data sources, including information on known relationships between customers (such as family members, close associates etc.) may be considered challenging due to data protection and privacy concerns. For instance, the fact of the PEP being an important official of a certain political party, or a same-sex partner of PEP, would reveal political opinions or sexual orientation. Both are considered sensitive data, and as such the processing of those personal data for one or more specified purposes may be prohibited unless the data subject has given explicit consent to it or for reasons of substantial public interest. This, however, does not prevent financial institutions to obtain such information directly from customers or through public sources. In this respect, it should be recalled that financial institutions should have appropriate risk management systems and take reasonable measures to determine whether the customer or the beneficial owner is a politically exposed person. This requirement should apply to family members or close associated of PEPs.

vii. **The right of anonymity and to data deletion may limit the period of record-keeping requirements and their availability for ML/TF investigations.** Customer and transaction records are required to be kept for a minimum period of five years as per the FATF Standards. Data protection laws may have maximum retention periods that are shorter than the minimum retention periods provided under the FATF standards. In some jurisdictions, there remains uncertainty as to how data retention requirements interact with data protection laws and the "right to be forgotten/right of anonymity" that exists as a corollary of right to data protection.

ANNEX-2 – SELECTED EXAMPLES AND PRACTICES

2. This section highlights country examples on constructive engagement between AML/CFT and DPP authorities, and other practices to promote information sharing within financial institutions, between the public and private sector and among the financial institutions. Country examples are presented for information and meant to be illustrative only. Their inclusion in this guidance does not amount to an endorsement by FATF. This section builds upon the information contained in Section 3 of the TF Risk Indicator Report and contains additional practices and examples provided by countries. These practices and examples relate to the following broad areas:

A. Interplay between AML/CFT and data protection frameworks.

3. Some countries have issued guidance to financial institutions to ensure that they are able to reconcile and comply with the regulatory expectations contained in the two types of legislations. In some countries AML/CFT supervisory authorities also meet and consult with each other to better articulate their respective regulatory objectives. Such dialogue happens prior to rule making by the data protection and privacy authorities and also on an ongoing basis, with a view to provide further guidance and responses to frequently asked questions (FAQs). Creation of working groups between supervisory authorities, data protection authorities and regulators, FIUs and financial services to ensure a coordinated approach and consistent guidance on respective regulatory requirements

France

Each instruction, guideline or position of the French supervisory authority in the field of AML/CFT should, prior to its adoption and its publication, receive an opinion of an advisory committee called the Consultative Commission Anti-Money Laundering and Terrorism Financing (CCLCBFT) which has been set up by the board of the supervisory authority. The French Treasury Department, as well as the French Financial Intelligence Unit and other concerned authorities, including the French data protection and civil liberties' authority (the CNIL - Commission for Data Protection and Liberties), are invited to participate to meetings of the CCLCBFT. It was especially the case when the French supervisory authority issued guidelines on exchange of information within a financial group and outside the group.

Moreover, the CNIL shall also issue opinions on the government's draft legislation that will impact data protection or create new files in matter of ML/TF. Finally, from 2005, the French DPP authority has adopted a single authorisation (general standard) in cooperation with public authorities and private sector representatives. The single authorisation is regularly updated. The aim is to find a balance on the implementation of AML/CFT measures and the data protection requirements for a harmonised and more comprehensible framework by the concerned parties. Furthermore, this single authorisation is also a tool for simplification; nearly 1800 organisations have notified a commitment of compliance using this framework. Besides this single authorisation permits the sharing of customer data under conditions with competent French legal authorities in charge of the fight against ML/TF.

4. In many cases data protection and privacy authorities are also consulted and invited to provide specific comments on AML/CFT measures to avoid any potential conflict and uncertainty between the two regulatory provisions. Data protection and privacy authorities are also encouraged to consult with AML/CFT authorities in development of measures. Such practices foster and develop

an environment of collaborative partnership between the two authorities and reinforce the point that their policy goals and objectives are not necessarily mutually exclusive.

Canada

DPP authorities and AML/CFT authorities routinely work together prior to the drafting of relevant legislation. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal private-sector privacy law. The Office of the Privacy Commissioner of Canada has posted guidance on its website, "Privacy and PCMLTFA: How to balance your customers' privacy rights and your organisation's anti- money laundering and anti-terrorist financing reporting requirements. There is also a set of Questions and Answers, developed with input from FINTRAC.[16] The guidance acknowledges that the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) requires organisations subject to the Act to undertake certain compliance activities, such as client identification and record keeping activities. In addition, certain transactions are required to be reported to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). It further states that the Office of the Privacy Commissioner of Canada supports efforts to combat money laundering and terrorist financing and that programmes or initiatives should be implemented in a manner that is privacy sensitive and consistent with privacy laws.

5. In some cases, data protection authorities are part of the AML/CFT institutional framework and are directly involved in the AML/CFT rule-making process. The close interaction and involvement of agencies helps better coordination and appreciation of different perspectives.

Spain

The main co-ordination mechanism for developing and co-ordinating Spain's AML/CFT policies is the Commission for the Prevention of Money Laundering and Monetary Offences. It is comprised of over 20 key agencies, including the Spanish Data Protection Agency. One of the main functions of the Commission is issuing an opinion on draft legal provisions regulating matters related to the prevention of money laundering and terrorist financing. This high level co-ordination has permitted to adopt legislation where there are waivers of the rules laid down in the Data Protection Law.

6. In certain jurisdictions, the data protection legislation provides for certain derogations and carve-outs which may be necessary to comply with obligations imposed by other legislation. This may relate to the restrictions on the right of access of the data subject, right to obtain consent, prior notification, right to be forgotten etc. These derogations are aimed at balancing security and privacy concerns. National authorities can consider providing more guidance in these areas, if found appropriate. In the European Union (EU) context, work on harmonising the European data protection Rules is underway.

[16] See the Office of the Privacy Commissioner of Canada

European Union

In the EU context, the EU General Data Protection Regulation (GDPR) was adopted at the EU level on April 14, 2016 and will be directly applied in all EU countries. It replaces EU and national data protection legislation. This will become applicable on May 25, 2018. It is a further step towards the harmonisation of European data protection rules. The GDPR considers location data, IP addresses and online identifiers personal data in most cases; as this data could be used to identify individuals, in particular when combined with unique identifiers. The GDPR has also introduced additional transfer tools (codes of conduct and certifications) in order to facilitate exchange of information.

Italy

Domestic legislation provides clear gateways for the processing and sharing of personal data for the purposes of compliance with the AML/CFT laws and regulations. In some instances, for further clarity, national data protection authorities have issued a general order on AML measures on group-wide communications, which facilitates group-wide data sharing in financial intermediaries. The consent from the data subject is not required in such cases.

7. In certain jurisdictions, financial institutions are enabled to share customer information through specific exemptions under the data protection legislation and by lifting restrictions on sharing of information for the purposes of AML/CFT. Financial institutions should carefully consider all such derogations while making a determination on their own procedures and practices with regard to sharing of information.

Singapore

The exchange of customer information between financial institutions is subject to Singapore's Banking Act and Trust Companies Act, which supersede the general data protection provisions laid out in the Personal Data Protection Act (PDPA). Financial confidentiality provisions under the Banking Act and Trust Companies Acts are lifted for the combatting of money laundering and terrorist financing (e.g. for compliance with requests made by a parent supervisory authority, internal audits, or risk management purposes by head-offices). Further, the PDPA requirements are also lifted and financial institutions are also required to share information with their head offices and their branches and subsidiaries within the financial group under the MAS AML/CFT Notices, where necessary for money laundering and terrorism-financing risk management purposes.

B. Group-wide Information sharing

8. Sharing of STRs by a subsidiary or branch of a financial institution with its head office complements the group-wide risk management processes and discharge of oversight responsibilities by head office. Moreover, further sharing of STRs within the group also promotes a more effective internal control procedures and risk management. This is specifically allowed in certain jurisdictions, subject to appropriate confidentiality controls.

USA

In January 2006, FinCEN and federal banking agencies (OCC, FRB, FDIC and OTS) determined that a U.S. branch or agency of a foreign bank may share a SAR with its head office. The January 2006 Guidance also stated that a U.S. bank or savings association may share a SAR with its controlling company (whether domestic or foreign). The sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including overseas) promotes compliance with the applicable requirements of the Bank Secrecy Act (main AML/CFT law) by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a depository institution's compliance with applicable laws and regulations.

Further, in November 2010, the joint guidance issued by FinCEN and federal banking agencies provided that a depository institution that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate, provided the affiliate is subject to a SAR regulation. The sharing of SARs with such affiliates facilitates the identification of suspicious transactions taking place through the depository institution's affiliates that are subject to a SAR rule.

France

Article L. 561-20 of the French monetary and financial code authorises exchange of information in this context. Furthermore, financial institutions have to fill in -on a yearly basis- an AML/CFT questionnaire including legal obstacles that they met in the area of information exchange with their branches or subsidiaries. In such situations, the foreign laws and regulations that prohibit/hinder a financial institution to implement equivalent AML/CFT measures in their branches and subsidiaries abroad must be sent by the REs to the French supervisory authority. The FIU must be also informed of these difficulties by the REs.

9. In some financial groups, analysis of suspicious information shared with group compliance is conducted by a monitoring and analysis centre, which is established centrally within a financial group to consolidate its focus on suspicious customers and to reduce the number of access points so as to prevent information from leaking. Such a centre can take prompt actions on different circumstances of suspicious transactions and alert other departments through their group system, which aims to prevent the customers from having exposure in more than one location or aspects of the flow of transactions or funds that affect operations in the relevant jurisdictions.

C. Information sharing between financial institutions not part of the same group

10. Timely and spontaneous sharing of relevant information by financial institutions more generally among one another with sufficient safe harbour provisions and protection from legal repercussions may help fight ML/TF more effectively, reinforce the integrity of the financial system and prevent its abuse by criminals. It also has the ability to provide better and more comprehensive intelligence to law enforcement authorities. In some jurisdictions, there are specific legislative enablers and safe harbour provisions to facilitate such sharing of information among the financial institutions which are part of the framework.

USA

Section 314(b) of the USA PATRIOT ACT (Information sharing Between Financial Institutions) provides that two or more financial institutions and any association of financial institutions may share information with one another regarding individuals, entities, organisations, and countries suspected of possible terrorist or money laundering activities. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities shall not be liable to any person under any law or regulation of the US, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the disclosure.

11. In some countries, exchange of information between two financial institutions which do not belong to the same financial group is permitted if some criteria are met.

France and Romania

In France, exchange of information between two financial institutions which do not belong to the same financial group is permitted if some criteria are met (Art. L. 561-21 of the financial and monetary code). Among these conditions, financial institutions are required to ensure that their counterpart applies AML/CFT measures consistent with the French requirements implementing the *FATF Recommendations.*

In Romania, Article 25 (4) of the AML/CFT Romanian Law permits financial institutions to exchange information with another financial institution. In particular, paragraph (b) permits credit and financial institutions to exchange information subject to secrecy when they (1) are within the same group, (2) are situated in the EU, the EEA or a third state which imposes similar AML/CFT requirements (3) apply CDD and record-keeping measures which are equivalent to those under the AML/CFT Law and (3) are subject to AML/CFT supervision. Credit and financial institutions may also exchange information subject to secrecy, even when they are not within the same financial group, if (1) they are situated in the EU, the EEA or a third state which imposes similar AML/CFT requirements (2) the information relates to the same client and transaction (3) they are within the same business category (4) are subject to similar secrecy and protection of data requirements.

12. Specific bilateral arrangements to facilitate information sharing among financial institutions for AML/CFT purposes have been reached between some jurisdictions. It highlights the importance of mitigating specific national/regional ML/TF risks through the mechanism of bilateral or multilateral arrangements.

USA and Mexico

Ongoing efforts have taken place between the U.S. and Mexico to jointly increase financial transparency and to prevent ML/TF in the context of correspondent banking.

As part of on-going monitoring requirements, US banks are required to monitor all transactions

when they are an intermediary financial institution and file STRs as appropriate. US banks regularly send Requests for Information (RFIs) to respondent institutions to request additional information related to an unusual transaction. This is intended to clear alerts rather than file STRs. Due to the Mexican bank secrecy provisions and Data Privacy Law, Mexican banks could not respond, which could result in more STRs and termination of respondent accounts. Mexican banks inability to respond to U.S. banks' RFI may result in U.S bank filing of STRs and potentially terminating the correspondent account. In order to address this, in December 2014 the Mexican AML/CFT General Provisions applicable to banks were amended to allow, for the first time, the possibility of Mexican banks sharing information with foreign banks, for AML and CFT purposes.

Specifically, the Mexican government amended its AML/CFT General Provisions applicable to banks and has set in place a legal mechanism by which Mexican banks can share information of their clients and occasional customers, as well as of their transactions with foreign banks, exclusively for AML/CFT purposes. Pursuant to the Mexican Credit Institutions Law, banks shall treat their clients' and occasional customers' information as confidential. Banks are therefore forbidden from divulging the transactional history, or personal data of their clients' or occasional customers' to anyone but the account holders, beneficiaries, trustees, creditors or legal representatives. As an exception, banks shall provide said information if requested by: (i) a Judge through a subpoena; (ii) the Attorney General's office; (iii) the Military Attorney General's office; (iv) the Ministry of Finance authorities for AML/CFT or tax purposes, or (v) the federal oversight authority. Likewise, banks may share the relevant information with other banks for AML/CFT purposes, regarding their clients' and occasional customers' information, as well as of their transactions.

Prior to starting the sharing such information, the Mexican Ministry of Finance has to approve the foreign banks. Likewise, before Mexican and foreign banks begin to exchange information, they have to convene in writing the confidentiality of the information, as well as to state the information and positions of the individual officers authorised to conduct the exchange. Such agreement has to be filed before the National Banking and Securities Commission.

U.S. and Mexican authorities and banks jointly developed the questionnaire currently used as a template for the information sharing mechanism. In this regard, before or at the time of sharing information, Mexican banks shall provide the authorities copy of the information shared and relevant data thereof.

With this mechanism, Mexican banks can now share information with non US banks as well, subject to the same protocols.

13. In other cases, countries have mandated financial institutions to share specific information on certain financial transactions through centralized databases operated by such institutions or a financial authority, and take that information into account as part of the risk assessment that such institutions must carry out on their customers.

Mexico

In 2017, based on the same rationale as that related to credit bureaus, an AML/CFT regulation was issued to mandate banks to provide to a centralized database operated by the central bank or by such banks certain information on every international wire transfer or domestic wire transfer in foreign currency that they send or receive on behalf of their customers. In addition, under that regulation, banks are obligated to obtain from the database certain aggregate information of the wire

transfers processed by their customers in the banking system as a whole and take that information into account to carry out the due diligence on their customers that request a wire transfer, and the general risk assessment of them. Customers must consent with their respective banks that they submit and obtain that information from the database. The applicable AML/CFT regulation specifies the information that banks must submit to the database as well as the statistical information that the database will provide to the banks. The central bank has developed this database and banks will be able to exchange the information on their customers transactions at the end of 2017 and in a second stage, banks will have to provide certain KYC information and documents of such customers and check that information in the database.

14. There is a case for exploring how private sector entities could share specific threat information and high risk customer information with one another. In some jurisdictions databases to share STRs and related information have been created to facilitate information sharing among obliged entities, as well as administrative and law enforcement authorities. This facilitates better information sharing, as well as intelligence to assist in decision-making by authorities and the private sector, wherever relevant.

Spain

Article 33 of the Law on the prevention ML/TF permits obliged persons to exchange information relating to the transactions reported to the FIU with the sole purpose of preventing or forestalling transactions related to ML/TF when the characteristics or pattern of the specific case suggest the possibility that, following its rejection, a transaction wholly or partially similar to the latter may be attempted with other obliged persons.

To that end, central data bases can be created to share this information. Obliged persons and the judicial, law enforcement and administrative authorities competent for the prevention or suppression of ML/TF may consult the information contained in the files created. Regarding the obliged entities, access to the data shall be limited to the internal compliance units established by obliged persons.

D. Information sharing between financial institutions and authorities

15. A close relationship between the private and public sector is a critical element of a well-functioning AML/CFT system. The FATF Standards require countries to develop strong legal and operational frameworks to inform the private sector of ML/TF risks and to ensure that the private sector takes ML/TF risks into account in the course of its business. In the TF context, in particular, this may require combining information obtained from reporting entities with contextual and sanitised information from authorities.

Russia

Under the provisions of the Federal law on AML/CFT, a system of cooperation between FIU-Rosfinmonitoring, supervisory body- the Bank of Russia and REs is provided for in cases where there has been a denial in conducting transactions, opening an account or a contract has been terminated. In all such cases REs have to report to the FIU, where information is analysed and then transferred to the Bank of Russia in order to be communicated to the credit institutions and non-credit financial institutions via secured channels. The information received by REs is to be taken

into account by them in conducting risk assessment of their clients thus facilitating determination of relevant level of risk and elaboration of corresponding commensurate risk mitigation measures.

a) Public/Private Partnerships

16. The private sector holds a wealth of data, which can be utilised by the law enforcement for investigative purposes. In some countries, a public-private partnership has been created to foster information exchange between the public and private sector and among financial institutions which are part of that partnership. The objective of such formal or informal platforms is to provide a conducive environment for feedback and guidance between public and private sectors, as well as to share operational intelligence, information on risks and prevent, detect and disrupt possible threats.

Switzerland

Switzerland has different mechanisms or platforms to mutually exchange information with the private sector. In 2010, in the context of the revision of the FATF Standards, the Swiss authorities established a working group with the private sector bodies (ISFIN) to ensure mutual exchange of information in relation to the development of the regulatory framework in the field of AML/CFT. More recently, in the broader context of the interdepartmental coordinating group on combatting ML and FT established in 2013 – that is also responsible for the NRA – an additional contact group with the private sector has been set up. This group encompasses experienced selected AML/CFT experts in different sectors subject to AML/CFT legislation, such as banks, insurances and MVTS. It is established as a permanent platform to exchange views on the evolution, understanding and mitigation of existing and emerging ML/FT risks. It has already identified areas of future work between the public and the private sectors, such as typologies of TF and correspondent banking. This group helps enhance the communication with the private sector and awareness-raising on AML/CFT matters.

Hong Kong, China

The Fraud and Money Laundering Intelligence Taskforce is a public-private intelligence sharing mechanism involving the Hong Kong Police, the Hong Kong Monetary Authority and the banking industry with the aim of improving the detection, prevention and disruption of fraud, money laundering and other types of financial crimes relevant to Hong Kong's economy. Launched in May 2017 under a 12-month pilot project, the taskforce builds on existing levels of informal cooperation and sharing; preparatory meetings have taken place through 2016 to provide a formal structure for banks and competent authorities to improve collective understanding of threats to enhance targeting and intervention activity for law enforcement and better risk management for banks. The taskforce operates at both strategic and operations levels with threat-specific information alerts disseminated to the wider financial sector through a secure platform.

Australia

On 3 March 2017, AUSTRAC launched Fintel Alliance, which brings together government, industry, academia and international partners in collaborative and secure information sharing environment, thereby constituting a holistic approach to discovering, understanding and disrupting serious and organised crime, bribery and corruption and terrorism through the analysis of financial intelligence. The Fintel Alliance membership continues to grow with new applications currently being assessed. As of the end of April 2017, the Fintel Alliance comprises 19 partners including AUSTRAC, the AFP, NSW Police, the ATO, Australian Banks – ANZ, Commonwealth, Macquarie

Bank, National Australia Bank, Westpac, Western Union and PayPal. The UK National Crime Agency has joined the Fintel Alliance, and AUSTRAC is in discussions with other potential international partners.

The Fintel Alliance has established an Operations Hub where Government and industry intelligence analysts work side by side in joint operational projects, sharing information in near real-time. Three projects were undertaken to establish operations:

- examining the Panama Papers;
- identifying and profiling online money mules; and
- enhancing the use of Australian Cyber Online Reporting Network data.

17. These partnerships acknowledge the importance of involving the private sector, not only as a source of information, but also as a recipient for sensitive information and intelligence held by the public sector to better detect potential terrorist financing. Such sharing often happens in a secured environment after proper clearances are obtained, in order to facilitate further data-mining, operational analysis and scanning by the private sector to fill potential intelligence gaps. The engagement must be an ongoing process and not just transactional and driven by particular events, as the private sector should also have an accurate understanding of the constantly changing risk environment to complement the efforts of law enforcement.

Canada

Promoting TF-vigilance and STR Reporting by REs: Immediately after the attacks in Ottawa & Quebec, FINTRAC issued an advisory to REs to highlight the importance of filing STRs that may relate to similar types of TF threats. STR filings increased by 22% in the month of the Ottawa attacks (over 8,700 in October 2014). In addition to issuing reminders following other ISIL related attacks, FINTRAC has also developed and shared relevant TF indicators with REs.

Developing a real partnership with REs and sharing Operational Alerts and Briefs: Over the last few years, FINTRAC has worked closely with major financial institutions in fight against ML/TF. FINTRAC has developed a new line of products which include "Operational Alerts". Its purpose is to provide up-to-date indicators of suspicious financial transactions and high risk factors related to specific methods of ML/TF that are important either because they represent new methods, re-emerging methods or long-standing methods that present a particular challenge. This is intended to operationally support REs in identifying, assessing and mitigating related risks, as well as the reporting of related suspicions to FINTRAC. FINTRAC also developed "Operational Briefs" to provide clarification and guidance on issues that impact the ability of REs to maintain a strong regime of compliance with the Canadian legislation. More specifically, these products are focused on risk and vulnerabilities associated with exploitation for ML/TF, and on meeting STR obligations. FINTRAC is also currently developing a suite of TF-relevant "Operational Alerts" to provide Canadian REs with important contextual knowledge on TF, and attempt to provide indicators/red flags that REs can operationalise and use in their in house transaction monitoring and internal investigative processes, and ultimately increase the volume and quality of TF-related financial intelligence from REs.

18. The private sector is often looking for assistance and more detailed contextual information from the public sector to help interpret the data they already have. This could include, for example,

sharing a list of relevant individuals (i.e. people under monitoring, surveillance or investigation) suspicious behaviour. Such list-based approaches may help in identifying specific transactions and to detect the network or associations of subjects related to those listed. However, sharing lists of subjects is a sensitive issue as preserving the confidentiality of on-going investigations and operations is a priority for law enforcement authorities. This also has the potential to flag such customers as high risk and may lead to suspension or termination of business relationships, without due process of law or consideration, leading to legal challenges. Even if it is not possible to divulge the particular facts of a case, a general indication of the type of activity occurring can assist them to provide actionable financial intelligence. The sharing of indicators provides reporting entities with the ability to better detect suspicious activity and provide more effective STRs to the FIU.

19. The private sector maintain certain non-financial data about a customer for CDD purposes such as Internet Protocol (IP) addresses, mobile phone numbers, email and residential address and real-time geolocation data for online banking users. In combination with information from competent authorities, such information can become useful for law enforcement for detection and investigation purposes.

b) Information sharing in the context of suspicious accounts and transactions

20. Specific safe harbours provisions or specific forums and gateways can allow the sharing of suspicious transaction information, without necessarily the full content of the STR itself. Under strict provisions to protect the confidentiality of the information, those specific gateways can allow better information sharing not only between financial institutions that don't belong to the same group, but also in an inter-agency context. Such specific gateways aim at an effective and timely exchange of such information and helps law enforcement in pursuing its objectives of countering money laundering and terrorist financing.

EU-OF2Cen

EU-OF2Cen initiative is an EU-funded Italian project on internet fraud that now is rolled out at EU level. Its aims to enable the systematic, EU-wide sharing of internet fraud related information between banks and law enforcement services for the prevention of payments to fraudsters and money mules and for the investigation and prosecution of the perpetrators involved. The project is co-funded by the European Commission and supported by several key stakeholders from the banking sector and law enforcement.

21. Collaborating and sharing information, experiences and trends on risk indicators, for example the ones associated with TF, FTFs and small terrorist cells and raising awareness in a proactive manner by authorities helps build the capacity of the private sector. Meaningful results have been achieved through these successful public partnerships at FATF and Egmont group (for example, the recent TF Risk indicator report finalised by FATF, EGMONT bulletin regarding FTFs etc.)

USA

FinCEN's regulations under Section 314(a) of the USA PATRIOT Act enable FinCEN to reach out to more than 43,000 points of contact at more than 22,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering. FinCEN makes these requests for its own analytical and investigative purposes and on behalf of federal, state,

local, and certain foreign (e.g. European Union) law enforcement agencies. Section 314(a) provides lead information only (financial intelligence) and is not a substitute for a subpoena or other legal process, which is typically used following the identification of relevant information to obtain the information for further investigative or evidentiary purposes.

Through an expedited communication system, FinCEN's 314(a) process enables an investigator to provide sensitive investigative lead information directly to reporting entities. FinCEN provides a secure e-mail system to disseminate this sensitive information. Based upon the initial information that the financial institutions provide, the investigative focus quickly zeros in on relevant locations and activities. In addition FinCEN will organise and host information sharing discussions with appropriate financial institutions to issue requests for information pursuant to Section 314(a). This cooperative partnership between the financial community and law enforcement allows disparate bits of information to be identified, centralised and rapidly evaluated.

Furthermore, the Domestic Security Alliance Council, or DSAC, is a security and intelligence-sharing initiative between the FBI, the Department of Homeland Security, and the private sector, including the largest US banks. Created in 2005, DSAC enables an effective two-way flow of vetted information between the FBI and participating members.

European Bankers Alliance initiative

The European Bankers Alliance initiative was launched in 2015, involving leading international financial institutions operating in the EU and Europol. It aims to help financial institutions develop jointly with law enforcement 'red flag' indicators related to human trafficking, to scan their systems for suspicious transactions and then alert the police.

22. Terrorism and TF information, by its nature, is highly sensitive and needs protection. A lack of trust between competent authorities and the private sector may inhibit sharing sensitive data. The public sector has the difficult task of balancing the confidentiality of sensitive operational information and creating awareness of TF risks with stakeholders. This highlights the importance of building a close relationship based on mutual trust and confidence. Strong formal and informal relationships with the private sector can assist in breaking down some of the barriers/delays in accessing information. In certain jurisdictions for example, often individual contacts are maintained by authorities with the money laundering officers of the financial institutions via whom information can be obtained.

UK

The Joint Money Laundering Intelligence Taskforce is a shared endeavour between financial institutions, industry regulators, Government and law enforcement operating in the UK. It was established in February 2015 and is now a permanent part of the UK's response to money laundering and terrorist financing. Its purpose is to provide an environment for the financial sector and government to exchange and analyse intelligence to detect, prevent and disrupt money laundering and wider economic crime threats against the UK. Its work includes strategic information sharing on common money laundering and terrorist financing methodologies, risks and typologies which are developed and shared with the wider financial sector through targeted alerts. It also has a tactical information sharing function which seeks to fill intelligence gaps where suspected laundering crossed multiple financial institutions. This tactical information sharing function is delivered through a co-located operations group, where vetted members of financial institutions meet with law enforcement officers every week to progress enquiries of

mutual interest. This work is underpinned by clear legal framework (provisions of section 7 of the Crime and Courts Act) and formal Information sharing Agreement. Enquiries progressed through this co-located operations group have resulted in arrests, the recovery of criminal funds, changes to banks internal systems and controls and new bank led investigations.

c) Guidance and Feedback

23. It is also important to provide the private sector with guidance and feedback, including to clarify regulatory expectations regarding the implementation of AML/CFT requirements, or to provide feedback on their reporting. For the private sector, this reinforces the need to commit substantial resources to compliance and engagement with law enforcement. Information shared on the emerging trends, patterns of behaviour and threats is vital for the private sector in order to enable them to run or modify their transaction monitoring systems, keeping in view the evolving situation and also to sensitise their frontline staffs who have a direct day to day relationship with customers.

24. Authorities may also discuss and share the types of information and intelligence that are of value to the private sector in identifying suspicious activity. While sanitised case studies and typologies on money laundering and terrorist financing can often be produced by the FIU in the form of an annual report, newsletter or e-bulletin, more detailed versions of case studies or analysis of past pattern can be shared with specific entities though appropriate channels, such as the forums and partnerships noted above. Another useful mechanism used to disseminate case studies and typologies are National Risk Assessments. These assessments are useful in engaging with the private sector at an early stage and in increasing the awareness of specific risks.

25. Information about particular countries which may pose a greater risk of terrorist financing or certain businesses that may pose a heightened security risk can also be shared by authorities with the private sector. In some cases, authorities may provide detailed data analysis on geographical areas concerning borders, logistical or transit areas. In other cases, financial information seized by law enforcement (e.g. bills of lading, receipts, etc.) may be shared with financial institutions, which may then use it to check against records in their own system to identify any relevant suspicious transactions.

France

The French FIU gives feedback to all entities which submit STRs. This opportunity to provide feedback is administered both generally and specifically. General feedback and guidance is provided through conferences, annual reports, participation in the AML Group of the Bankers' or Insurance's Association and compliance meetings with financial institutions. Specific feedback and guidance is given through informal contact with staff in companies, through offering acknowledgement of the receipt of reporting and offering review of reported cases. Furthermore, since the 3rd of June 2016, to organise the sending of information from financial institutions with the aim of reinforcing the fight against TF, the FIU has the power to designate natural or legal persons that might present higher ML/TF risks, which implies that financial institutions shall put in place enhanced CDD measures and special monitoring on these designated transactions or individuals.

Russia

General cooperation with the private sector participants, including for the purposes of improving quality of information sharing with competent authorities and feedback, is conducted regularly through established under the Interagency Commission on AML/CFT Consultative Council where largest financial institutions associations are represented and through established as a working body of the abovementioned Interagency Commission Compliance Council representing particular entities carrying out operations with money and other assets.

26. Guidance, feedback and outreach provide REs with meaningful or "targeted" information with the explicit purpose of helping the private sector provide better suspicious activity reporting. This cycle (or "feedback loop") ultimately leads to even better outreach by the competent authorities to the reporting institutions that further enhance reporting standards. This may also help the private sector needs to build typologies across a number of parameters. This can be carried out keeping in view the sensitivity of the information and the kind of input solicited from the private sector.

China

The People's Bank of China summarised main features of suspicious transactions related to TF, developed TF suspicious transaction monitoring model, and shared this model with key financial institutions and financial institutions in key regions. Use of this model leads to a significant increase of the number of TF related STR reported by financial institutions and leads to several successful investigation and prosecution of TF Crime. A commercial bank successfully screened transactions of one individual related to ISIL. At present, the PBC is making continuous optimisation and adjustment of the model based on practice.

Australia

Regular meetings with relevant private sector institutions– e.g. AUSTRAC engages with private industry through quarterly forums with major reporters and efforts to share information about behaviour patterns.

Romania

The annual report of the Romanian FIU is a strategic analysis product and primarily aims to provide relevant feedback to reporting entities. It shows the FIU's perspective considering its position as collector of information from the entire financial and non-financial system. The material provides a description of the main categories of suspicious financial behavior, based on the information from STRs submitted. Through its partnership with the reporting entities, the FIU seeks to support their need to know: What they should report? What the other entities are reporting from their field? The feedback increases the trust and helps reporting entities regulate the suspicious behavior detection systems. In addition, the reports are relevant to the common effort of the LEAs.

27. Providing feedback on the quality of reporting is vital to ensure that financial institutions develop a sense of ownership and are able to update their systems and procedures. This also facilitates a clear articulation of the supervisory expectations and a better response from the financial institutions to meet those objectives. Guidance, especially when shared with a wider audience is also helpful in developing a good industry practice across the sector.

France

Many FIUs and sector regulators provide such feedback on a regular basis, with a view to improve the quality and quantum of reporting being made by the financial institutions. For example, France provides feedback during bilateral meetings with reporting entities on an annual basis and provides general feedback during industry forums.

Turkey

In Turkey, MASAK regularly meets with compliance officers of the banks in relation to AML/CFT matters which also include terrorist financing risks. In those meetings, compliance officers of banks are informed of the latest developments and the parties exchange ideas with each other.

Australia

Australia provides guidance and feedback on STRs to a number of key stakeholders on a periodic basis. Each quarter the FIU and law enforcement will meet with the four largest banks to discuss compliance issues and provide feedback on STRs. These meetings have resulted in a 300% increase in STRs relating to TF, following targeted outreach on TF risk indicators.

Hong Kong, China

The Joint Financial Intelligence Unit (JFIU) and the Hong Kong Monetary Authority (HKMA) have worked together to increase both the quality and quantity of STRs in the territory. A guidance paper was issued in December 2013 by the HKMA and JFIU providing feedback from thematic examinations (such as specific guidance on quality and consistency of reports) and specific industry training was jointly provided in 2014. Immediately following this work STR volume increased by 14% from 27,328 in 2013 to 31,095 in 2014. In parallel JFIU provides sector wide feedback in annual AML training for all sectors and individually on a needs basis while the HKMA continues to include reviews of STRs made by banks in its on-site work with a focus on quality. General feedback and guidance to private sectors is also provided by JFIU and HKMA, for example through STR quarterly reports promulgated in JFIU's website, conferences and AML/CFT seminars. Specific feedback and guidance is also given through informal contact or ad-hoc meetings with the reporting entities offering views of the reported cases.

28. Feedback from the private sector on drafts of risk profiles and risk indicators may be helpful in order to refine the final product; before they are issued by the authorities as a formal guidance. Some countries have developed a TF platform for this purpose as well as for providing feedback on STRs and share new trends and methods.

29. Information regarding real time incidents needs to be more detailed and specific to enable the private sector to take immediate action. Data held by the private sector can also assist authorities to identify specific threats and to provide real-time information during or after a terrorist incident, for example. However, concrete information relating to specific individuals and events are often subject to restrictions. Practical challenges exist with respect to ongoing or active terrorism or terrorist financing investigations. In some cases, authorities and private sector entities are therefore not able to act in good faith because of legal restrictions, privacy protection or liability issues. Establishing exceptions or protocols should be considered to allow authorities to share information

with the private sector, as needed on an urgent basis, when there is a real-life incident unfolding or where there is actual, or potential for, loss of life.

30. Some countries have developed a separate online portal and other tools for making requests for information from the private sector and for sharing of information in a secured and efficient manner. This ensures that such requests are prioritised and are addressed in a timely manner, especially in matters involving terrorism or terrorist financing, where the objective is to prevent such attacks.

China and Turkey

Online portals for making requests and receiving reports from the private sector and for providing information to the private sector are being used in certain countries (e.g. China - Digital Information Inquiring System) between the public security and the banking sector. In Turkey, MASAK requests the financial data in banks electronically through red network established with each bank and the data imported electronically via red network. The security of data is ensured through adequate safety protocols and authentications.

d) Sector-specific engagement, outreach and guidance

31. Some countries have developed specific engagement programmes with sectors that appear vulnerable to threats, including TF threats. Such sectors may or may not be within the regulated community, but may be important in view of the emerging pattern and analysis. Local authorities and other stakeholders in vulnerable terrorist areas, including the NPO sector may also be involved to collaborate and identify preventive and other measures to address these threats.

France and Switzerland

Reaching out to vulnerable sectors is an important strategy of many jurisdictions in the fight against terrorism and TF. For example, Ministry of Finance (MoF), France communicates with art and antiquities dealers in order to draw their attention to the specific TF risks related to their field of business, especially with regard to ISIS's ongoing financing activities. The MoF has published a guide for NGOs, which invites financial institutions to undertake concrete measures to sensitise their customers to these specific risks (antiques, oil trade with Iraq). Similarly, following the publication of the NRA in Switzerland, the Swiss authorities initiated a dialogue with the art trade sector to discuss the AML/CFT measures applied by this sector. Separate meetings were held with the sector to raise awareness. This included, representatives of a major international auction house involved in the business.

Canada

Outreach to the charitable sector is conducted to advise charities of their legislative obligations and how to protect themselves from terrorist abuse. This includes general guidance on topics related to sound internal governance, accountability procedures and transparent reporting, as well as specific tools such as a checklist on avoiding terrorism abuse and a web page on operating in the international context. Outreach can take on a variety of forms, including a web presence/RSS feed, email distribution lists, webinars and face-to-face meetings.

e) Mechanisms of Information sharing

32. Two-way relationships between the private and public sector are necessary to combat ML/TF. Mechanisms for information sharing can include formal meetings and informal briefings, both at the one-on-one level and with multiple entities. Many countries hold at least a yearly forum or seminar with the private sector to discuss emerging threats, risks and trends. Operational entities such as law enforcement or security agencies are often included to provide practical case examples or specific information on risk. In other cases, discussions on MLTF risks take place as part of the conferences, seminars, and training for reporting entities. Additionally, this outreach may also occur at the initiative of the private sector to enable more expansive discussion of the potential criminal activity.

33. There may also be a case for a having a mechanism or process within a jurisdiction for the private sector to report potential TF transactions or at least those that appear to indicate that a terrorist act may be imminent to law enforcement/security services in near real time. This presupposes that the competent authority has the channel to receive this type of information and can act accordingly. Examples include dedicated telephone "hotlines or a legal obligation on financial institutions to report such cases on an immediate basis rather than within the time-frame of a STR filing obligations.

34. In some cases, specific TF working groups or task forces have been established between the public and private sector. These types of task forces provide a forum for operational collaboration which is instrumental in improving the analysis and investigation functions of all parties involved.

Egypt

The Federation of Egyptian Banks (FEB), established as a non-profit independent entity, connects all Egyptian banks and foreign banks working in Egypt. The objectives are to discuss and share common issues between the members of the federation; this is in addition to giving opinions of draft laws and suggesting amendments of current legislation related to the banking sector.

In 2003 a Compliance Officer Association was created as an initiative of the FEB. All compliance officers of the banks operating in Egypt are members in this association. Regular meetings are held on issues regarding combatting ML/TF. The Central Bank and FIU are always invited to attend these meetings to provide feedback and technical assistance on the issues raised by the compliance officers.

FATF

PRIVATE SECTOR INFORMATION SHARING

The guidance identifies the key challenges that inhibit sharing of information to manage ML/TF risks, both group-wide within financial groups, and between financial institutions which are not part of the same group. It articulates how the FATF standards on information sharing apply and highlights examples of how authorities can facilitate the sharing of information, as well as examples of constructive engagement between the public and the private sectors.

www.fatf-gafi.org | November 2017

Appendix VV:

FATF, *FATF Report: Operational Issues Financial Investigations Guidance* (Paris: FATF, 2012)

FATF

FATF REPORT

Operational Issues Financial Investigations Guidance

June 2012

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

Photocredits coverphoto: ©Thinkstock

TABLE OF CONTENTS

FINANCIAL INVESTIGATIONS GUIDANCE

I. PURPOSE OF THE GUIDANCE

1. During the latest revision of Financial Action Task Force (FATF) standards, greater attention was given to the operational anti-money laundering/countering the financing of terrorism (AML/CFT) framework. One goal was to strengthen the law enforcement standards (Recommendations 30 and 31) to enhance the functions, responsibilities, powers and tools of law enforcement to effectively conduct money laundering (ML), terrorism financing (TF) and asset-tracing investigations. The revised standards now recognise financial investigations as one of the core elements of the FATF's operational and law enforcement Recommendations. This guidance note is not a standard or interpretative note and is only intended to help countries better understand law enforcement's role in the larger AML/CFT context, specifically addressing the role of financial investigations. The intention of this guidance note is to assist policy makers as well as practitioners by providing ideas and concepts that they can incorporate into their AML/CFT frameworks that might lead to more effective financial investigations. These ideas can go beyond the scope of the standards but are intended to provide examples of ways in which countries conduct financial investigations. As an added benefit, the guidance can also be useful to future AML/CFT assessments and could assist countries in improving the effectiveness of the operational AML/CFT regime.

2. The term *financial investigation*, for the purpose of this guidance note, means an enquiry into the financial affairs related to criminal conduct. The major goal of a financial investigation is to identify and document the movement of money during the course of criminal activity. The link between the origins of the money, beneficiaries, when the money is received and where it is stored or deposited can provide information about and proof of criminal activity.[1] By identifying the extent of criminal networks, the scale of criminality, by tracing proceeds of crime, terrorist funds and other proceeds subject to confiscation and by developing evidence which can be used in criminal proceedings, the overall effectiveness of a country's AML/CFT regime will be enhanced. This guidance contains overarching concepts, strategies and techniques which are meant to be applicable to different legal systems and different types of operational frameworks and is intended to assist countries on how best to implement the FATF Recommendations associated with conducting financial investigations. This guidance will highlight areas where training and technical assistance for financial investigators and prosecutors[2] can be sought but is not to be viewed as a training manual on financial investigations. Throughout the document references are made to information that provides further detail on financial investigation.[3]

3. Before any of the requirements of the FATF standards can be implemented by operational authorities, a comprehensive legal framework is necessary to underpin these requirements, and the

1 See FATF (2012), Interpretative Note to Recommendation 30, 2nd paragraph.

2 For the purposes of this guidance note the term prosecutor also includes investigative magistrate and investigative judge

3 See also the list of selected sources relating to financial investigation at the end of this document.

use of investigative techniques can only be applied if they are permitted by and within the possibilities of the basic principles of a country's domestic legal system. This guidance will highlight elements of the Palermo Convention[4] which are necessary to implement many of the law enforcement powers and techniques described in this guidance.

STANDARDS RELATED TO LAW ENFORCEMENT

4. The FATF Recommendations are designed to detect illicit financial activity, protect the integrity of financial markets, bring criminals to justice and prevent threats to national security. Law enforcement should seek to prevent, deter and disrupt ML, associated predicate offences, the financing of proliferation of weapons of mass destruction and TF activity. Also, law enforcement should be aiming to deprive criminals of their illicit proceeds and terrorists of the resources needed to finance their activities. For the purposes of this guidance note – which seeks to clarify the role of law enforcement in conducting financial investigations – the following FATF Recommendations are relevant:

5. **National cooperation and coordination:** According to the new standards, each country should have a national policy on anti-money laundering and counter terrorist financing, (Recommendation 2). This policy should be informed by the risks identified, and such policy should be regularly reviewed in order to ensure that it stays accurate and contemporary. Knowledge acquired through financial investigations can be used for risk assessment and monitoring purposes. Countries need a national policy to drive the national agenda for combating money laundering, associated predicate offences, terrorist financing and proliferation. Countries should have formalised co-ordination mechanisms which enable authorities to develop and implement these policies. This should facilitate co-operation, informal and formal, between authorities in general and within law enforcement in particular.

6. **Statistics:** FATF places emphasis on effectiveness, and the collection of data is a necessary element to understand how countries determine the effectiveness of financial investigations. For example, money laundering offences and activities should be pursued criminally using financial investigations, and offenders should be prosecuted and appropriately sanctioned. Recommendation 33 is designed to ensure that effective record-keeping systems are in place for reporting statistically what has been accomplished through ML/TF investigations, prosecutions, convictions, property freezing, seizures and confiscation, along with other relevant data.

7. **ML and TF offences:** Recommendations 3 and 5 are the core Recommendations requiring that money laundering and terrorist financing activities be criminalised as independent criminal offences. To successfully prosecute these offences without a prior financial investigation is extremely difficult. This guidance note is to assist countries to better develop their capacity to conduct a proper financial investigation.

8. **Confiscation and provisional measures:** Recommendations 4 and 38[5] address measures to identify, trace and evaluate property which is subject to confiscation. The Recommendations call for

[4] United Nations (2000).

[5] FATF (2010): A list of selected sources for financial investigation with complete bibliographic information is included at the end of this report.

the use of provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property. The standards recommend that countries initiate appropriate investigative measures.

9. **Responsibilities of law enforcement and investigative authorities:** Recommendation 30 calls on countries to designate criminal investigators to pursue ML and TF offences. New requirements include the need to pursue parallel financial investigations as well as to make use of domestic and international investigative task forces or multidisciplinary teams. Therefore, countries should ensure that their legal framework does not impede the usage of such multi-disciplinary groups. The Interpretative Note to Recommendation 30 applies ***to criminal investigators*** who are responsible for pursuing the criminal violations involving the ML and TF offences. The note also clarifies that law enforcement investigators of designated offences[6] should either be authorised to pursue the investigation of any related ML/TF offences during a parallel investigation or be able to refer the case to another designated agency to follow up with such an investigation. Further, this guidance note also applies not only to those ***competent authorities*** which are not law enforcement authorities per se but also to those authorities which have the responsibility for pursuing financial investigations of predicate offences to the extent that they are exercising functions covered under Recommendation 30. For example, anti-corruption enforcement authorities and tax authorities with enforcement powers may be designated to investigate ML and TF offences arising from or related to corruption or serious tax offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets in accordance with the laws of the jurisdiction. This guidance is also relevant to ***public prosecutors***, especially when their role is to co-ordinate the necessary investigative resources in the field which are required to pursue complex financial investigations and organised crime cases. Prosecutors are often responsible for a variety of tasks associated with the financial investigation and in preparing evidence to support formal charges. While the focus is on creating specialised "financial investigators", all criminal investigators should be trained on the value of financial evidence to support all criminal investigations. Raising awareness should also apply to street level crimes, in addition to long-term investigations, thus requiring changing the dynamics and attitudes of investigators and prosecutors regarding the utility of financial investigations. This guidance should also be useful to ***policy makers*** and those who deliver technical assistance.

10. **Powers of law enforcement and investigative authorities:** Recommendation 31 stresses the need for investigators to have access to all necessary documents. This includes having powers to compel the production of financial records and obtain evidence. The Recommendation is designed to enable the use of a wide range of investigative techniques which include undercover operations, intercepting communications, accessing computer systems and controlled delivery. Section VI of this report addresses these techniques. Specific requirements also include establishment of mechanisms to identify the owner/controller of accounts, including the ability to identify assets without tipping off the owner and to seek and utilise information from the FIU.

11. **International co-operation:** Recommendation 40 calls on countries to establish mechanisms allowing financial investigators to obtain and share information on each other's behalf. Countries are expected to establish mechanisms for investigators to use their powers to assist

6 See FATF (2012), Glossary.

foreign financial investigations. Recommendation 40 states that law enforcement should be allowed to establish and utilise joint investigative teams with law enforcement in other countries and promotes the posting of liaison officers. Some co-operation can be accomplished through bilateral and multilateral arrangements, including memoranda of understanding (MoUs), when needed. Financial investigators are encouraged to strategically include co-operation with non-counterparts as part of financial investigations, indirectly or directly. Recommendation 40 is designed to ensure that information received from other countries is used for investigative and law enforcement purposes and that information received is protected from unauthorised disclosure. Further, the Recommendation advocates that countries establish procedures to allow informal exchanges of information to take place (prior to the submission of a formal request); in essence, advocating the exhausting of all forms of informal co-operation prior to the submission of a mutual legal assistance (MLA) request.

12. **Cash couriers:** The requirements to collect, record and share information related to Recommendation 32 are invaluable when pursuing a financial investigation. In particular, on-going criminal investigations can benefit greatly when it is known that targets or associates have previously filed cross-border cash declarations. These declarations often help investigators establish knowledge and intent in on-going money laundering or criminal investigations. While the main objective of Recommendation 32[7] is to put measures in place to detect the physical cross-border movement of currency and negotiable instruments, a financial investigation is an important follow up component of any Recommendation 32 regime.

OBJECTIVES AND BENEFITS OF FINANCIAL INVESTIGATION

13. Countries should ensure that financial investigations become the cornerstone of **ALL** major proceeds-generating cases and terrorist financing cases and that their key objectives include:

- Identifying proceeds of crime, tracing assets and initiating asset confiscation measures, using temporary measures such as freezing/seizing when appropriate.
- Initiating money laundering investigations when appropriate.
- Uncovering financial and economic structures, disrupting transnational networks and gathering knowledge on crime patterns.

14. A financial investigation involves the collection, collation and analysis of all available information with a view towards assisting in the prosecution of crime and in the deprivation of the proceeds and instrumentalities of crime. Criminals usually like to maintain some degree of control over their assets, and as a result there is usually a "paper trail" that will lead back to the offender. That paper trail can also be followed to identify additional offenders and potentially the location of evidence and instrumentalities used to commit the crimes. The ability of law enforcement agencies to conduct financial investigations and have access to financial and other information is essential to effectively combating ML, associated predicate offences and TF offences. Such investigations will

7 FATF (2005).

often establish the existence of otherwise unknown crimes and assets that have been purchased with proceeds of criminal activity, thus allowing these assets to become subject to confiscation.

15. A financial investigation can be used as an instrument to reveal undiscovered predicate offences and to identify other people or companies. Thus, it is imperative for countries to use financial intelligence upstream and downstream within their value chain. This means that the flow of financial intelligence between regulators, supervisors, FIUs, law enforcement and other competent authorities (the value chain) should be free-flowing to and from all entities in accordance with existing domestic laws, policies and procedures and should be results-driven, not process-driven. If such a fluid system of sharing financial information and intelligence is established, the country will make more effective use of financial data, thus becoming more effective in combating money laundering, terrorist financing and major proceeds-generating offences.

16. Countries should take appropriate measures to protect the human rights of the targets of their investigations. Financial enquiries are often intrusive and result in obtaining private information on an individual. Competent authorities involved in financial investigations must be aware of their country's human rights legislation protecting the right to privacy, along with associated considerations. Investigators should be able to justify such enquiries as proportionate, non-discriminatory, legitimate, accountable and necessary to the investigation being undertaken. As a rule, such measures ensure that the targets of investigation have the right to a fair trial, the presumption of innocence and the protection of property.

II. OPERATIONAL FRAMEWORK

INVESTIGATIVE STRATEGY

17. Financial investigation should be an integral part of an overall crime strategy. Countries should establish a comprehensive policy that sufficiently emphasises financial investigation as an integral part of law enforcement efforts. Clear objectives, dedicated action, sufficient resources, training for investigators and use of the legal tools available in a comprehensive, creative, consistent, and committed manner are all important elements of an effective financial investigation strategy in any country. Countries should take active measures to ensure that financial investigations become a routine part of all law enforcement inquiries related to crime with financial gain.

18. Countries should be proactive in developing effective and efficient strategies to make financial investigations an operational part of their law enforcement efforts. The following are some of the key elements that should be contained in these strategic plans:

- Ensuring support from high-level officials within the country who publicly promote and adopt a national AML/CFT strategy.
- Releasing public statements by high-ranking officials supporting and demonstrating commitment to the national strategy and recognising their accountability.
- Establishing strategic planning working groups to develop an effective policy that incorporates the skills of all relevant agencies into an action plan; these groups include representatives from all relevant agencies and components participating in financial investigations.
- Conducting needs assessments and advocacy in promoting proper allocation of resources.
- Creating specialised investigative units that focus on financial investigations.
- Developing operational initiatives that promote the proactive use of powers to freeze assets.
- Articulating clear objectives for relevant departments and agencies that include effective coordinating structures and accountability.

19. Countries should make it a policy priority to ensure that there are an adequate number of properly trained financial investigators. These financial investigators should be experienced in financial investigation matters involving both domestic laws and international conventions and standards. Countries should create institutional conditions that provide the appropriate environment to carry out financial investigations and to facilitate cooperation by providing the proper legal authority for any involved competent authorities as indicated in Recommendation 31. Financial investigations should be worked in close association with or fully integrated within "normal" or other predicate offence investigations. Ensuring that financial investigative specialised

units can work closely with different competent authorities where specialised knowledge and expertise is required should be part of "standard operating procedures."

20. Countries should establish a strategic approach to financial investigations and consider implementing programmes whereby agencies, such as confiscation agencies, certain law enforcement agencies or financial intelligence units (FIUs), are reimbursed costs incurred on financial investigations with asset recovery actions such as the hiring of experts, translation costs, international travel, etc.

PARALLEL INVESTIGATIONS

21. Parallel investigations represent, in relation to financial investigations, focusing on the predicate offence and the money laundering offence simultaneously. In relation to terrorism investigations, parallel investigations focus on the terrorism offences and terrorist financing offence at the same time.[8] Recommendation 30 states that, for all money laundering, associated predicate offences and terrorist financing, law enforcement authorities should develop a proactive parallel investigation. The concept of having parallel investigations brings together expertise from both investigative backgrounds which is complementary and ensures offences are fully investigated.

22. Conducting a parallel financial investigation of the predicate offence is being proactive, as it identifies the proceeds of the crimes currently under investigation for seizure/restraint. It therefore ensures that the assets will not dissipate/disappear and prevents the infiltration of illegal profits into the legal economy, thereby removing the instrument for committing future crimes. The practice thus contributes to upholding the principle in both law and society that no person should benefit from crime.

23. Financial investigations are data intensive. Specifically, they involve records, such as bank account information, which point to the movement of money. Any record that pertains to or shows the paper trail of events involving money is important. The major goal in a financial investigation is to identify and document the movement of money during the course of the commission of an offence. The link between where the money comes from, who receives it, when it is received, and where it is stored or deposited can provide proof of criminal activity. Financial information can also assist the parallel investigation into the predicate offences by:

- Identifying motives, associations and links to people and places.
- Identifying the use of other services such as phones, transport and amenities relevant to the case.
- Locating or identifying suspects, witnesses or victims.
- Providing information on a suspect's movements (proactive, covert use of financial information).
- Providing information to address the issue of prolific and priority offenders where no previous method has been successful.
- Tracing persons.

8 See Section III on terrorist financing.

24. For many major proceeds-generating offences, money laundering is simply the by-product of criminal activity. After the criminal receives the proceeds of the crime, he/she usually wants to do something with these proceeds. The ability to follow the paper trail allows the full development of the facts and circumstances involved in the case to be shown in a logical and sequential pattern, and simplifies the understanding of how the financial pieces fits together. Parallel investigations ensure competent authorities uncover and identify all of the participants in a criminal enterprise. A parallel financial investigation provides insight into the hierarchy of criminal organisations, exposing them to possible prosecution.

25. Information, intelligence[9] and evidence obtained during parallel investigations can be shared and resources can be effectively used to avoid duplication of services. For example, a predicate offence investigation may be utilising the interception of communication to collect information/evidence not only of a predicate offence but also of the associated money laundering offence; this information could then be used in seizure/restraint and forfeiture orders. A financial investigation enhances and corroborates a predicate offence investigation, as it shows lifestyle, unexplained wealth and, depending on the country, can be used as indirect proof (inferred by the courts) as the only explanation that the wealth is from illegal activity, thereby helping to establish sufficient evidence to prosecute a person on criminal charges for both predicate and related money laundering offence. This will form the basis for seizure and forfeiture and can be accomplished through the collation and presentation of either direct or circumstantial evidence. Thus, financial investigations help to target the top echelon of a criminal organisation.

26. Countries should consider including in their standard operating procedures for investigative agencies some form of checklist or outline of the essential elements for conducting financial investigations. This can help structure each financial investigation and be used as a guideline for investigators.

MULTI-DISCIPLINARY GROUPS OR TASK FORCES

27. Particularly in large, complex financial investigations, it is important to assemble a multi-disciplinary group or task force to ensure the effective handling of the investigation, prosecution and eventual confiscation. There should be a strategic approach to intra-agency and inter-agency co-operation in an effort to support information/intelligence sharing within and between agencies and with foreign counterparts.

28. Multi-disciplinary groups may comprise a range of individuals, including specialised financial investigators, experts in financial analysis, forensic accountants, forensic computer specialists, prosecutors, and asset managers. Experts may be appointed or seconded from other agencies, such as a regulatory authority, the FIU, a tax authority, an auditing agency, the office of an inspector general, or even drawn from the private sector on an as-needed basis. The multi-disciplinary groups should include individuals with the expertise necessary to analyse significant volumes of financial, banking, business and accounting documents, including wire transfers, financial statements and tax or customs records. They should also include investigators with experience in gathering business

[9] The term *intelligence* in this context includes and focuses on intelligence agencies working on national security matters.

and financial intelligence, identifying complex illegal schemes, following the money trail and using such investigative techniques as undercover operations, intercepting communications, accessing computer systems, and controlled delivery. Multi-disciplinary groups should also consist of criminal investigators who have the necessary knowledge and experience in effectively using traditional investigative techniques. Prosecutors also require similar expertise and experience to effectively present the case in court.

29. After assembling multi-disciplinary a group, it is imperative to have efficient and effective co-ordination between members of the team as well as all agencies involved. The failure of agencies or departments to link information/intelligence often plagues complex financial investigations. Some mechanisms that promote intra-agency and inter-agency co-operation are:

- Establishing information sharing systems whereby all investigative services would be aware of previous or on-going investigations made on the same persons and/or legal entities so as to avoid replication; conducting conflict resolution discussions and promoting cross-fertilisation.
- Establishing policies and procedures that promote the sharing of information/intelligence within intra-agency and inter-agency co-operative frameworks; such policies and procedures should promote the strategic sharing of the necessary information.
- Establishing a process whereby intra-agency or inter-agency disputes are resolved in the best interest of the investigation.
- Competent authorities should consider establishing written agreements such as MoUs or similar agreements to formalise these processes.

30. To enhance the level of expertise in relation to financial investigation within competent authorities, it should be possible to engage experts. In some cases, it may be useful or necessary to appoint experts or consultants who bring technical expertise in financial analysis, forensic accounting and computer forensics. Adequate safeguards should be in place when engaging private entities which minimise the risks of compromising the integrity of investigations.

31. Countries should develop a strategy to enhance co-operation between the public and private sectors beyond their reporting obligations (see Annex). As a source of financial information, the private sector is the owner of its data, has a vested interest in protecting its standing, has the ability and the expertise to process its data and often may be in a better position than law enforcement agencies. Adequate protection of information and right to privacy should also be part of the information exchange done within legal parameters. Thus, information exchange within legal parameters should be enhanced between the sectors to better and more effectively identify activity that may assist law enforcement in conducting financial investigations.

ASSET RECOVERY

32. Successful asset recovery requires a comprehensive plan of action that incorporates a number of important steps and considerations. Competent authorities will need to gather and assess the facts to understand the case, assemble a team, identify key allies, communicate with foreign practitioners (if a foreign nexus is established), grapple with the legal, practical, and

operational challenges and ensure effective case management. Countries should also strategically look at options other than criminal confiscation, such as *non-conviction based* (NCB) or even administrative proceedings.

33. One of the biggest challenges in asset recovery investigations is producing the evidence that links the assets to the criminal activities (*property-based* confiscation) or proving that assets are a benefit derived from an offence committed by the target (*value-based* confiscation). To establish this link investigators must identify and trace assets up to the point where the link with the offence or location of the assets can be determined. To achieve this, countries should consider creating specialised confiscation units, made up of financial investigators and prosecutors to identify and trace assets for the purpose of confiscation. If such an approach is taken, financial investigators dedicated to tracing and confiscating assets must then work closely with their counterparts in pursuing the criminal prosecution. Failure to do so can have negative consequences for the criminal case, and that in turn is likely to affect confiscation efforts.

34. As discussed in the Interpretative Notes to Recommendations 4 and 38, countries should establish mechanisms that will enable their competent authorities to effectively manage and, when necessary, dispose of, property that is frozen or seized or has been confiscated.[10] These mechanisms should be applicable both in the context of domestic proceedings and pursuant to requests from foreign countries.[11] Asset management units should work closely with financial investigators and prosecutors to prevent the confiscation of assets that could be too cost-prohibitive or cumbersome to maintain.

35. Another challenge in asset recovery investigations is the lack of central oversight as each asset recovery case passes through the various stages of the judicial system. A lack of central oversight of the process can result in blockages within the criminal justice pipeline. This can result in each stage of the process becoming fragmented; dealt only in isolation, making it difficult to co-ordinate financial investigation, seizure and confiscation from start to finish. To overcome this, countries should consider the creation and use of a national asset recovery database which records information on each asset recovery case as it passes through the criminal justice system. This allows information to be considered and analysed centrally with all stakeholders uniformly applying a statistical methodology. This should enable the identification of blockages in the process which in turn allows the swift resolution of such issues.

36. Such a database provides a single source of historic information about asset recovery actions for the use of on-going investigations and also facilitates greater understanding and co-operation among competent authorities. Such a system often contributes to better co-ordination, allowing for more assets to be identified, seized and successfully confiscated. A national database is also an important tool because it helps to improve the effectiveness of the asset recovery regime and support a "joined-up" approach to legal and operational processes. Statistics for the purposes of Recommendation 33 may also be retrieved from the database.

10 FATF (2010).

11 See Brun, J.P., *et al* (2011).

REGISTRIES

37. As mentioned in Recommendation 24, countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. Moreover, as mentioned in Recommendation 25, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries that can be obtained or accessed in a timely fashion by the competent authorities. Such accurate and timely information is vital to a financial investigation. Complex financial investigations involving the use of corporate vehicles require imaginative, tenacious and expert investigators. Hence, in order to properly investigate complex cases involving corporate vehicles, countries should provide financial investigators more education, development and training regarding:

- The nature of corporate vehicles around the world and their potential for misuse.
- The most effective investigative skills and techniques for "piercing the corporate veil".

38. In order to facilitate financial investigations, countries could develop and maintain publicly available registries, such as company registries, land registries, and registries of non-profit organisations. If possible, such registries should be centralised and maintained in electronic and real-time format, so that they are searchable and updated at all times. Such a system will speed up the access of financial investigators to necessary information related to identifying, tracing, freezing and subsequently confiscating assets.

39. In order to assist competent authorities in obtaining access to relevant information in financial investigations, certain basic information on legal entities should be maintained in corporate registries.[12] Such basic information must be easily verifiable and unequivocal.[13] Where feasible, the transition of company registry systems from passive recipients of data to more active components in a country's AML/CFT regime is encouraged. Countries are also encouraged to direct more resources to their company registries to ensure that the basic information supplied is compliant with the Recommendations. Registries would benefit from implementing a robust *on-going* fact-checking component (even if based solely on statistically significant random sampling). Those that demonstrate an effective capacity to enforce financial penalties or other punitive measures against noncompliant registered legal entities will contribute to improving the accuracy of data. As a result, financial investigators would have immediate access to high-quality data rather than the outdated often inaccurate information.

40. Countries should make technological investments in their corporate registry systems. If a registry is to become an efficient AML/CFT tool, this development, including the upgrading of resources specifically for this purpose, needs to be planned carefully. A computerised registry is preferable to a paper-based one, and an online registry is preferable to a closed-network.

---

12 See FATF (2012), Interpretative Note to Recommendation 24 - Transparency and Beneficial Ownership of Legal Persons.

13 See US Department of Justice (n.d.)a, for a list of the information that should be maintained.

41. Countries could assign unique identifiers to legal entities incorporated within their jurisdiction. This enables financial investigators to collect evidence from different domestic agencies within the jurisdiction (for example, tax, licensing, or municipal authorities) most efficiently. This is especially pertinent to operational entities, and if the process of receiving a unique identifier is sufficiently streamlined, it may be further applicable to all legal entities in the jurisdiction (including foreign legal entities, which may have only an operational connection or only be administered from that jurisdiction).

42. Documented particulars of a legal entity's organisation, including those details that indicate beneficial ownership and control, copies of all banking documents, as well as all powers granted to non-officers, should be kept at the registered domestic address of the legal entities. This allows law enforcement authorities to find all necessary information in one location. Moreover, such information should be held physically or electronically within the jurisdiction under whose laws it has been created.

III. TERRORIST FINANCING

43. Money laundering and terrorist financing activity appear as interrelated topics; however, nuanced differences exist between these two distinct criminal offences. These differences need to be understood by law enforcement and those who conduct financial investigations. While terrorist organisations may utilise money laundering techniques when raising funds from criminal proceeds, there are certainly many sources and techniques that these groups use in order to raise funds "legitimately" without engaging in illegal activity[14]. Put another way, money laundering is the process of making dirty money appear clean whereas terrorist financing most often involves clean money being utilised for nefarious purposes.

44. Terrorist financiers want to mask their activities from law enforcement authorities. The motivation of the perpetrators is ideology based with the primary goal of advancing the organisations goals or agenda. This includes having access to funds to meet broad organisational requirements including, but not limited to, propaganda, recruitment, travel and acquiring weapons.

45. In the case of a terrorism investigation, a terrorist financing investigation is crucial, as it can identify targets early in a terrorism plot, such as when they set up a safe-house, and it allows more time for investigation and disruption. Terrorist financing should be viewed not only from an evidentiary perspective but, arguably more importantly, from an intelligence standpoint. Terrorist financing investigations can greatly benefit from focusing on the relationships financial information reveals and the intelligence value that can be derived from the associated "non-financial" information such as phone numbers, email addresses, passport numbers, etc. contained in financial documents. Detecting and investigating terrorist activity is significantly enhanced when national security intelligence and financial information are used together. Exploiting this additional intelligence can identify those leads that may otherwise go undetected and help prevent future attacks.

46. In order for a terrorist operation to be conducted there must be a source of funding no matter how big or small. While the sources of funding are only limited by imagination, individuals engaged in terrorist financing can be viewed with more specificity. Financial supporters of terrorist operations may be involved in four distinct but interrelated roles: *donor*, *fundraiser*, *facilitator*, and *operative*. More specific examples of these different interrelated roles will help explain how terrorist financing in practice can occur, but are not to be considered as legal definitions. *Donors* are individuals who, wittingly or unwittingly, support the terrorist organisation's goals through financial contributions and usually exhibit limited interaction with the group beyond monetary support. *Fundraisers* are individuals who actively solicit funds on behalf of the terrorist organisation and are often more engaged in the movement and concealment of money. *Facilitators* are directly associated with terrorist organisation leadership and operatives, often directly involved in promoting the terrorist agenda and knowledgeable of operational plans. Finally, the *operative* is an individual committed to conducting a terrorist attack and, through either funding provided by the terrorist organisation or via self funding, procures the necessary resources to this end.

47. While it is certainly possible for one individual to fulfil all four financial roles (the "lone wolf" example), most often the previously mentioned financial hierarchy is the norm within organised

14 See FATF (2008), for descriptions and examples of how terrorists raise move and use funds.

terrorist's infrastructures. Identifying the financial role that an individual plays within the organisation is the key to focusing investigative strategies in an effort to disrupt terrorist financing activity. In order to be effective, countries should develop legal mechanisms that enable their law enforcement and other competent authorities tasked with investigating terrorist financing to collaborate with their counterparts in the intelligence community. Countries should create an environment whereby these typically two distinct cultures work toward the common goal of disrupting terrorist financing.

48. In the case of terrorist activity (such as a bombing where there will be serious injury and loss of life), investigation of the financing of the operation should be integrated with investigation of the terrorist activity since the financing of an operation is an integral element in the overall activity cycle of a terrorist group. Parallel investigations not only foster relationships between different competent authorities but also encourage working relationships among competent authorities, the financial sector, and financial regulators. These relationships promote a more comprehensive approach in developing capability and financial intelligence that can be useful in tracing terrorist financial trails – not only in post-attack investigations but also during the planning and preparation stage – so as to be able to prevent attacks and work towards a common goal of preserving life. Community, financial sector and competent authorities have knowledge or information that could lead to useful pieces of intelligence. At the same time, the regulatory and competent authorities have the capability to provide the policies and the tools necessary to build that intelligence.

IV. SOURCES OF INFORMATION

49. Financial investigators develop hypotheses and draw conclusions based on available information. A financial investigation combines tried and tested investigative techniques and traditional accounting and auditing practices to investigate the financial affairs of targets of investigations. Facts that are relevant to a financial investigation may be found from a variety of sources. Traditional "fact-finding" is, of course, highly relevant in financial investigations and includes interviews with suspects, searches of residences and/or offices, forensic examination of computer(s), collection and analysis of financial and business records to include bank statements, tax returns, etc.

50. The nature of the hypothesis determines to a large extent the type of information required to prove the merits of the hypothesis. Identifying the type of information needed allows financial investigators to determine where such information is held. Once financial investigators have determined where the required information is held, they should determine the methods and challenges in obtaining the information. Thus, they should develop and implement an action plan that leads to the successful acquisition of the required information and such an action plan could include many of the investigative techniques discussed in this guidance note.

51. After identifying a potential evidence source, the evidence needs to be collected. Regardless of the source, all evidence should be legally obtained; otherwise, unlawfully obtained evidence could jeopardise the success of the prosecution or confiscation. Investigators should be aware of any legal privilege issues while searching for evidence and seek advice from prosecutors or other relevant competent authorities. Moreover, some information may be considered potential *evidence* from a prosecutorial stand-point however be considered sensitive *intelligence* by intelligence agencies. Thus, co-ordination between prosecution and intelligence authorities is required.

DATA SOURCES AND TYPES OF INFORMATION

52. Within each country there will be differences in the way that various types of information can be made available to investigative authorities and this may be influenced by legal requirements including human rights considerations (such as freedom of information and privacy legislation). The producers and owners of the different information and intelligence products will differ between countries. Additionally, access to that information or intelligence and under what circumstances presents a challenge to countries when designing an effective AML/CFT legal and operational framework. Access to and management of sensitive personal data by the competent authorities requires adequate training of staff in order to ensure adherence to data protection laws and laws that protect the right to privacy.

53. This guidance is primarily concerned with examining how information and intelligence are made available in support of financial investigations, prosecutions and the identification of assets for confiscation efforts. In order to conduct financial investigations, law enforcement should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

54. The form of the data will vary considerably and will range from papers/documents to electronic data to physical items. The ownership and control of these data types varies. On the one hand, much of the data law enforcement can access is of a public nature and is freely available to the general population. On the other hand, data related to personal, financial or law enforcement records are protected and are often considered highly sensitive and confidential. Safeguards need to be put in place to ensure that this data is protected from misuse and is being accessed and utilised for legitimate purposes.

55. The sources of information that law enforcement and competent authorities can use in furtherance of financial investigations varies but typically can be found in six different categories:

- **Criminal records and intelligence:** This is law enforcement information related to the subject and/or criminal activity. Information such as previous arrests, indictments, convictions, but also reports of links with known criminals. Criminal information is typically gathered from surveillance, informants, interviews/interrogation and data research, or may be just picked up "on the street" by individual police officers.
- **AML/CFT Disclosures:** In addition to suspicious transaction reports (STRs), this includes other information as required by national legislation such as cash transaction reports, wire transfer reports and other threshold-based declarations or disclosures.
- **Financial Information:** This is information about the financial affairs of entities of interest that helps to understand their nature, resources, structure and capabilities, and it also helps predict future activity and locate assets. This goes beyond the information contained in AML/CFT disclosures and is normally maintained by private third parties. This includes bank accounts, financial accounts, other records of personal or business financial transactions and information collected in the context of meeting customer due diligence (CDD) obligations.
- **Classified information:** Information that is gathered and maintained for national security purposes to include terrorism financing information. Access is typically restricted by law or regulation to particular groups of persons.
- **Open source:** All information that is available through open sources such as the internet, social media, print and electronic media, as well as via registries operated publicly or privately.
- **Regulatory information:** Information that is maintained by regulatory agencies; access is typically restricted to official use only. This category of information could be held by central banks, tax authorities, other revenue collecting agencies, etc.

56. Multi-disciplinary groups or task forces (described in Section II) serve to integrate information from different law enforcement and intelligence sources which had previously been separated by organisational and technical boundaries. In some jurisdictions this requires changes

in laws and regulations or may require formalised agreements such as MoUs. These task forces leverage existing technologies and develop new technologies in order to provide cross-agency integration and analysis of various forms of data. Furthermore, this information is stored in centralised databases so that any future investigation of any new target of a participating task-force agency can be cross-referenced against that historical data.

V. LAW ENFORCEMENT COLLABORATION WITH FINANCIAL INTELLIGENCE UNITS (FIU)

57. Along with intelligence divisions of law enforcement or other competent authorities, FIUs are one of the competent authorities that can initiate or enhance financial investigations. Financial intelligence collected by law enforcement, FIUs, and other competent authorities should be thoroughly manipulated and result in the proactive initiation of financial investigations. A core function of FIUs is to analyse the information it collects and to disseminate the results of this analysis. An FIU's analytical capabilities allow it to develop different intelligence products that can be useful to investigative authorities. As a routine task, FIUs spontaneously (*i.e.,* without being solicited) disseminate intelligence to investigative authorities relating to suspected ML and TF offences. Disseminated information could relate to an existing entity of interest, support an existing investigation, or prompt a proactive investigation based on new information made available to investigative authorities.

FIU AND AML/CFT DISCLOSURES IN FINANCIAL INVESTIGATIONS

58. Effective financial investigations are characterised by extensive law enforcement use of FIU information and exchanges of information and personnel. Investigative authorities should be able to ask the FIU for relevant information they may hold when conducting lawful investigations. FIUs should be able to respond to information requests from competent authorities pursuant to Recommendation 31. Under Interpretative Note to Recommendation 29 the decision on what information an FIU can provide in response to a request from a competent authority should always remain with the FIU.

59. The overarching aim of both the FIU and investigative authorities should seek to work as a *virtual team*, sharing information in appropriate circumstances to support financial investigations. Successful and effective financial investigations can be achieved through obtaining and using the outcomes of FIU financial analysis, as well as proactive sharing of information between the FIU and investigating authorities. Providing an FIU with an information requirement – (such as) detailing information priorities – can assist the FIU in identifying useful information for spontaneous dissemination. Many investigative authorities have seconded personnel working in the FIU, or FIU personnel seconded to investigative authorities, to facilitate co-operation between the FIU and to assist the effective exchange of information. Single points of contact in investigative authorities and FIU can also assist consistent, efficient information exchange.

60. Formal arrangements between investigative authorities and the FIU can be documented in MoUs, memorandum of agreements (MoAs) and standard operating procedures (SOPs). Documenting how competent authorities and FIUs interact and establishing communication channels can provide clarity on the procedures and processes that are required in order to exchange information appropriately. Agreeing on the use of standard electronic reports and request forms that can be securely exchanged between the FIU and investigative authorities can also facilitate efficient exchange of information. When exchanging bulk or structured data in relation to financial investigations (such as computer files with the results of analysis) consideration should also be given on compatibility of software used by competent authorities and the FIU. Some jurisdictions provide their investigative authorities with restricted access to the FIU database. Investigators are able to directly query the FIU database in certain agreed circumstances. Arrangements for

investigator access to the FIU database should take into consideration information handling issues such as confidentiality, human rights, privacy and data protection.

LAW ENFORCEMENT UTILISATION OF AML/CFT DISCLOSURES AND FIU ANALYSIS IN FINANCIAL INVESTIGATIONS

61. While this guidance is not focused on the analysis function of the FIU, FIUs can provide high-quality, useful and timely analysis to law enforcement and other competent authorities. This can only be accomplished through a two-way mechanism between the FIU and recipients of their information which will require feedback from all parties involved.

62. AML/CFT financial disclosures and FIU analysis are considered a particular category and source of information collected as part of a national AML/CFT regime. This information is intended to be available to law enforcement, and in particular, to financial investigators. Reporting entities are required to file AML/CFT disclosures. These disclosures will include suspicious transaction reports (STRs) and other information required by AML/CFT legislation such as cash transaction reports, wire transfers reports and other threshold-based declaration/disclosures and reports made in relation to the physical cross border transportation of currency and bearer negotiable instruments.

63. AML/CFT disclosures constitute a particularly valuable source of information for financial investigations. Given that the main focus is on the use of STRs, the unique nature of this data should be highlighted. In most countries, STR information is used for intelligence purposes and is not used as evidence in court proceedings. In some countries, STR information is directly admissible in court and when such instances occur between these different systems, countries should coordinate and promote the effective use of the information. There are also strict confidentially issues associated with access to and use of this information. It is essential that only appropriately trained and authorised law enforcement officers have access to this information.

64. The national and international frameworks for providing access to FIU/STR information are important in determining how intelligence can be made available to operational authorities and developed into investigative leads or evidence. In order to promote the timely sharing of information, law enforcement authorities can expect to see clear and precise handling instructions from the FIU upon initial dissemination and where possible prior consent to share this information.. Such arrangements could be discussed bilaterally between FIUs in order to address any privacy concerns and to ensure that such information is shared lawfully and appropriately with the competent authorities conducting a lawful financial investigation. However, if such prior consent (also known as third party rule) is required, FIUs should establish mechanisms whereby such consent is obtained in a timely manner. Because of the practical differences among countries, there is no exact model for STR utilisation that would necessarily fit every country. Regardless, countries should consider putting into place mechanisms that allow their investigative authorities prompt delivery of FIU information and analysis in furtherance of their investigations. The procedures for delivery should be clearly delineated and subject to strict safeguards to ensure proper security and use of the information. Any model should have in place monitoring systems while ensuring that the process is free of unnecessary hurdles. In all cases, investigators should handle information in accordance with confidentiality, human rights, privacy and data protection requirements.

ACCESSIBILITY OF FIUS TO ENHANCE FINANCIAL INVESTIGATIONS

65. The objective of this section is to ensure FIUs work with law enforcement agencies and that financial intelligence is promptly available to enhance investigations. Requesting all relevant FIU information should be a basic step in the investigation of any predicate offence and any crimes, which are financially motivated. This should be included in an investigators "checklist." This is one of the reasons why it is essential that law enforcement has timely access to AML/CFT disclosures filed in their country. As stated earlier, this access does not have to be direct but should be prompt so as to facilitate the incorporation of significant and relevant findings and to further active investigations.

66. Information contained in STRs, when checked against operational or historical intelligence databases, can complement existing ML/TF investigations by helping to identify laundered money and money intended for terrorist use. STRs can help investigators connect other pieces of information, provide information on where the proceeds of criminal activity or funds intended for terrorist use are located and when and where these funds are moved, or even what methods are being utilised. STRs are not to be considered as criminal charges and should not be viewed as "criminal activity reports". However, in many cases, the financial activities reported in the STRs are themselves illegal, such as check, credit card or loan fraud, check kiting, counterfeiting, embezzlement and the structuring of transactions to avoid the filing requirement of threshold based reporting.

67. FIUs can enhance investigations by responding to requests by investigative authorities. This information can support existing activity by identifying and locating proceeds of crime and also supply information which can assist in securing convictions and confiscations. The FIU will hold, or have access to its own information and information gathered from 3rd parties (domestic and foreign) that can enhance investigations. Some of this information will be confidential or sensitive and may be restricted in the manner in which it can be shared. These restrictions may be imposed by law or by the 3rd party originator of the information. When receiving information from the FIU, investigators should note the restrictions on the use of information, and, how it can be utilised or "handled", in particular for investigative purposes. It is important that law enforcement personnel handling this information be trained and knowledgeable on the applicable disclosure rules.

REVIEW OF STR INFORMATION AND OTHER AML/CFT DISCLOSURES

68. A financial investigator's understanding is often greatly increased when STR- or disclosure-related information is compared with information from other sources. The real added value of STR information lies in the analysis/assessment (usually in the first instance by the receiving FIU), when STR information is combined with information from other sources, other STR information, other types of transaction reports and open and closed sources of intelligence. The cross reference of STR information with other information available to law enforcement is therefore fundamental for the successful utilisation of STR information in financial investigations. It is essential that law enforcement and the FIU work together to ensure that both parties understand what checks have been conducted and which aspects of the disclosure are the most useful to pursue.

69. A cursory review of the STR information generally includes a selected approach for those STRs that will be assessed and researched on other databases including existing intelligence on

illegal activities, criminal records, on-going investigations, historical investigative reports, and in some cases income tax records. These preliminary investigative steps are part of the process to identify those STRs that merit further investigation and de-confliction of STRs with on-going criminal investigations.

70. The need for efficient utilisation of limited resources is a challenge faced by most investigators. When necessary, STRs should be prioritised based on relative significance and general investigative priorities and strategies for the country. In some countries, where a large number of STRs are generated each month, experienced and sufficiently trained support personnel can be designated to conduct initial reviews. These reviews would identify those STRs of particular interest to law enforcement based on pre-established criteria, e.g., STRs that reflect structuring or illegal money transmitting activity. Such an approach narrows the field of STRs to be reviewed and eliminates from consideration those that investigators may have decided not to pursue. Providing an FIU with an information requirement – (such as) detailing information priorities – can assist the FIU in identifying useful information for spontaneous dissemination. This demonstrates the need for law enforcement and FIUs to share information upstream and downstream allowing for more effective allocation of resources.

71. Concerning other AML/CFT disclosures, such as those described above in the section on data sources and types of information, countries should ensure that such information is readily available to FIUs and the competent authorities conducting lawful financial investigations in accordance with confidentiality, human rights, privacy and data protection requirements.

REVIEW OF CROSS – BORDER CASH DECLARATIONS FOR FINANCIAL INVESTIGATIONS

72. Recommendation 32 calls on jurisdictions to implement measures to detect and prevent the physical cross-border transportation of currency and bearer negotiable instruments, which are one of the main methods used to move illicit funds, launder money and finance terrorism.[15] This collected information can be useful to financial investigations. As a result, such information should be accessed, verified and analysed by competent authorities in furtherance of financial investigations. This analysis can result in the identification of frequent travellers, links between travellers, and the discovery of other evidence or leads. Recommendation 32 requires jurisdictions to ensure that persons who make a false declaration/disclosure and persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments (BNI) related to ML/TF are subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative. In practice, this means that jurisdictions need to be able to investigate and/or prosecute and sanction such conduct.[16]

73. Recommendation 32 calls for sharing of information with the FIU, other domestic partners and international counterparts, subject to strict safeguards to ensure proper use of the data. It is best practice to set out such safeguards in law and co-operation agreements such as MoUs. It should be noted that information sharing and feedback among the FIU, other domestic partners and international counterparts can considerably improve the targeting of illicit cash couriers. It is best

15 See FATF (2005).

16 *Ibid.*

practice to ensure that the information being shared is comprehensive, tailored to the needs of the FIU and law enforcement authorities and includes all recorded data. It is also best practice to ensure that the sharing is takes place in a timely fashion (preferably in real time). Recommendation 32 calls on countries to implement a system that informs the FIU of suspicious cross border transportations incidents or ensures that the FIU has access to information on all cross-border transportations of currency and BNI. The competent authorities conducting financial investigations should routinely access this information in furtherance of their investigations.

74. As mentioned in the FATF Best Practices Paper on detecting and preventing illicit cross-border transportation of cash[17], investigating the reasons why a false or no declaration/disclosure was made may uncover information that may be useful for intelligence purposes, or to support an investigation, prosecution and/or sanction against the traveller.[18] This information could be important for an on-going financial investigation, thus access to such information by the competent authorities should be timely and efficient. Moreover, ML/TF cases can result equally from truthful declarations/disclosures or false declarations/disclosures, and such information can be useful to financial investigators by providing new investigative leads and perhaps evidence.

17 *Ibid.*

18 *Ibid.*

VI. INVESTIGATIVE TECHNIQUES

75. This section describes various investigative techniques that can be used in financial investigations. It is not exhaustive in covering all techniques but only highlights techniques that have specific relevance in relation to financial investigations. Recommendation 31 states that countries should use a wide range of investigative techniques which include undercover operations, intercepting communications, accessing computer systems, and controlled delivery. Countries can implement these requirements within their legal systems. This guidance note recognises that countries may have differing mechanisms available to investigators for compelling records that are relevant to financial investigations. For example, some countries use production orders, subpoenas, orders issued by prosecutors, orders issued by investigative magistrates, etc. Regardless of the instrument or process used, it is important that the financial investigator has access to and effectively uses such powers so as to obtain necessary information.

76. **Physical Surveillance:** This is a useful technique to gain general background and intelligence and information on individuals/businesses, habits and relationships of suspects. Surveillance can be especially useful in financial investigations in cases involving the movement of bulk currency and by identifying "gatekeepers" involved in the development and implementation of ML or TF schemes. Surveillance of targets can often identify where financial and related records might be stored and lead to the discovery of assets. In addition, surveillance can help corroborate financial data and identify other targets and associates.

77. **Trash runs:** (*i.e.,* searching the suspect's discarded trash for evidence): This technique can be an effective way of obtaining leads where assets are maintained, as well as help develop probable cause for more coercive measures and evidence for use at trial. Suspects frequently discard evidence, including financial records and correspondence that may be valuable to a financial investigation.

78. **Compulsory measures to obtain evidence:** These measures, including the use of search warrants and other instruments, should be used to gather evidence of criminal activity that cannot be obtained by other means. The timely use of these powers to obtain evidence minimises the opportunity for suspects to purge records and/or destroy evidence. In addition to seizing paper documentation, investigators should seize and examine computer systems and other electronic data. The execution of these powers should be properly planned and be lawfully conducted in accordance with existing policies and procedures. Moreover, to protect the integrity of evidence, investigators should adhere to the established policies and procedures related to the handling of evidence to include chain-of-custody documentation. If such policies and procedures are not present, countries should develop appropriate policy and procedures that ensure the proper handling of evidence. Adherence to such policies and procedures protects the integrity of evidence as it is introduced into court proceedings. When financial investigators encounter computers or other digital media during the course of an investigation, they should consider the value of the evidence these may contain. In these instances, consulting with a trained computer evidence specialist or technical expert is appropriate. Attempts to access electronic data or transport and store electronic evidence by untrained investigative personnel, without the necessary equipment may result in unintentional tampering and/or permanent lost of valuable evidence. In all instances, original digital evidence should be deposited in an appropriate evidence container and a written chain of evidence should be

prepared at the same time. Analysis of this evidence should be conducted by a computer forensic specialist.

79. **Interviews[19]:** Investigators should use this technique to gather evidence and information in furtherance of their financial investigation. Investigators should first attempt to obtain voluntary statements from suspects and witnesses. However, if suspects or witnesses will not voluntarily submit to an interview, their *testimony* may be compelled in accordance with a country's existing laws, policies and procedures. Such interviews should not commence before careful consideration of the potential negative impact on the investigation by soliciting the suspect's/witness's co-operation. Detailed reports of investigation should be completed to document interview results. Investigators should consider all other legal means of obtaining evidence to corroborate testimony and statements. Interview reports may be invaluable in refreshing investigators and witnesses' recollections of events during criminal or civil proceedings.

80. **Controlled delivery:** This is an effective investigative technique involving the transportation of contraband, currency, or monetary instruments to suspected violator(s) while it is under the direction or surveillance of law enforcement officers. The contraband, currency or monetary instruments may be discovered subsequent to a seizure at the ports of entry or through other investigative means such as undercover operations. Controlled deliveries are conducted to:

- Identify, arrest, and convict violators.
- Disrupt and dismantle criminal organisations engaged in smuggling contraband, currency, or monetary instruments across borders.
- Broaden the scope of an investigation, identify additional and higher level violators, and obtain further evidence.
- Establish evidentiary proof that the suspects were knowingly in possession of contraband or currency.
- Identify the violator's assets for consideration in asset forfeiture.

81. Although controlled delivery can be a successful technique, there are serious risks that should be adequately addressed. For example, there is a risk of losing the evidence during the course of the controlled delivery. Countries should ensure that their competent authorities are properly trained in using this technique, that clear policy and procedural guidelines are established and followed and that proper operational oversight is conducted at the managerial level.

82. **Intercepting communications:** Electronic surveillance techniques, such as electronic intercepts of wire, oral communications, electronic media and the use of tracking devices can be very useful in financial investigations. This technique can help identify co-conspirators, provides insight into the operations of the criminal organisation, provides real time information/evidence that can be acted upon using other investigative techniques and can lead to the discovery of assets, financial records and other evidence.

83. Countries should train their competent authorities to properly intercept communications in furtherance of financial investigations in accordance with the basic principles of their domestic

19 See US Department of Homeland Security (n.d.).

laws, policies and procedures. Countries should ensure that their competent authorities are properly resourced so that such operations are available to the competent authorities as a viable investigative technique. However, intercepting communications is intrusive, coercive and resource intensive measure, thus countries should put in place mechanisms that ensure the usage of this technique is used lawfully, effectively and efficiently.

84. **Undercover operation:** This is an investigative technique that can be effective regarding financial investigations but also has inherent risks. Undercover operations typically allow investigators access to key evidence that cannot be obtained through other means. An undercover operation is an investigative technique in which a law enforcement officer or operative of a law enforcement authority, under the direction of a law enforcement authority, takes action to gain evidence or information. Properly conducting undercover operations often requires substantial resources, extensive training and significant preparatory work. The resources, the unique and diverse required skill sets and the inherent risks typically make utilising this technique a last resort – normally after more traditional investigative techniques have been unsuccessful. The actions performed by law enforcement during undercover operations should be in accordance with the basic principles of existing laws, policies and procedures, and all undercover officers should be highly trained before engaging in such operations.

85. There are various significant factors that should be considered when contemplating the use of an undercover operation. The investigators should determine motive/reliability of informant(s) (if applicable), research applicable laws and policies, conduct background investigation(s) of the potential subjects and determine that an undercover operation will likely yield positive results. The investigators should continuously re-evaluate the need for an undercover operation and be prepared to terminate the operation when appropriate. Resources that are to be employed must also be considered such as the person(s) to be used in undercover capacity, other staff needed to support the operation, equipment needs and plans for locations and estimated expenses. Investigators should also establish termination criteria, secure advice from a prosecutor and obtain the necessary approvals required by the country's laws, regulations and policies.

86. Given the inherent risk with this technique, undercover operations proposals should be *reviewed and authorised* by designated officials from the competent law enforcement authorities. These officials should be knowledgeable on all aspects of undercover operations. Moreover, the proposal should indicate that traditional investigative techniques have been utilised and have been largely unsuccessful and that the undercover operation is likely the only technique available to gather evidence of the suspected criminal activity. Only highly trained undercover agents should be used in undercover operations[20].

87. **Methods of Proving Income:** A key component of financial investigations is the determination of the financial gain or profit derived from the predicate offence. Establishing the amount of the illegal proceeds often supports the motive for the crime and provides circumstantial evidence of the predicate offence. For this reason, it is essential that financial investigators be proficient in the various methods of proving income and determining which method is applicable, based on the facts and circumstances of a particular investigation.

20 See US Department of Homeland Security (n.d.), for more information about undercover operations.

88. This guidance encompasses two general evidentiary ways of proving income. These include using direct evidence, as in the *specific items method*, or circumstantially, as in the three indirect methods of proof: (1) *net worth and expenditures*, (2) *sources and applications* and (3) *bank deposits*. These methods are discussed in more detail in the Annex to this report.

89. While financial investigators are conducting financial criminal analysis using the indirect method of proof, they should be cognizant that all *indirect method* investigations are subject to evidentiary difficulties, which can be addressed by properly completing the following investigative steps:

- Account for all sources of funds such as inheritances, loans and transfers between accounts. Non-income sources need to be identified in order to accurately compute unreported income for serious income tax evasion cases or illicit source income for other predicate offences.
- Address defences raised by the suspect. Indirect methods of proof are based on circumstantial evidence. Any reasonable defence raised by the suspect needs to be investigated in order to determine whether or not it has merit.
- Establish a likely source of income for the understated income in a tax evasion investigation or the predicate offence as a source of the unexplained income.
- The investigator must identify all cheques payable to cash and determine whether or not there are any missing checks, particularly when using the *bank deposit method* of proof. This is because cheques payable to cash and missing cheques should be considered a source of currency deposited, hoarded or spent, unless there is compelling evidence to refute it.

VII. TRAINING

90. Training and education programmes should be standardised within the competent authorities, basic training should be envisaged at entry level, and specialised training on select officers should be conducted at both entry level and throughout the investigator's career. However, such specialisation would differ between the tasks of a financial investigator and those of a financial analyst. Officers on such specialised career paths should be provided career and pay incentives. Basic financial investigative skills should be routinely included in training for entry level police officers and other competent investigators.

91. The training structure should follow operational needs. Formal selection of staff should be followed by formal instruction in the three primary disciplines: financial intelligence, evidence gathering, and asset tracing/freezing. Further training should be given on money laundering investigation, enhanced financial intelligence, criminal confiscation and non-conviction based confiscation. Where possible, the training should be aligned with training for line managers and specialist prosecutors. Moreover, the judiciary should be trained on appropriate laws and how to properly adjudicate on financial investigative matters.

92. Training should not be exclusive to law enforcement but should include those sectors that are required to report suspicious activity and others that may pose a risk. The FATF and FATF-style regional bodies have developed typologies reports describing various ML/TF methods and techniques. This material may also be a useful to include in training on financial investigation.

93. Training may also include multiple jurisdictions in order to share best practices, learn differences in legal procedures and enhance co-operation. Moreover, staff should be vigilant in staying current to new trends and typologies. Countries should encourage their financial investigators to attend regional and international training workshops with their foreign counterparts.

94. Reports are an integral part of financial investigations, thus report writing should be part of the training curriculum for financial investigators and intelligence analysts. The ability to convey concepts, findings and conclusions in a clear, concise and informative manner is essential to the success of complex financial investigations. Countries should dedicate the necessary resources to train their competent authorities properly in the skill of report writing. In financial investigations, report writing takes on an even greater importance because the investigations can be lengthy, complex and multi-jurisdictional. Accurate, timely and concise reports will assist, for example, in drafting the necessary background information to meet evidentiary requirements in domestic court proceedings as well as MLA requests for evidence. It is imperative that practitioners document their findings periodically throughout the entire investigation, as well as after significant events. Reports should be written in a clear and concise manner, preferably on the same day as the event being described, and should include all relevant information and events. They should be reviewed and approved by a supervisor as soon as possible.

95. A sample curriculum of training courses for financial investigators is available[21]. This list and types are not exhaustive but cover many skills required to be a high-quality financial investigator.

21 See (NPIA (National Policing Improvement Agency), n.d. a-g; Golobinek, R., 2006).

VIII. INTERNATIONAL CO-OPERATION

96. Recommendation 40 states that countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international co-operation in relation to money laundering, associated predicate offences and terrorist financing. This guidance note recognises the importance of international co-operation for successful financial investigations. Financial investigations often reach beyond domestic borders; therefore, it is important that competent authorities immediately focus on both formal and informal international co-operation efforts and ensure they are maintained for the duration of the case. Establishing early contact aids practitioners in understanding the foreign legal system and potential challenges, in obtaining additional leads and in forming a common strategy. It also gives the foreign jurisdiction the opportunity to prepare for its role in providing co-operation.

97. There are particular channels for international co-operation which can be used by financial investigators:

- Contact existing liaison officers[22] in or of the foreign jurisdiction.
- Exchange information between national (or regional) police units using channels such as INTERPOL, Europol and other regional law enforcement bodies.
- Inform the national FIU which has a possibility to contact its foreign counterparts and collect further intelligence through the Egmont Secure Web or by other means.
- Through the central authority for transmitting MLA requests to foreign countries.

98. In order to legally obtain evidence that is admissible in court, investigators and/or prosecuting authorities must make use of the applicable international arrangements which may be based on reciprocity, MoUs, bilateral or multilateral arrangements. Once a decision has been taken as to which country has responsibility for prosecuting and/or investigating which part of the case, mechanisms should be agreed ensuring that all relevant evidence can be made available in the competent country in a form that will allow production in a criminal court and which respects due process of law.

99. Forming personal connections with foreign counterparts is also important to successful financial investigations. A telephone call, an e-mail, a videoconference or a face-to-face meeting with foreign counterparts will go a long way to moving the case towards a successful conclusion. Communication is important in all phases: obtaining information and intelligence, making strategic decisions, understanding the foreign jurisdiction's requirements for assistance, drafting MLA requests or following up requests for assistance. It helps reduce delays, particularly where differences in terminology and legal systems may lead to misunderstandings.

---

22 This should include multinational bodies such as EUROJUST (a European agency with some non EU liaison officers) or multinational judicial or police networks that may exist in some regions of the world (in the European Union for instance the European Judicial Network).

100. Some important information can be obtained more quickly and with fewer formalities through direct contact with counterpart law enforcement agencies and financial intelligence units or from liaison magistrates or law enforcement attachés posted locally or regionally (agency-to-agency assistance). Such assistance may lead to a more rapid identification of evidence and assets, confirm the assistance needed and even more importantly provide the proper foundation for a formal MLA request (government-to-government assistance). Such contacts also offer an opportunity to learn about the procedures and systems of the foreign jurisdiction and to assess various options for conducting investigations, prosecutions and proceeds of crime actions.

101. In order to constructively and effectively provide the widest range of international co-operation, it is essential for financial investigators to discuss issues and strategy with foreign counterparts. Such discussions should involve consideration of conducting a joint investigation or providing information to the foreign authorities so that they can conduct their own investigation. If the financial investigation is in the early stages and investigators are concerned about the integrity of the investigation, they can still engage with their foreign counterparts and discuss issues from a "hypothetical" perspective. Such discussions allow all involved parties to get a better understanding of the parameters and requirements of an investigation without having to discuss too many specific details. Such details can be shared at a later stage as necessary.

102. To address the transnational nature of MLAs requests, all countries should be able to investigate, prosecute and bring to judgment cases of ML, associated predicate offences and TF regardless of whether the predicate offence occurred within its jurisdiction or abroad. If the predicate offence was committed in a foreign country, the prosecution of the money laundering offence generally requires some knowledge of the associated predicate offence in the foreign jurisdiction, and such information should be made readily available.

103. In the FATF best practices paper on confiscation[23], mention is made of best practices for countries to help strengthen legal frameworks and ensure that asset tracing and financial investigations can be conducted effectively. These best practices include having appropriate procedures and the legal framework to allow the informal exchange of information, the use of appropriate regional and international bodies to facilitate co-operation, the spontaneous sharing of information with proper safeguards and the entering into of asset sharing agreements.

23 FATF (2010).

ANNEX

ADDITIONAL INFORMATION

BASIC INFORMATION THAT SHOULD BE MAINTAINED IN A CORPORATE REGISTRY

- Entity name (including governmentally unique identifier and alternative names)
- Date of incorporation, formation, or registration
- Entity type (for example, LLC, sociedad anónima)
- Entity status (for example, active, inactive, dissolved—if inactive or dissolved, date of dissolution and historical records of the company)
- Address of the principal office or place of business
- Address of the registered office (if different from principal office) or the name and address of the registered agent
- Particulars of formal positions of control, that is, directors or managers and officers (for example, president, secretary)
    - — If a natural person—their full name, any former name, residential address, nationality, and birth date
    - — If a corporation—the entity name, address of the principal office, address of the registered office, and (if applicable) for foreign corporations, the registered office in its country of origin
- History of filings (for example, formation documents, annual returns, financial filings, change of registered office, change of registered agent, and so on)
- Required annual returns that verify the correctness of each particular required to be filed in the system, even if it has not changed since the last filing date
- To the extent feasible and appropriate, electronic copies of filings and documents associated with the legal entity (for example, formation documents, annual returns, financial filings, change of registered office, change of registered agent, and so on).

ADDITIONAL INFORMATION ON UNDERCOVER OPERATIONS

OPERATION STAFFING AND TRAINING

1. Article 29 (1)(g) of the Palermo convention calls on countries to initiate, develop or improve specific training programs for its law enforcement personnel, including prosecutors, investigating magistrates and customs personnel regarding the use of undercover operations. The number of employees involved with an undercover operation will naturally be dictated by the nature of the operation.

INDIVIDUALS PROPERLY TRAINED IN VARIOUS ROLES ARE NORMALLY INVOLVED IN EVERY UNDERCOVER OPERATION.

2. For example: The *supervisor's* responsibilities include overall management control of the operation and will ensure that the daily activities of the other participants are directed towards the objectives of the operation. A *cover agent* should be assigned at location of the undercover operation to perform on-site liaison with the undercover agent and be primarily responsible for the safety and security of the undercover agent. The *undercover agent* must be trained and is generally brought from another location into the area where the undercover operation will be conducted. They may develop multiple cover identities so that at any given occasion they can work on undercover assignments under each identity. A *tech agent* is a trained technician who is knowledgeable in the installation and operation of audio and video monitoring equipment. The *tech agent* is a regular member of the undercover operation team and should participate in all the periodic review, pre-operational and post operational meetings. The *case agent* will manage the day to day activities of the undercover operation. Other duties of the case agent involve timely reviewing, analyzing, and determining the value of all information or evidence obtained. Typically, the *case agent* is responsible for report writing, documenting evidence, duplicating and storing recordings and other record keeping functions.

CONFIDENTIAL INFORMANTS

3. Undercover operations may be supported by cooperating private individuals (confidential informants) who can play an effective role in the success of an undercover operation. A well-placed cooperating private individual can assist the undercover agent in making contacts with the subject(s) of the operation, and lend credibility to the undercover agent. While the confidential informant is not a member of the investigative team, he or she is often in a fiduciary/controlled status to the law enforcement agency conducting the undercover operation. The confidential informant role is often critical to the undercover operation. However, the appropriate law enforcement personnel should closely monitor all the confidential informant's activities in any undercover operation.

DEVELOPING INFORMATION GATHERED BY AN UNDERCOVER OPERATION

4. In an undercover operation, evidence and information gathered is transmitted to the cover agent by reports of activity prepared by the undercover agent. These reports detail the undercover agent's activities as it relates to the operation. They should contain the names of all people with

whom the undercover agent had contact; and should include a comprehensive summary of the day's events.

5. Another source of information or evidence gathering may come from electronically monitored conversations between the undercover agent and the subject(s). The content of these monitored conversations will not be included in the undercover agent's daily activity reports except for a reference to with whom and at what time the conversation took place.

6. Additional information and evidence can also be obtained by other members of the investigative team and support personnel by such investigative activities as surveillance, public record checks, law enforcement contacts, financial information analyses, etc.

REVIEW AND CONCLUDING THE UNDERCOVER OPERATION

7. It is a good practice to have periodic reviews (*i.e.,* 90 day intervals) of ongoing undercover operations. The participants in this review should include the supervisor, case agent, cover agent and if possible, the undercover agent. This review should address and memorialize the progress of the operation within the stated objectives and any changes in strategy and/or actions needed to realize the goals.

8. The termination of an undercover operation should generally be decided based on facts and circumstances. These include whether the stated objectives have been accomplished, cannot be accomplished or would require expending an unreasonable amount of resources. An undercover operation should also be terminated when the allegations are proven false.

ADDITIONAL INFORMATION ON NET WORTH METHOD COMPUTATION

9. The purpose of a net worth computation is to arrive at taxable or illegal income. The basic computation of net worth is assets less liabilities. The change in net worth is the difference in net worth from period to period, for example one calendar year to the next. Changes in net worth can be the result of purchasing assets, selling assets, reducing liabilities or increasing liabilities. Expenditures are then added to any change in net worth to determine the total amount of funds used by the subject in any given period.

10. A net worth statement (Assets - Liabilities = Net Worth) is similar to a balance sheet in its presentation (Assets - Liabilities = Owner's Equity).

11. The net worth indirect method of proof is a very effective method of determining income amounts derived from illegal activities. There are three basics steps in calculating the illegal income as follows:

12. **Calculate the change in a subject's net worth (assets less liabilities).** Determine the net worth at the beginning and end of a period (a taxable year or years), subtract the beginning period's net worth from the ending period's net worth. This computation yields the change in net worth, either an increase or decrease in net worth.

13. **Make adjustments to the net worth computation**. These include personal living expenses (expenditures), certain losses and legal income sources.

14. Illegal or unexplained income is determined through the **comparison of total income to known sources**; any unexplained income is attributed to the illegal sources.

SELECTED SOURCES OF INFORMATION FOR FINANCIAL INVESTIGATION

FATF

FATF (2005), *International Best Practices: Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments (SR IX)*, FATF, Paris, France. www.fatf-gafi.org/topics/fatfrecommendations/documents/bestpracticescashcourierssrix.html

FATF (2008), *Terrorist Financing*, FATF, Paris, France www.fatf-gafi.org/topics/methodsandtrends/documents/name,1599,en.html

FATF (2010), *Best Practices Confiscation (Recommendations 3 and 38),* FATF, Paris, France www.fatf-gafi.org/topics/fatfrecommendations/documents/bestpracticesconfiscationrecommendations3and38.html

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations*, FATF Paris, France www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfrecommendations2012.html

COUNCIL OF EUROPE

Golobinek, R. (2006), *Financial Investigations and Confiscation of Proceeds of Crime: Training Manual for Law Enforcement and Judiciary*, Council of Europe, Strasbourg, France www.coe.int/t/dghl/cooperation/economiccrime/SpecialFiles/CARPO-ManualFinInv_eng.pdf

OECD

OECD (2009), *The Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, OECD, Paris, France, www.oecd.org/dataoecd/61/17/43841099.pdf

OECD (2009), *The Bribery Awareness Handbook for Tax Examiners and Tax Auditors*, OECD, Paris, France, www.oecd.org/dataoecd/20/20/37131825.pdf

UNITED KINGDOM

ACPO (Association of Chief Police Officers) Centrex (2006), *Practice Advice on Financial Investigation,* www.surreycc.gov.uk/__data/assets/pdf_file/0007/171970/Advice-on-financial-investigation.pdf

NPIA (National Policing Improvement Agency) (n.d.)a, *Enhanced Financial Investigation Skills Course*, NPIA, London, United Kingdom

NPIA (National Policing Improvement Agency) (n.d.)b, *Financial Intelligence Officer course*, NPIA, London, United Kingdom

NPIA (National Policing Improvement Agency) (n.d.)c, *Cash Seizure Course,* NPIA, London, United Kingdom

NPIA (National Policing Improvement Agency) (n.d.)d, *Financial Investigation Course,* NPIA, London, United Kingdom

NPIA (National Policing Improvement Agency) (n.d.)e, *Internet Research Skills for Financial Investigators,* NPIA, London, United Kingdom

NPIA (National Policing Improvement Agency) (n.d.)f, *Proceeds of Crime Management Course,* NPIA, London, United Kingdom

NPIA (National Policing Improvement Agency) (n.d.)g, *Confiscation Course,* NPIA, London, United Kingdom

NPIA (National Policing Improvement Agency) (n.d.)h, *'Making Sure Crime Doesn't Pay' - Delivering excellence in Proceeds of Crime Training,* NPIA, London, United Kingdom

UNODC

UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, www.unodc.org/pdf/crime/corruption/Handbook.pdf

UNITED NATIONS

United Nations (2000), *United Nations Convention against Transnational Organised Crime*, United Nations, New York, US, www.unodc.org/unodc/en/treaties/CTOC/index.html

UNITED STATES

US Department of Homeland Security (n.d.), *Cornerstone Outreach Initiative,* www.ice.gov/cornerstone, accessed 29 June 2012

US Department of Justice (n.d.)a, *Financial Investigations Guide* www.justice.gov/criminal/afmls/pubs/pdf/fininvguide.pdf , accessed 29 June 2012

US Department of Justice (n.d.)b, *Financial Investigation Checklist* www.justice.gov/criminal/afmls/pubs/pdf/fininvcheck.pdf, accessed 29 June 2012

US Government Accountibility Office (1997), *Investigators' Guide to Sources of Information*, General Accounting Office, Washington, US, www.gao.gov/special.pubs/soi/os97002.pdf

USAID (United States Agency for International Development) (2005), *Anti-Corruption Investigation and Trial Guide*, ARD, Burlington, Vermont, US http://pdf.usaid.gov/pdf_docs/PNADE146.pdf

WORLD BANK- UNODC (STAR INITIATIVE)

Brun, J.P., *et al* (2011), *Asset Recover Handbook: A Guide for Practitioners,* StAR Initiative, World Bank and UNODC, Washington, US
www1.worldbank.org/finance/star_site/documents/arhandbook/ar_handbook_final.pdf

Stephenson, M., *et al* (2011), *Barriers to Asset Recovery: An Analysis to the Key Barriers and Recommendations for Action, StAR Initiative*, World Bank and UNODC, Washington, US
www1.worldbank.org/finance/star_site/documents/barriers/barriers_to_asset_recovery.pdf

StAR (2009), *Recovering Stolen Assets: Towards a Global Architecture for Asset Recovery*, StAR Initiative, World Bank and UNODC, Washington, US
www1.worldbank.org/finance/star_site/documents/global_architecture/GlobalArchitectureFinalwithCover.pdf

Burdescu, R. (2009), *Income and Asset Declarations: Tools and Trade-offs*, StAR Initiative, World Bank and UNODC, Washington, US
www1.worldbank.org/finance/star_site/documents/income_assests/ADincomeasset.pdf

Greenberg, S., *et al.* (2009), *A Good Practice Guide for Non-conviction-based Asset Forfeiture*, StAR Initiative, World Bank and UNODC, Washington, US
www1.worldbank.org/finance/star_site/documents/non-conviction/NCBGuideFinalEBook.pdf

OECD and the International Bank for Reconstruction and Development/The World Bank, (2011) *Tracking Anti-Corruption and Asset Recovery Commitments* (StAR), StAR Initiative, World Bank and UNODC, Washington, US
www1.worldbank.org/finance/star_site/documents/AccraReport/Report/Accra%20Commitments.pdf

Appendix WW:

FATF, *FATF Report: Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated with Gold* (Paris: FATF, 2015)

FATF REPORT

Money laundering / terrorist financing risks and vulnerabilities associated with gold

July 2015

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

For more information about the Asia/Pacific Group on Money Laundering (APG), please visit **www.apgml.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF and APG (2015), *Money laundering and terrorist financing risks and vulnerabilities associated with gold,* FATF, Paris and APG, Sydney
www.fatf-gafi.org/topics/methodsandtrends/documents/ml-tf-risks-and-vulnerabilities-gold.html

Contents

GLOSSARY OF TERMS AND ACRONYMS

AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
ASM	Artisanal or small-scale mining (ASM)
DNFBPs	Designated non-financial businesses and professions
EAG	Eurasian group on combating money laundering and financing of terrorism
FIU	Financial intelligence unit
FSRB	FATF-Style Regional Body
Gold Bullion	Refined gold, valued by weight
Gold Ingot	Block of gold, usually in the shape of a bar
HSI	Homeland Security Investigations (United States)
Investment gold	Particular class of gold with a specific purity
LEA	Law enforcement agency
LSM	Large-scale or medium-scale mining
MENAFATF	Middle East & North Africa Financial Action Task Force
ML	Money laundering
STR	Suspicious transaction report
TBML	Trade-based money laundering
TF	Terrorist financing

EXECUTIVE SUMMARY

This joint FATF–Asia/Pacific Group on Money Laundering (APG) research project into the gold sector arose as a result of the apparently natural transition or displacement of money laundering (ML) and terrorist financing (TF) from the formal financial sector and the cash market to the gold market, as regulators and law enforcement harden those environments.[1]

Chapter 2 identifies the features of gold that make it attractive to criminal organisations as a mechanism to move value.

Chapter 3 maps the nature, source and scope of gold production, markets and trade, to assist practitioners to recognise the common predicate offences (such as theft, smuggling, fraud, illegal schemes and tax evasion) that occur in the gold market. A good understanding of how these activities operate is required to recognise the ML and TF activity that is being perpetrated.

Chapter 4 builds a library of 'red flag' indicators that could assist designated non-financial businesses and professions (DNFBPs), financial institutions and others in identifying and reporting suspicious activities associated with ML and TF in the gold sector.

The key findings of this report are intended to promote effective risk mitigation and preventative measures or encourage further work on areas requiring further investigation.

Key findings:

- Gold is an extremely attractive vehicle for laundering money. It provides a mechanism for organised crime groups to convert illicit cash into a stable, anonymous, transformable and easily exchangeable asset to realise or reinvest the profits of their criminal activities.
- The gold market is a target for criminal activity because it is highly lucrative. Understanding the various stages of the gold market continuum, and the types of predicate offending that can occur in each stage, is critical in identifying money laundering and terrorist financing risks emanating from this industry.
- Further research is required to establish the impact of regulation on detecting and discouraging criminal activities in the gold market, and the potential links between the gold market and terrorist financing. Such research into the correlation between financial flows and the gold market will also lead to a better understanding of how criminals use gold and gold products to launder money.

[1] See also, *Money Laundering and Terrorist Financing through Trade in Diamonds* Report, FATF (2013a).

1. INTRODUCTION

Gold has been used in various cultures since antiquity as a medium for exchange or payment. Historically, governments minted coins out of a physical commodity such as gold, or would print paper money that could be redeemed for a set amount of physical commodity (Gold standard). Most modern paper currencies are referred to as 'fiat currencies'. They have no intrinsic value and are used solely as a means of payment. Even with the modern use of fiat money, precious metals remain an alternative means of payment due to their high intrinsic value and ease of exchangeability.

Recent shifts in the global economy have resulted in an increased demand for stable-value investments and commodities. Gold is a universally accepted currency that has remained stable in spite of fluctuations in global financial markets. Internationally enforced anti-money laundering (AML) measures are influencing a shift in criminal behaviours towards methodologies with lower law enforcement visibility, which makes gold very attractive. Further, gold is an integral part of the cultural heritage of many countries, like China and India, where it features heavily in religious and social exchanges.

As with the diamond sector, the gold sector (via dealers in precious metals) is covered under the FATF Standards by Recommendation 23 - Designated Non-Financial Businesses and Professions (DNFBPs). However, like the diamond sector, it is different from other DNFBPs.

This paper is not intended to describe the various elements of the gold market continuum - it is complex and there are a number of papers that cover this topic comprehensively. In order to effectively understand gold market vulnerabilities, this report should be read in conjunction with, for example:

- *The Direct Economic Impact of Gold*[2] - written by PriceWaterhouseCoopers and commissioned by the World Gold Council which is working diligently to improve governance and compliance of the entire gold industry. This paper provides a unique look at the entire gold value chain.
- *The Gold Paper*[3] authored by the British Jewellers' Association and the National Association of Goldsmiths.

In addition to reviewing existing literature on the gold sector, this report is the result of extensive consultation with the international public and private sector via:

- *Survey responses from public and private sector participants involved in the gold market.*
  Separate questionnaires were directed at both the Government and private sectors, circulated through FATF, APG and other FATF-Style Regional Body (FSRB) jurisdictions, for completion by relevant bodies. Analysis of these responses assisted in identifying or confirming commonalities amongst various jurisdictions regarding the challenges in understanding and tackling the vulnerabilities of the gold market to ML and TF.

---

2 PricewaterhouseCoopers (2013), 'The Direct Economic Impact of Gold'. Hereafter referred to as the 'PWC Report'.

3 British Jewellers' Association (BJA) and National Association of Goldsmiths (N.G.A) (2013), 'The Gold Report'. Hereafter referred to as the 'Gold Paper'.

- *Case studies provided by law enforcement agencies.*
  This report uses the limited number of case studies that were reported to illustrate the operating environment and to help develop 'red flags' to identify ML and TF activity.

2. GOLD AS A VEHICLE FOR MONEY LAUNDERING – SIGNIFICANT VULNERABILITIES

There are two broad characteristics of gold and the gold market which make it enticing to criminal groups. The first is the nature and size of the market itself which is highly reliant on cash as the method of exchange. The second is the anonymity generated from the properties of gold which make tracking its origins very difficult to do. These factors make gold highly attractive to criminal syndicates wishing to hide, move or invest their illicit proceeds.

THE GOLD MARKET IS CASH INTENSIVE

The regulatory characteristics of the gold market in a number of countries make it attractive for organised crime groups to own cash-for-gold businesses in order to place and integrate illicit proceeds. Given the limited level of industry oversight and licencing requirements, cash-for-gold businesses have the potential to provide criminal groups with a continuous supply of untraceable gold commodities from various sources. Furthermore, this supply is purchased at below market cost, directly from the general public—who do not have to prove that they own the second-hand gold presented for sale.

The high-volume, low value transactions conducted through these cash-intensive businesses can be easily falsified or co-mingled with the proceeds of crime, while the purchased gold can be used to make untraceable gold-based payments for illicit goods and services. Because much of the recycled material is purchased in cash, large numbers of transactions are undertaken anonymously.

Individuals who have a need to launder cash, especially those involved in organised crime, are very willing to participate in the cash-for-gold business because there is a high propensity to make a profit and in most jurisdictions there is little governance or oversight of this type of activity. People with no criminal history are also prepared to undertake this activity even if they suspect that the underlying purpose of the activity is ML.

Trade in recycled gold, both legal and illegal, requires little start-up capital and therefore operations can be very itinerant, opening and closing with little difficulty. This adds to the difficulty for regulators to monitor these activities.

Case study 1 illustrates how cash from the sale of drugs is exchanged for gold and smuggled internationally by a third party money laundering syndicate.

Case study 1. **Third party gold smuggling syndicate used to launder proceeds of illegal drug sales**

In early 2014, the French police uncovered an international money-laundering network, used to launder the proceeds of the sale of cannabis in the Paris region of France. This case study summarises the findings of the French law enforcement investigation. Moroccan dealers smuggled hash to France and sold it at street level. An Indian national (who was subsequently arrested in

March 2014) organised the collection of the proceeds from the street sales. This money collection (called '*amana*' by the syndicate) was undertaken by so-called '*salafs*' (mules) who were aware that they were dealing with the proceeds of the crime, but not of the crime itself. This was an intentional decision by the group to put some distance between the predicate criminal activity and the *salafs*. This segregation of roles makes it difficult to demonstrate that the money is the proceeds of a specific predicate offence, which is necessary in a number of jurisdictions to prove money laundering.

In this case study, the *salafs* took their orders from the Moroccan drug dealers and supplied the money to the Indian national. The investigation estimated that in a six-month period the *salafs* collected well in excess of EUR 10 million. Whilst the Indian national kept a very low profile in France (he had no official income apart from his wife's social allowances, and lived in social housing in the suburbs of Paris), he held a number of valuable assets in India.

On receipt of the money, the Indian national arranged the transportation of the cash by car to Belgium where it was used to purchase gold and jewellery. The bulk of the cash was deposited in cash into the different accounts of companies associated with an identified gold trader and used to purchase gold from a wholesaler. False invoices generated by the Indian national (in the name of companies set up by him) were used to support the transactions on the gold coins and ingots as well as gold certificates, whenever authorities would question the holder of the gold.

The investigation established two main routes used to move the gold to India.

First route: Both the jewellery and the gold were sent to Dubai using false invoices and fake companies in the UAE. If the transactions were completed without intervention these false invoices were destroyed and if not, then they were used to support the activity. The investigation established that the gold trader kept official records for the sale of 190 kilograms of gold in 11 months with a value of approximately EUR 6 million. However, the investigation calculated the need for gold by the syndicate was closer to 20 kilograms of gold per week. Details of this shortfall of gold were not established.

The Indian national used relatives to transport the gold to India and the UAE with one of the relatives travelling more than 200 times to India and the UAE from 2008 to 2014 (two to three times a month) The head of the India syndicate controlled a travel agency in India which provided flight tickets to the mules and sometimes fake invoices for the purchase of gold. According to information, the gold was not smuggled to Dubai but officially exported and declared to customs, using the false invoices as a cover.

In the first instance the gold was transported to Dubai where it was sold to local people or Indian nationals (via a *hawaladar*). On the sale of the gold the Moroccan drug dealers were paid via controlled foreign exchange operations in Dubai. The physical gold was then smuggled into India, in this instance with the assistance of an employee of a travel agency based in Dubai who recruited mules to undertake the work for a small fee amounting to approximately EUR 220. The investigations identified, couples, elders and on one occasion the use of a 'toddler' to undertake this activity.

A jeweller transformed the gold to make it easier to conceal including mixing gold flakes with coffee,

nickel electrolysis of jewels, and 100 g gold drops for internal concealment.

Second route: An alternate route to transport the gold from Belgium to India was via the international airports of Bangkok and Singapore to a professional Burmese smuggler. The gold was then conveyed through Myanmar to India where it was sold.

Irrespective of the route used, from the moment the money was collected off the streets in France, it took five days for the money launderers to pay back their Moroccan silent partners.

The Indian syndicate's profit was based upon the conversion and resale of gold. By smuggling gold and avoiding taxes, the Indian syndicate was able to sell it competitively and still make a profit. The gold in question was purchased at EUR 31 per gram in Belgium and resold for EUR 36.32 per gram in Dubai or India. The Belgium gold trader received a fee of EUR 325 per kilogram which equated to a profit of EUR 5 000 per kilogram for the syndicate.

This system used by the Indian syndicate was so profitable that the Indian gave up his normal commission of 2.25% on the money laundered. His only desire was to channel as much *amana* as possible in order to buy the gold again and again. Thus he offered the unique opportunity for his Moroccan partner to launder his money at no cost.

Source: French National Judicial Police (DCPJ)

Case study 2 below illustrates how buying gold for cash can allow criminal organisations to place, layer and integrate funds into the formal financial sector.

Case study 2. **Trading in gold to legitimise the proceeds of drug trafficking**

The United States Homeland Security Investigations (HSI) uncovered a scheme where illicit proceeds from a drug trafficking organisation were being used to purchase gold.

A criminal organisation in the US was buying gold from various precious metals retailers using illicit proceeds from narcotics sales. The gold was then sold to a precious metals broker who then sold it to other businesses.

The proceeds of the sale were then wired to a third party out of the US with links to the drug trafficking organization, thus completing the money laundering cycle.

Source: US-HSI

GOLD CAN BE TRADED ANONYMOUSLY AND TRANSACTIONS ARE DIFFICULT TO TRACE AND VERIFY

As the following case study from Belgium illustrates, many transactions involving gold occur anonymously, with little to no record identifying the seller, or purchaser, of gold. This means that law enforcement agencies have little to assist them to identify what the source of the gold is or the identity of the person who sold it. It may be difficult to refute false claims about the source of gold due to the challenges in correctly identifying gold.

Case study 3. **Buying and selling gold anonymously**

A wholesaler in precious metals (wholesaler A), held various bank accounts in Belgium. Analysis of these accounts showed that the wholesaler mostly paid suppliers of precious metals in cash. Over the period of one year a total amount in excess of EUR 800 million was withdrawn in cash. The account mainly received payments from a Belgian bank for purchases of bullion gold.

Company/trader B supplied used gold to wholesaler A and is paid in cash. Company/trader B also pays its gold suppliers in cash. In its financial records, company/trader B records the supplying companies as private individuals, without any form of identification. Company/trader B is suspected to be a cover for the owners' illegal activities, i.e. laundering proceeds of crime by exchanging money.

Wholesaler A was known to the police to engage in money laundering. Its customers are apparently mainly shops selling gold in Antwerp, private individuals and intermediaries that were all recorded as "private individuals" in the accounts. Wholesaler A did not ask its customers for any identification nor did he inquire into the origin of the gold. Enquiries established that much of this gold was said to have come from the 'black market' (jewellery theft) as well as from criminal organisations linked to prostitution and drugs. Wholesaler A paid for the gold in cash, larger quantities of gold were split up so the price would never be more than EUR 15 000, the threshold for anti-money laundering / countering the financing of terrorism (AML/CFT) reporting of cash transactions.

Apart from company/trader B, other suppliers of wholesaler A's were also known to the police. This lead to suspicion that wholesaler A was being used to launder criminal proceeds. Providing anonymity and cash payments attract customers from a criminal environment.

Source: Belgium Financial Intelligence Unit (FIU)

GOLD IS A FORM OF GLOBAL CURRENCY AND ACTS AS A MEDIUM FOR EXCHANGE IN CRIMINAL TRANSACTIONS

Due to the inherent value of gold, and its worldwide exchangeability, retail gold is often seen as a viable alternative to cash to settle debts and distribute profit from criminal activity. Particular ethnic groups operating international *hawala* networks have been found to use gold as a medium to settle outstanding balances (although such use of gold is not an illegal activity in itself)[4]. Case study 4, highlights that a syndicate leader, who was a former bank manager and had intimate knowledge of the formal banking sector, strategically identified gold as a way to launder money and pay his criminal associates for their services. Similarly, in case study 5, a corrupt official seeks to distort the link between himself and a bribe by asking for the bribe to be paid in gold to his wife.

[4] *Hawala* (and other similar service providers such as *Hundi*) are defined as money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time (FATF (2013b), *The role of hawala and other similar service providers in money laundering and terrorist financing*).

Case study 4. **Major drug syndicate paid workers in gold**

An investigation into a well-organised and resourced drug syndicate identified a former bank manager as the head of the operation. Allegedly, the suspect was involved in financing and facilitating the multi-million dollar cannabis and amphetamines production operation and was linked with several well-known criminals.

The head of the operation was suspected of laundering the proceeds from the drugs syndicates through the purchase and sale of gold, the purchase of cattle and through gambling. Authorities believe the suspect used cash to purchase gold from prospectors at a reduced price and then sold the gold to unrelated businesses and declared it as legitimate revenue. Police located a large quantity of gold nuggets and AUD 161 000 cash hidden by the syndicate.

Those involved in the operation were paid well, and some received bonus payments in drugs and gold. One worker was paid a total of AUD 250 000 in cash, drugs and gold in the four seasons he was involved in the operation. Syndicate chiefs were paid more than AUD 300 000 each harvest, as well as being paid in gold bullion.

Commonwealth proceeds of crime action was taken against the offenders and resulted in the restraint of over AUD 4 million worth of assets, including rural properties, cattle, machinery, AUD 220 000 cash and a large quantity of gold. The law enforcement operation led to the arrest of number of syndicate members, who were subsequently charged and jailed for lengthy periods of time.

Source: Australian FIU

Case study 5. **Gold used to exchange value in corruption deals – no banking transactions linking the perpetrators**

Chairman A is the head of an Indian public entity responsible for awarding contracts for industrial work. Person B is the Managing Director of a company that has applied for a contract with the public entity. Person B approaches Chairman A's friend, Person C, to broker a deal to obtain the contract with a bribe of INR 2 million (Indian rupees).

Chairman A directed Persons B and C to contact his wife for the details on how the money was to be exchanged. Chairman A's wife asked for the cash to be converted into gold and handed over to her. Once the gold was provided to her by Person B, she deposited the gold into a bank locker.

Acting on a tip off, the Central Bureau of Investigation registered a case against Chairman A and conducted searches at his premises and lockers and recovered the gold.

The Central Bureau of Investigation charged the offenders for the predicate offence under Prevention of Corruption Act, which is a scheduled offence under Prevention of Money Laundering Act of India and 10kg of gold was restrained as part of a money laundering investigation.

Source: Enforcement Directorate of India

INVESTMENT IN GOLD PROVIDES RELIABLE RETURNS

In the money market, gold as an asset is used to reduce risk and stabilise return on investment. The predominant reason for this is that for the average investor, the gold trade is more easily understood and gold is trusted more than complex financial instruments. Further, gold is less volatile than most commodities and equity indices which allow account managers to better balance investment portfolios because it gives them greater ability to manage risk associated with volatility. For these same reasons, there is a bias for money laundering syndicates to prefer cash or precious metals such as gold when conducting transactions especially international transactions. Case study 6 illustrates that criminals are willing to invest in, and stockpile gold, to distance themselves from the predicate crime, even as a medium-term investment.

Case study 6. **Investing in gold to realise the proceeds of crime at a later date**

A Swiss financial intermediary, which offers a complete set of services related to melting, refining, sourcing and trading of precious metals, received a business proposition via e-mail from a person with an Asian-sounding name. The intermediary did not know the person nor the e-mail address (through a commercial provider).

In this e-mail message, the sender indicated that a large sum of gold was to be put up for sale. Attached to the e-mail message was a letter, including letterhead, from a company in Switzerland. In this letter, the company confirmed that it had been asked by a second company to locate potential buyers and serve as the clearing agent for the gold transaction. The letter claimed that this second company was also domiciled in Switzerland and had been contacted directly by a bank, which was the actual seller of the gold. The bank in question, however, was not mentioned. The business proposition was referred to as “a major gold deal” and that the sale price would be 4% below the London Gold Fix rate.

The reporting financial intermediary suspected foul play as such large gold transactions are usually handled by professional dealers and yet the bank seeking to sell the gold was not mentioned in the offer. In addition, the reporting financial intermediary suspected that neither of the two companies mentioned were licensed to act as financial intermediaries.

A report was made to the Swiss FIU and as a result of a search of the FIU database; it became apparent that a representative of one of the companies involved had been convicted in a fraud case abroad several years before. The financial intermediary surmised that perhaps some of the illicit gains from this fraud had been used to buy gold. This gold would then have been hoarded somewhere and now that the gold price had risen; the moment to sell had come.

The Swiss FIU contacted the partner FIU abroad to find out whether all of the assets in question had been seized at the time of sentencing. The foreign FIU replied that there was the suspicion of fraud and the person in question had been investigated by the responsible police. He was also known under his first name and under an alias name. However, records were no longer available. For this reason, a possible link between the gold and illicit gains from fraudulent activities could not be explored further and the suspicious transaction report (STR) could not be forwarded to a law

enforcement authority.

Source: Switzerland FIU

GOLD IS EASILY SMUGGLED AND TRADED – BOTH PHYSICALLY AND VIRTUALLY

The survey responses for this report indicate that the majority of money laundering and predicate offences relating to the gold market are associated with international and domestic trading.

In the physical sense, it is easy to melt gold bullion and convert it into different forms to disguise the fact that it is gold. For example, there have been media reports about the interdiction of gold shipments between North and South America where the gold was disguised as American souvenirs. The case studies below, give examples of gold being reshaped into cones and common items such as wrenches, nuts, bolts and belt buckles. Gold in these forms is easier to conceal from border authorities and its value can be considerably understated on the Bills of Lading.

Case study 7. **Gold reshaped into common objects to avoid detection by customs**

The United States Homeland Security Investigations (HSI) and Internal Revenue Service-Criminal Investigation (IRS-CI) uncovered a scheme related to gold being reshaped and exported as common objects like cones. From December 2001 through May 2003, Jaime Ross, owner of Ross Refiners, a gold refining business in Manhattan's Diamond District in New York, was selling bulk quantities of gold to an undercover agent posing in an undercover operation as a narcotics money launderer.

Ross would sell the gold knowing that the currency used allegedly came from narcotics sales. Ross would recast the gold into cones and alter the colour of the gold to avoid detection while being smuggled to Colombia. Ross was arrested on 4 June 2003 and charged with money laundering and failing to file IRS Forms 8300, declaring the cash transaction relating to the sale of gold.

Source: US-HSI

Case study 8. **Gold reshaped into common objects like wrenches, nuts, bolts, belt buckles etc.**

Under 'Operation Meltdown', The United States Homeland Security Investigations (HSI) investigators uncovered a carousel scheme in which jewellers were converting the proceeds from drug sales into the equivalent value in gold.

The scheme involved a criminal organization with links to gold suppliers in the New York area that were laundering millions of dollars in drug proceeds. The HSI investigation disclosed that the exported gold from Colombia was described as 'gold pigments' and upon importation into the United States the same merchandise was then described as 'gold bullion'.

The gold bullion was then transported to New York, where jewellers who were cooperating with drug trafficking organisations disguised the gold into a wide range of common objects like

wrenches, nuts, bolts, belt buckles and trailer hitches. These items were exported back to Colombia at a declared value far below the worth of their weight in gold. Upon arrival in Colombia, the same gold was recast into bullion and exported again to the US as 'gold pigment'.

The investigation of this case resulted in the arrest of 23 jewellers charged with money laundering and others arrests along with the seizure of 140 kg of gold, more than 100 loose diamonds, USD 2.8 million, 118 kg of cocaine, 6 guns and two vehicles.

Source: US-HSI

Because the exact amount of gold harvested from recycling activity is difficult to identify, smuggling is an ideal method of moving it from one location to the next either domestically or to international jurisdictions where it can then be refined.

Criminals may recruit couriers to carry gold across borders both legally and illegally (smuggling). This allows the criminals to remain anonymous and distance themselves from the transfer.

The classification and description of gold as an excuse to move value are techniques used by the criminal organizations to give the appearance of legality to the flow of funds of licit or illicit origin and also allow the gold itself to be transferred to places more conducive to their ongoing criminal activity. This usually occurs through routes that do not have strong governance over the tracking of the movement of gold or the gold is smuggled to avoid detection.

In some cases due to the nature of the market, the gold does not have to exist or be moved physically to be traded. Rather, citing 'gold' as the traded good on an invoice can be used to justify large movements of money, either domestically or across borders.

This is a form of trade-based money laundering (TBML) which is actually promoted by the market itself; the movement of value without the movement of the underlying commodity was created to reduce the cost of physically moving a risky, high valued commodity. TBML is 'the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins.'[5]

As indicated, the gold sector includes depository and certificate products which provide legal title to gold bullion which is stored on behalf of the owner. These certificates provide another mechanism for criminals to launder money whilst distancing themselves from the asset. These certificates can be purchased or traded by third parties.

5 FATF (2006), *Trade Based Money Laundering*, p. i.

3. OPPORTUNITIES FOR GENERATING ILLICIT PROFIT IN THE GOLD INDUSTRY

This chapter outlines some of the many opportunities available for criminal groups to exploit the gold market for profit. As with the mining of other precious materials, the journey of gold, from production to the consumer and investor, consists of several stages. There are two main sources of 'new' gold put on the market each year – the first is gold that is mined and the second is gold that is recycled. Mining accounts for two thirds of 'new' gold production each year and recycling accounts for the remaining one third.[6]

This section gives an overview of the type of predicate offending that can occur in the gold market continuum to assist practitioners to better understand the related money laundering and terrorist financing risks. This is intended to provide practitioners with a starting point as there is limited knowledge of the financial flows associated with the gold industry.

Practitioners should also be aware that criminal organisations may choose to infiltrate this industry to easily access mechanisms to place, layer and integrate their illicit proceeds with the proceeds of legitimate activity in the gold industry.

LARGE-MEDIUM SCALE MINING

Large scale or medium scale industrial mining (LSM) covers formalised extraction processes using industrial and mechanised methods.[7] This sector is dominated by large corporate companies such as Anglo Gold Ashanti, Rio Tinto and Newmont.[8] LSM operations require significant capital which may be sourced privately or publically. Projects of this kind have high barriers to entry. Research by PricewaterhouseCoopers in 2012, identified China, Australia, the United States, Russia, Peru, South Africa, Canada, Mexico, Indonesia, Ghana, Uzbekistan, Brazil, Papua New Guinea, Argentina and Tanzania as the world's largest gold producers (in order of significance).[9]

- *Corruption*: Due to the high barriers to entry, including obtaining the necessary environmental and regulatory permission of LSM projects, these activities are susceptible to corruption of a large scale. The capacity to obtain the necessary clearances through corruption maximises the benefits and minimises the costs associated with mining, to the detriment of other businesses and individuals.
- *Theft of mined ore*: As the concentration of gold ore extracted from the ground can only be estimated, there is potential for organised crime groups to infiltrate the production supply chain, siphon off mined ore and have it refined, then sold, to generate income.

6 PWC Report, p. 12.

7 Gold Paper, p. 7.

8 Gold Paper, p. 7.

9 PWC Report, p. 3.

- *Fraud and other scams involved with mining gold*: Due to the broad appeal of gold to a large sector of the population and the speculative nature of mining start-up companies, the gold market is highly susceptible to fraudulent schemes and other scams, such as Ponzi schemes, which provide fertile ground for organised groups to generate illicit funds.

ARTISANAL SMALL-SCALE MINING

Artisanal or small-scale mining (ASM) is usually informal or semi-formal gold collection using basic hand tools or simple mechanised equipment. It is often carried out by individuals, sometimes seasonally or as a nomadic activity, or by groups. This form of collection accounts for about 12% of global mine supply and provides income to significant numbers of people, especially in less developed or emerging economies.[10]

- *Illegal mining*: Due to the challenges of governing this sporadic form of mining and the low barriers to entering the sector, there is significant scope for organised crime groups and terrorist groups to harvest gold ore from ASM operations. Similar to LSM mining, corruption can also assist to facilitate illegal ASM activities. Case study 9, illustrates the lucrative nature of illegal mining. Case study 10 explains how a narco-terrorist group used the proceeds of illegal gold mining to support their operations.
- *Smuggling*: Gold that is illegally mined will often need to be smuggled into another jurisdiction to be refined. This is because gold refineries are not necessarily located in the same jurisdiction that the gold ore is mined. Sophisticated smuggling syndicates are engaged to transport the illegally mined ore across borders. Case study 11 provides an example of ASM and gold smuggling in Ecuador.

Case study 9. **Example of gold smuggling and laundering from Zimbabwe**

The Zimbabwe FIU commenced an investigation based on a suspicious transaction report (STR) from a financial institution in Zimbabwe (Bank A). This STR reported that the subject, a holder of a personal bank account, attempted to make a cash deposit of ZAR 4.1 million (South African rand, equivalent to about USD 410 000) into his account and sought to immediately withdraw the money in US dollars.

Prior to the attempted transaction, his account had been overdrawn, thereby raising suspicion regarding the source of the substantial cash deposit. The bank was not satisfied that the funds were from a legitimate source, and it declined to accept the deposit and immediately filed an STR with the FIU.

The FIU conducted an interview with the individual who explained that the money was proceeds

10 PWC Report, p. 17.

from the sale of gold which he had purchased from small-scale miners and illegal dealers who operate in and around Kwekwe, one of Zimbabwe's gold producing regions. The Kwekwe region is dominated by small-scale licensed miners as well as illegal gold "panners" who prefer to make a quick sale and, therefore, sell to buyers such as the subject who pay cash on the spot. It was also asserted that gold buyers such as the subject, offer the small-scale and illegal miners, not only cash on the spot, but also offer a more attractive price than the state licensed buyer, which withholds a percentage as a statutory levy.

The subject told the FIU that he smuggled the gold to South Africa (with which Zimbabwe shares a border), where he would sell the gold to different buyers, including licensed gold millers. The subject indicated that his buyers, in turn, smuggled some of the gold from South Africa to Asia where they sold it to jewelers. The subject added that the attempted deposit was intended to enable him to exchange the South African rand (which he gets upon disposal of the gold in South Africa) for US dollars, which he would use to purchase more gold on the black market and continue the cycle. The US dollar is the currency acceptable to the gold suppliers.

On being asked how he disposed of his ZAR4.1million, after his bank had declined to accept his deposit, the subject revealed that he exchanged the South African rand through black market currency exchangers in Harare.

This case is one of many similar STRs which the Zimbabwean FIU has received and processed. While a few of the illegal gold dealers change their South African rand to US dollar, through banks, many others prefer to change the South African rand on the foreign currency black market to avoid detection.

Source: Zimbabwe FIU

Case study 10. **Mining and commercialising of gold to finance terrorism - Colombia**

A narco-terrorist group takes control of a territory where a gold mine is in production. To gain control of the mine the narco-terrorist group extorts the owners by way of violence and forcing the community to transfer the ownership titles to the group.

This narco-terrorist group uses the mine illegally where part of the gold from the mine is sold to a legal business and the transaction is paid in cash. The cash is then used to buy equipment, munitions, medicines, and other supplies needed to continue with their terrorist activities. The remaining gold is safely kept for future transactions.

Source: GAFILAT

Case study 11. **Illegal mining in Ecuador**

In 2010, approximately 20% of the Ecuadorian territory was registered as mining territory. However, the informal and sometimes illegal nature of the mining sector in Ecuador has impeded the ability of Ecuador and its neighbouring countries to identify how much gold is being mined and leaving the country illegally.

Ecuador estimates its annual production to be approximately 15 to 20 tonnes of gold.

Artisanal mining produced approximately six tonnes of gold in the 2012 equalling approximately USD 9.5 million in revenues for the State. Of the total of six tonnes produced, approximately two tonnes were dedicated to internal consumption (for jewellery) and the four remaining tonnes were legally exported, returning approximately USD 160 million during 2012.

The illegal mining is calculated to amount to between six and eight tonnes of gold every year. A significant amount of this production is smuggled over the border. This is due to the fact that it is easier in the neighbouring countries to sell the gold because, unlike in Ecuador, permits are not required.

Source: Ecuador FIU

RECYCLING

Recycled gold accounts for about one third of new gold introduced to the market each year.[11] Sources of recycled gold include industrial equipment, scrap generated from retail manufacturing, or jewellery. Recycling of gold is more likely to occur in areas of high gold consumption and is not tied to areas where gold is mined. In 2012, the United States, Italy, China, India, the United Arab Emirates, Turkey, the United Kingdom, Mexico, Egypt and Indonesia were the top source countries for the supply of gold for recycling purposes in order of quantity supplied. The supply of recycled gold is more responsive to demand than gold from mining where lag-time in development and other barriers limit rapid responses.

- *Theft*: Many jurisdictions identified jewellery theft as a significant form of predicate offending that occurs in the gold market. Cash-for-gold businesses provide criminals with the opportunity to convert stolen gold into cash without having to prove ownership over the second-hand gold presented for sale.

SMELTING/REFINING

All gold, both mined and recycled, is required to go through a refining process, referred to as smelting, to bring it up to what is referred to as 'investment quality'. Refineries may or may not operate in the same jurisdiction where the gold is mined, and in the majority of cases they do not.

11 PWC Report, p.1.

- *Smuggling*: As mentioned in the section on ASM, illegally mined gold will often need to be smuggled to a refinery to be smelted. Whilst some enforcement action has been undertaken against smelting operations, anecdotal evidence indicates that the smuggling of gold from both legal and illegal mine sites is widespread.
- *Misrepresentation/fraud*: Organised crime groups can misrepresent the purity, weight, origin and value of gold to create profits or to justify the instrument or proceeds of crime. As demonstrated in case study 12, misrepresentation can also aid in tax fraud.

Case study 12. **Fraudulent claims to earn tax credits – Australia**

Criminals can exploit jurisdictional tax schemes in relation to precious metals by combining trading and refining activities. In this case, 'syndicates' utilised inter-related transactions with associate entities to conceal the true nature of the transactions in order to fraudulently obtain tax refunds or avoid paying the Australian goods and services tax (GST). This process is also known as a 'missing trader' fraud.

Investigations suggest that gold bullion is cycled through gold refining entities, with claims that the bullion is broken down into a taxable form prior to being 'reconstituted'. It is then sold GST-free to a precious metal dealer after GST credits have been fraudulently claimed on the purchase by misrepresenting the nature and status of the transactions. Tens of millions of Australian dollars in GST payments are made on fraudulent claims.

Broadly, the criminal activity occurs through:

- Claiming GST credits on acquisitions of gold which were GST free and no entitlement exists.
- Incorrectly claiming GST credits under the special rules in relation to acquiring second-hand goods where gold is specifically excluded from the definition of second-hand goods under the GST Act.
- Incorrectly treating some supplies of gold bullion as GST free where the product does not meet the criteria under the Act.
- Individuals receiving payments emanating from the proceeds of the GST claims which are not being reported as income in the respective income tax returns.

Participants at the end of the supply chain are making GST-free sales (on the assumption gold has changed form) and claiming income tax credits on acquisitions from associated suppliers. Further, individuals within the syndicates are benefiting from the receipt of payments generated by the GST fraud which are not declared as income in the appropriate income tax returns.

Source: Australian Taxation Office

RETAILING

Retailing of gold is a significant market internationally, and as indicated below there is some understanding of the predicate offending that occurs in this sector, but there is little understanding of the financial flows in the trade. In 2012, the highest consumption demand came from India, China, the United States, Turkey and Thailand (listed in order of the size of the demand).[12]

- *Fraud:* As gold ownership has deep-rooted cultural significance, criminal organisations have developed a range of schemes to profit from the fraudulent sale of processed gold. These schemes can range from misrepresentation of jewellery pieces, to more complicated activities involving false identities and fraud committed online. For example, a jurisdiction who contributed to this report identified a scam involving a gold dealer looking for an interested partner to purchase gold from a royal family. Fake contact details and websites were created to project an appearance of professionalism in order to attract unsuspecting victims.
- *Exploitation of gold incentive schemes:* Due to the overall demand for gold-based commodities, many jurisdictions see the trade in gold as beneficial to their economy. For this reason a number of jurisdictions have incentive programs usually in the form of tax incentives to help promote the trade. Arbitrage between countries on the different schemes provides opportunities for organised crime to exploit these vulnerabilities by sourcing illegal payments from these jurisdictions for perceived legitimate activity.

INVESTMENT

Investment gold is a particular class of gold with a specific purity. Gold can act as a financial instrument through online gold trading services which provide loans and credit. The traders and recipients receive a right in gold without the actual physical exchange of gold.

- Tax fraud: As gold is easy to obtain and conceal, it often forms the basis of tax fraud where gold commodity is purchased and stored legally in foreign jurisdictions. Whilst stored in foreign jurisdictions, markets are set up to sell the value locally. This allows cash to be drawn on the value of the stored gold without actually accessing the gold.

12 PWC report, p. 29.

4. RED FLAGS

ML/TF ACTIVITY (AND UNDERLYING PREDICATE CRIME ACTIVITY)

CUSTOMER BEHAVIOUR

- Established customer (including bullion dealers) dramatically increasing his purchase of gold bullion for no apparent reason.
- Foreign nationals purchasing gold bullion through multiple transactions over a short time period.
- Bullion transferred among associates using bullion accounts (including family members) for no apparent commercial purpose.
- Occupation inconsistent with customer's financial profile. For example, the customer may list their occupation as 'student' or 'truck driver' yet transfer large values of funds to bullion accounts.
- Customer buying gold bullion and using a General Post Office (GPO), or private service provider, mail box as their address, without listing a corresponding box number.
- Unusual pattern of bullion transactions and the nature of the transactions are inconsistent with the customer profile.
- A previously unknown customer requesting a refiner to turn gold into bullion.

COMPANY BEHAVIOUR

- Non-reporting to the FIU by the gold industry organisations (where there is an obligation to report).
- Changes to business name of entities registered to deal in gold.
- Registration of a trading company in a tax haven even though its business relates to another jurisdiction.
- Movement of abnormally large sums of money in various accounts of the individuals and companies which are not related to the nature of their business.
- Unusual deposits i.e. use of cash or negotiable instruments (such as traveller's cheques, cashier's cheques and money orders) in round denominations (to keep below reporting threshold limit) to fund bank accounts and to pay for gold. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information.

- Numerous sole proprietorship businesses/private limited companies set up by seemingly unrelated people (proxies) but controlled by the same group of people. False addresses are used to register such businesses.
- Use of a corporate structure of shell companies located across the jurisdictions.
- Significant number of companies registered to one natural person.
- Commercial activities are not easy to track as the companies are registered elsewhere.
- No clarity of how the company transports the merchandise it has bought.

TRADE-BASED BEHAVIOUR (ALSO RELATED TO TRADE-BASED MONEY LAUNDERING)

- Cash payments for high-value orders are an indication of trade based money laundering (TBML) activity.
- Misclassification of gold purity, weight, origin and value on customs declaration forms.
- Gold is shipped to or from a jurisdiction designated as 'high risk' for money laundering activities or sensitive / non co-operative jurisdictions.
- Gold is transhipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
- Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.
- The transaction involves the use of front or shell companies. Both shell and front companies can be used to facilitate TBML but in different ways. A shell company has no real operating activity and is used to hide money laundering activity and the identities of individuals involved so as to obscure the money trail. If activity is traced to the company it is literally an empty shell.

PRODUCT DIFFERENTIATION

- The bullion has physical characteristics that are inconsistent with industry standards.
- Gold prices higher than those of the local gold market.

PAYMENT BEHAVIOUR

- A number of affiliated entities in the payments chain.

- Transit movement of funds and changes in purposes of payments.
- Payments to shell companies with further withdrawals.
- Granting of loans (with zero interest rates) to foreign companies.
- Granting of loans (with zero interest rates) to natural persons.
- Natural person or business sells gold saying that it comes from a place with no extraction license or from places with no gold mines.
- Large amount of funds transferred internationally and then withdrawn very quickly.
- International transfers to countries where the company is not registered.
- Significant cash withdrawals from bank accounts by participants within the gold trading industry.
- Division of funds in cheques and smaller cash transactions to pay for merchandise.
- Purchase of gold bullion with bank cheques may be an attempt to conceal the source of the funds and underlying ownership.
- The use of cash to purchase bullion, especially when there are multiple purchases in a short timeframe, or when large amounts are purchased at once, or when there are structured cash deposits into an account to finance a single gold bullion purchase.
- Original source of funds to buy gold bullion cannot be established. The transaction involves the receipt of cash (or by other payment methods, including cheques or credit cards) from third party entities that have no apparent connection with the transaction or front or shell companies or wire instructions / payment from parties which were not identified in the original letter of credit or other documentation. The transactions that involve payments for goods through cheques, bank drafts, or money orders not drawn on the account of the entity that purchased the items also need further verification.
- Transactions between domestic buyers and sellers with sales proceeds sent to unknown third parties overseas.

PREDICATE CRIME ACTIVITY

GOLD MINING BEHAVIOUR

- Production and commercialisation of gold by a person or business without a license.
- An ethnic community hires a third party for the entire operation of the mine.

- Licensed mines where the production has decreased with no apparent explanation.
- The development of mining activities using machinery and equipment that is not in accordance with the characteristics of the licensed small or artisanal mining.
- The development of mining activities without compliance with the administrative, technical, social and environmental regulation.
- The development of mining activities in prohibited areas.

CONCLUSION

The main finding of this report is that the characteristics of gold make it both attractive for, and vulnerable to, exploitation by criminal organisations that need to legitimise assets. Gold has intrinsic value, is easily smuggled and exchangeable worldwide and can be traded anonymously. Not unlike other precious stones and metals, gold's widespread historical and cultural significance, as well as its potential to legitimise illicit cash, create opportunities for its misuse.

This report has also identified a range of profit-making opportunities for criminals in the gold market continuum. The report also sets out a range of red-flags to identify predicate offences that could occur in the mining, recycling, refinement, retail and investment of gold. While the techniques employed to launder these profits may not be specific to the gold industry, it is important to note that criminal organisations are likely to benefit from infiltrating the gold market continuum due to the inherent value of gold and the ability to use gold to combine aspects of the placement-layering-integration process.

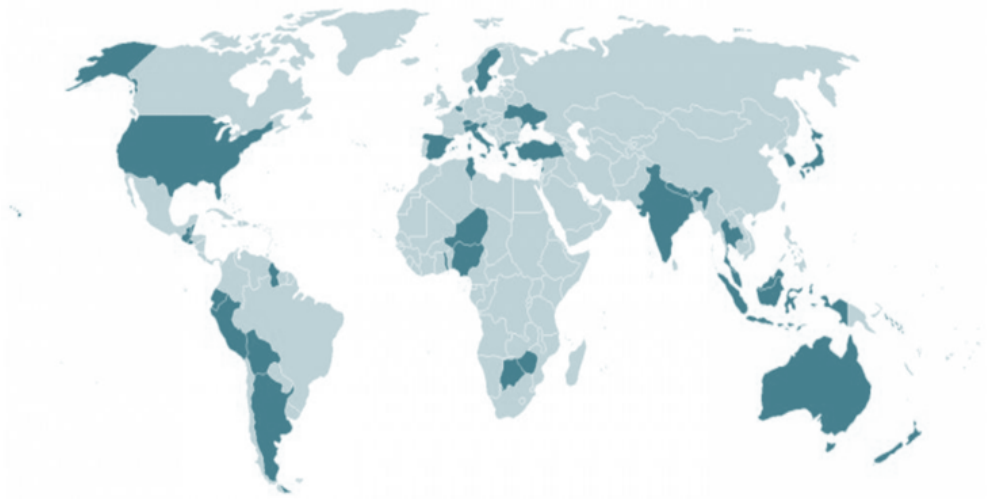
These are important findings, but further work needs to be done to identify any trends or patterns within jurisdictions and internationally in relation to money laundering and terrorist financing in the gold sector. While this report includes one case study on the abuse of the gold market by a terrorist group, it would be worthwhile considering to what extent terrorist groups are moving or raising funds through the gold sector. In addition to the financial flows, more information is required on the commodity flows.

Further work also needs to be done to map the regulatory controls relating to all aspects of the gold continuum, including formal and informal activity, to provide law enforcement agencies with an overview of starting points for regulatory information on gold production, wholesale, distribution and retail. Approximately one third of companies that responded to the questionnaire provided to the private sector revealed that they are not regulated by any Government or statutory authorities. While no conclusive statement can be drawn from this, it would be useful to undertake further study on how the gold industry is regulated both locally and internationally. A key question for this research is whether the gold industry is collecting relevant information, including financial information or customer details, to assist in the investigation of money laundering or terrorist financing and how this information is impacting on investigations.

APPENDIX A – ANALYSIS OF QUESTIONNAIRES

On the basis of the discussions held at the Middle East & North Africa Financial Action Task Force (MENAFATF)/FATF Joint Experts' Meeting in December 2013, a questionnaire was drafted to collect information from policy makers, investigators and FIU officials. The questionnaire was circulated through FATF and FSRB networks. Forty one countries responded to the questionnaire including Argentina, Australia, Belgium, Belize, Bhutan, Brunei Darussalam, British Virgin Island, Bolivia, Botswana, Denmark, Ecuador, El Salvador, Greece, Guatemala, Guyana, Italy, India, Indonesia, Japan, Lebanon, Malaysia, Nepal, New Zealand, Niger, Nigeria, South Korea, Peru, Singapore, Slovenia, Solomon Islands, Spain, St. Kitts & Nevis, Sweden, Switzerland, Thailand, Togo, Tunisia, Turkey, Ukraine, United States of America, Zimbabwe. The diagram below illustrates the geographical span of countries that responded to the questionnaire.

Graph 1. **Respondent countries to the questionnaire**



After consultation and discussion with private sector representatives, a questionnaire was also circulated to private sector representatives. The questionnaire was circulated through the FATF and the FSRBs Secretariats to the contact points of various countries who in turn obtained responses from the private sector. These countries included Australia, South Africa, Ecuador, Indonesia, Thailand, Japan, Lao PDR, Namibia, Peru and Switzerland. The questionnaire consisted of four parts relating to the mining, refining, financial gold products and gold trade sectors, the sectors responded as follows:

- Mining sector: Sixteen companies in six countries
- Refining sector: Seventeen companies in seven countries
- Financial gold products sector: Ten companies in three countries
- Gold trade sector: Forty companies in nine countries

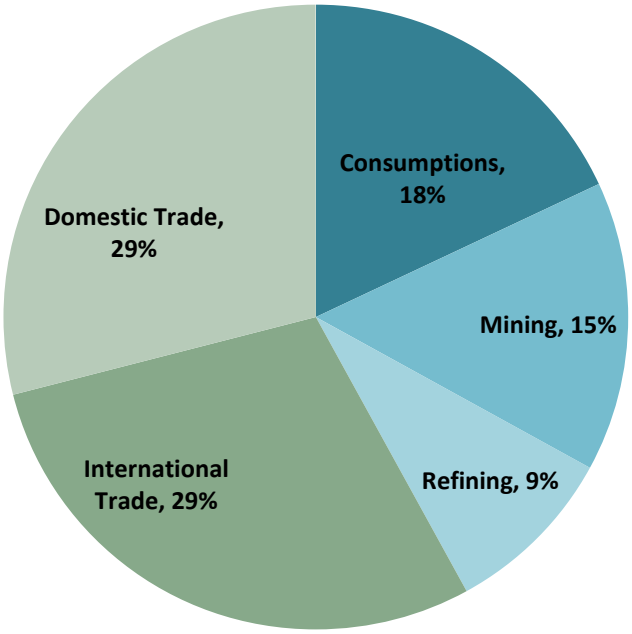
The results, summarised in the next section, lead to certain important findings relating to the money laundering and terrorist financing risks and vulnerabilities arising from gold mining, refining and trade, as well as the efforts being made to mitigate and combat such risks and vulnerabilities.

SUMMARY OF KEY FINDINGS OF THE QUESTIONNAIRE

In view of the limited sample size, the findings of the analysis of the questionnaire results are tentative. However, the tentative findings corroborate the observations which have been made in this Report on the basis of case studies, presentations made during APG Annual Meetings in Shanghai and Macau, the APG/Eurasian group on combating money laundering and financing of terrorism (EAG) Typologies Workshop in Mongolia and Joint Experts' Meeting in Doha.

The questionnaire results reveal that significantly high ML/TF risks and vulnerabilities arise in the domestic and international trade of gold. This is clearly demonstrated by the fact that jurisdictions have reported the highest number of predicate offences relating to gold, and ML cases related to gold, in the sectors relating to international and domestic trade of gold. The responses from the policy makers illustrate that besides the mining sector, the international trade sector is the most highly regulated. It is not clear whether that regulation relates to money laundering or whether, more broadly, international trade is a form of economic activity which is regulated in a lot of jurisdictions.

Graph 2. **Predicate offences and money laundering cases relating to gold**



Source: responses to questionnaire to policy makers

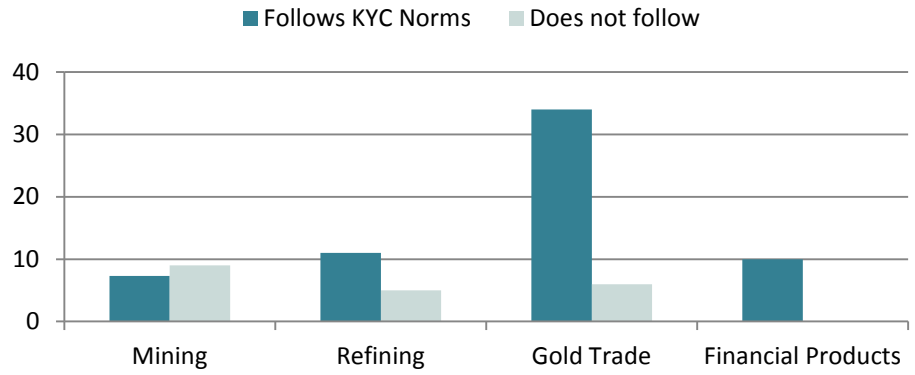
The questionnaire responses indicate that imported gold is a major source for the refinement and domestic consumption of gold. This supports findings of the literature review that gold is often not refined in the country where it is mined. These findings present vulnerabilities and risks arising from of trade-based money laundering related to gold. The details provided on reported predicate offence and ML cases indicate that while the absolute number of such cases may be low, the amount involved is substantial. Hence, even low volume of gold movement across border can transfer substantial value. The predicate offences relating to money laundering offences of gold are serious

in nature ranging from smuggling, fraud, corruption to narcotics trade. The statistical findings do not support commensurate international cooperation required to prevent and combat risks and vulnerabilities arising out of the gold trade.

Responses from the gold industry reveal that overwhelmingly the activities relating to mining, refining, trade and financial products of gold are carried out by the private sector. Most of the mining companies do not refine the gold which they mine and the refining companies also refine gold other than ore, in particular scrap gold. Most of the refining companies which have responded do not mark the gold that they refine. On the other hand, companies which are predominantly trading in gold do have quality marking norms for measuring the purity of gold.

The majority of companies in all four gold sectors (mining, refining, retailing and financial products) are subject to government regulation and laws but it is not clear how closely these controls relate to anti-money laundering or counter-terrorist financing. The majority of the companies in all four sectors settle their transactions through formal banking channels. Except for the mining sector, the majority of the companies in the other three Sectors follow know-your-customer (KYC) norms. Except for the financial gold product sector, the majority of the companies in the other three sectors do not claim to be operating in more than one country. Again apart from the financial gold products sector, the majority of the companies in the other sectors are affiliated to international/domestic associations.

Graph 3. **Application of KYC norms per sector**



Source: questionnaires responses

Note: the graph above illustrates that all of the companies in the financial gold products sector which responded to the Questionnaire follow KYC norms. Similarly, the majority of companies in the gold trade, also claim to follow KYC norms.

While the responses above indicate that there are measures in place to address the risks and vulnerabilities arising from gold production and trade, it is important to note that these responses are from the organised sectors of the gold market and the results may be very different for organisations operating in the sector in an informal or unorganised manner.

APPENDIX B – FURTHER CASE STUDIES ON MONEY LAUNDERING OR PREDICATE CRIME INVOLVING GOLD OR THE GOLD INDUSTRY

Case study 13. **Smuggling/undervaluation scheme using scrap gold**

The United States Homeland Security Investigations (HSI) uncovered a smuggling/undervaluation scheme with scrap gold upon entry to the United States (US). From January 2012 to November 2013, a US importer (ultimate consignee) was smuggling scrap gold into the US from countries in Central America at undervalued prices and subsequently providing payments to the exporters at overvalued amounts.

During this time frame two Central American companies sent scrap gold with a total declared value of approximately USD 6.4 million to the US importer yet during that same period wire transfers valued at approximately USD 24 million where sent back to the Central American companies for those imports. The owners of the US business were arrested and charged with conspiracy to commit money laundering using customs violations as a predicate offence.

Source: US-HSI

Case study 14. **Gold mines operated by family alleged to be involved in drug trafficking**

The reporting financial intermediary is a privately held group of international companies which has been operating since the 19th century and whose business is precious metals. The activities of the group are executed by its companies in Switzerland and in the USA.

Two mining companies were reported by the reporting entity on June 2007. Since the establishment of a business relationship between the reporting entity and the two mining companies, all obligations of due diligence according to the Swiss Anti Money Laundering Act and the US legislation in this field had been complied with.

The two companies sent gold from the mines for refining to the reporting intermediary. Once the transaction had been executed, the proceeds of the sale were transferred to the bank accounts of the companies. However, in March 2007, a magazine article about the owner family of the two mines was published. It claimed that the family had been involved in drug trafficking and had gained its fortune through trade in firearms. In the 1980s, one family member, who was close to the actual shareholders of the two mining companies, was prosecuted for drug trafficking but was later acquitted, only to be murdered a few years later. It seemed that during the processing of the Suspicious Activity Report (SAR) the owner family of the two mining companies was in court proceedings with a Canadian company in connection with the purchase of a mine in Peru.

As there only had been press articles and no entries in the police data bases, the Swiss FIU asked the financial intermediary for further information concerning the allegations in the press articles and their accuracy. As there had been no established connection to a predicate offence or money

laundering, the SAR at that stage could not be forwarded to the Law Enforcement Authority for action. However, the Swiss FIU made a request concerning the involved persons to a foreign FIU. The Swiss FIU was promptly informed that there was an ongoing criminal proceeding against one member of this family for embezzlement.

In November 2007, there had been a further SAR from the same financial intermediary. The financial intermediary had done some additional research and established that the press articles were false. Local barristers of the group of the financial intermediary had communicated to the financial intermediary that according to their current knowledge there had been no legal proceedings raised officially in relation to the two companies and its representatives.

After receipt of the second SAR, the Swiss FIU made another request to the foreign FIU concerning the two companies and its representatives. The reply was that there was a formal criminal investigation carried out by the Public Prosecutor regarding the companies and members of the owner family. The predicate offence alleged against the family was drug trafficking.

Due to this new information, the SAR was forwarded to the office of the Attorney General of Switzerland. The assets were seized by order of this competent law enforcement authority.

Source: Switzerland FIU

Case study 15. **Proceeds of alleged fraud involved in the gold market**

A financial intermediary operating in refining and trading of precious metals sent a suspicious transaction report (STR) to the Money Laundering Reporting Office Switzerland (MROS), the Swiss FIU, in April 2014.

The reporting financial intermediary is one of the world's largest processors of precious metals and is considered among the top three in Switzerland. Behind the decision of the financial intermediary to send an STR, was the publication of 'open source' information indicating that a client had been arrested following an investigation relating to fraud, forgery of documents, drug trafficking and money laundering. After undertaking due diligence, the financial intermediary could not exclude the possibility that the assets (i.e. the gold that was to be refined) were the proceeds of crime.

The STR related to the CEO and representative of a Spanish company specialising in buying retail gold with a turnover of more than EUR 1100 million in 2013. The company described itself as a very professional trading company for gold investments. A US private equity firm specialising in buying and building companies controlled at 51% of the company. The remaining 49% belonged to a European fund, of which the CEO and the representative of the Spanish company held 49%. The company was active in the sale of gold bullion and, more recently, in acquiring jewellery and other gold pieces in order to refine and transform them in gold bullion. In 2009, its turnover was less than EUR 150 million while the following year, in 2010, it was more than EUR 500 million. In 2012, the turnover doubled from that of 2010 and was approximately 1000 million.

The Swiss financial intermediary and the company were bound by a contract, which provided for both the refining of gold and the marketing and sales on behalf of the company. Based on the

information provided by the financial intermediary and information held by the Swiss FIU, there was a question as to whether there were reasonable grounds to suspect that the concerned assets (i.e. the gold) were the proceeds of crime.

In order to receive more information MROS sent two information requests to foreign FIUs. Unfortunately, only one foreign FIU answered the information request. The other FIU, the most important from the point of view of the relevance of the information, did not respond. Finally, the STR was forwarded by MROS to the competent law enforcement authority (LEA) in Switzerland. Before starting a preliminary investigation, the LEA waited on the results of the information request and, in particular, on more information about the investigation conducted on-site and about the reliability of the information concerning the alleged crimes. Meanwhile, the aforementioned company went through bankruptcy proceedings.

Source: Switzerland FIU

Case study 16. **Source of the commodity is often not revealed and therefore a significant conduit for stolen commodity**

The United States Homeland Security Investigations (HSI) uncovered a scheme where a jewellery businessman hired a burglary ring to rob clients of previously purchased jewellery.

The jewellery businessman would sell jewellery to clients and then hire an organized burglary ring and provide them the details of the jewellery to be stolen. The information provided by the jewellery businessman contained detailed product descriptions including the residential address of the customers. The burglary ring would then target both the jewellery the customer recently purchased as well as other items of value.

During an HSI undercover operation, the jewellery businessman purchased allegedly stolen jewellery from an undercover agent and indicated that the jewellery would need to be melted and sold as scrap.

The jewellery businessmen was arrested and charged with money laundering and sale of receipt of stolen goods.

Source: US-HSI

Case study 17. **Sale of gold used as justification for movement of funds to another jurisdiction – Costa Rica**

A company operating in country A frequently sent representatives to country B offering services to buy gold, jewellery and precious stones / metals above local market prices. As a consequence of this activity, high quantities of funds were transferred from country A to country B with the reason given that the funds will be used to buy gold. The funds were then withdrawn from financial institutions in country B as either cash or cheques very soon after the funds transfer were made. Little was known about the movement of the merchandise purchased.

The same organisation organised a significant event held at a luxurious hotel in country B, advertising an intention to buy gold. However, few clients were present at the event. Monies (of unknown source) said to be surplus to the cost of holding the event were then sent back to country A or sent to other countries where the company did not operate, with the argument that they would be used for similar events.

Source: Costa Rica FIU

Case study 18. A Gold Smuggling Case of Bangladesh

A smuggler used air route for this crime. He came from Riyadh in Saudi Arabia to Dhaka, Bangladesh by Saudi Airlines.

The smuggler's luggage was scanned and found to contain items consistent with metal goods. After opening the luggage, two bottles of a well-known soft drink were found in a carton. Each bottle contains 6 gold bars of investment quality; each gold bar was wrapped with foil paper.

The luggage also contained two 135 gr bars of luxury soap, each soap contained a gold bar weighing 100 gr. In the smuggler's trouser pocket, were 77 gold chains and 2 gold earrings with a total weight of 240 gr.

The authorities did not receive intelligence on this event prior to the detection. The smuggler was passing the 'green' channel. The duty officer scanned his luggage as a routine check and found the presence of the gold.

Bangladesh has a unique operating environment when it comes to the gold market. In recent times no gold has been legally imported into Bangladesh but still the gold market is operating. The smuggling of gold, either for domestic consumption or as a transit point for other countries, has replaced the lack of legal importation. This is despite the possibility of the death sentence for smuggling gold. *Hundi* or *hawala*[13] are the most practiced method of moving value in the country in relation to the movement of gold.

Analysis by Bangladesh Law enforcement concerning the movement of gold has established that Dubai, Mascot and Riyadh are the primary wholesale markets of gold. The gold is purchased from

13 See footnote 4 for a description of *hawala* or *hundi*.

those markets and smuggled to Bangladesh, or via Bangladesh to other parts of the world. It has been established that, on occasion, such gold is used in the barter for arms or drugs. The money used to purchase the gold is sent either by currency smuggling or Hundi however little is known about the people responsible for this.

On occasions it has been established that gold is smuggled to Bangladesh as a final payment to legal businesses where the partial payment owing has been undertaken legally. On other occasions people would smuggle gold to Bangladesh for purely economic reasons, in order to profit from the different market prices of gold globally.

Source: Bangladesh Law Enforcement (Police)

Case study 19. **A gold smuggling and money laundering case - Zimbabwe**

The Tunisian FIU received a Suspect Transaction Report (STR) related to a person X whose bank account registered a large amount of funds by means of cash remittances in short period of time and sought to withdraw the money in form of US dollar cash. Information gathered by the FIU as part of its analysis revealed that person X was linked to a network of gold smuggling.

In country A, gold is a regulated sector overseen by the Central Bank. Enquiries established that person X procured gold by different illicit ways, particularly gold smuggled through land frontiers and robbery.

Person X refined the gold into ingots and gave it to air hostess A. Air hostess A had access to all the airport zones and was able to avoid the customs and police controls. Air hostess A left the ingots supplied to her in a toilet near the gates and made a telephone call to smuggler/gold courier Y and told him where she had placed the ingots.

Smuggler/gold courier Y retrieved the ingots and flew to country T. Once there, smuggler/gold courier Y delivered the ingots to person Z in return he received payment and returned to country A where he shared the profits derived from gold smuggling with person X.

A month later the Tunisian FIU received additional information on person X. On this occasion person X had used the account of a company which he owned to try and disguise his identity. This was a more sophisticated scheme to conceal the nature of the transaction however the bank was able to detect the transaction because they had already flagged his name after the first STR. Person X had deposited an amount of ZAR 2.39million (approximately USD 239 000) into his company's account where, soon thereafter a converted US dollar amount was transferred to a third party telecommunications company.

Investigations by the FIU revealed that, after depositing the South African rand into his company's account instead of seeking to withdraw the amount in the form of US dollar cash, as he had wanted to do in his earlier activity; he instead transferred the amount, in batches, over a few days, to the telecommunications company to purchase mobile air-time in bulk quantities.

Investigations revealed that person X was purchasing bulk airtime on behalf of airtime vendors in

and around Kwekwe (Zimbabwe) and that person X made the purchases using the funds that he deposited as South African rand into his company's account, and which could now be transferred as US dollar. Person X would deliver the airtime to the airtime vendors in Kwekwe, who gave him instant cash, in US dollar. Through this method, person X had achieved his objective, to convert a large amount of South African rand cash into US dollar.

Person X would then use the USD cash to make gold purchases, which he smuggled and sold outside the country.

Source: Zimbabwe FIU

Case study 20. **Using a third party account to facilitate gold smuggling and money laundering**

A Suspect Transaction Report (STR) was received by the FIU relating to person Z from bank B. Bank B had become suspicious after person Z had made several large cash deposits, in South African rand, into the bank account of a company that he owned and controlled. The deposits were followed by withdrawals of the amount in US dollars. The total amount involved was USD 6.6 million.

Investigations by the Zimbabwe FIU revealed that person Z had been conducting the transactions on behalf of a well-known gold dealer, in return for a commission. Person Z's friend person Y, was known to be involved in illegally buying gold from illicit suppliers and then smuggling the gold for re-sale out of the country. Estimates based on the amount of USD 6.6 million involved in this case, suggests that over one tonne of gold was illegally acquired, and smuggled out of the country.

Source: Zimbabwe FIU

Case study 21. **Pakistan Gold Trade – A Need for a Temporary Ban on the Import of Gold Initiative**

The Gold initiative was an initiative of the Pakistan Government to diversify exports by promoting the export of value-added gold jewellery. For this purpose, special schemes were in operation to support jewellery exporters whereby they are able to import gold without payment of any duty on the condition that the same gold was re-exported after converting it into value-added jewellery.

These schemes were referred to as the "Entrustment" and the "Self Consignment" schemes. The Entrustment Scheme provides for the export of gold jewellery and gold articles. Under the scheme, the quantity of gold exported must equal the quantity of gold imported less the wastage that occurred in the manufacture of the items to be exported. The scheme allows foreign buyers, exporters or an authorized representative to send the gold by air/sea cargo or bring gold into Pakistan personally. The Self-Consignment Scheme regulates the export of gold jewellery and gemstones taken out by authorized representative of an exporter on self-consignment basis. Stringent conditions apply under both schemes, including measures that allow authorities to

monitor and oversee all relevant shipments.

As these schemes matured, there were reports that the some of the importers of gold were circumventing the procedures under the schemes to smuggle gold in and out of Pakistan. The Pakistani rupee exchange rate also came under pressure.

The Pakistani Government then took immediate steps to prevent further damage to the national economy. It decided to impose a short-term, temporary ban of 30 days on the duty-free import of gold under these special schemes. This allowed time to restructure these schemes to remove loopholes and deficiencies while still facilitating exporters of gold jewellery to contribute to the national objective of increasing exports. These reforms included limits to the amounts of gold that can be imported by a single party, a shortening of the maximum period within which the gold must be exported in the form of value added gold jewellery, and a stricter control by Pakistan's authorities of all relevant shipments. Also, the Government of Pakistan started auditing all the duty free imports of gold for export purposes in order to ascertain the misuse of the facility.

Source: Pakistan

Case study 22. **Smuggling of gold and jewellery from Special Economic Zones**

Special Economic Zones (SEZ) are designated areas that have been created to enhance trade and in particular increase exports for the purpose of earning foreign exchange. Imports into a Special Economic Zones are allowed duty free. However due to the relaxed rules governing SEZ, these zones are also vulnerable to money laundering and tax evasion activity.

Background: Directors of the companies identified in this case study were operating in the SEZ and had extensive contacts in the gold trade in India for more than 25 years. They had previously been investigated for gold smuggling and were also known to have committed customs/foreign exchange and income tax violations. One of the directors was also the owner of a gold manufacturing and trading company operating in Dubai.

Modus Operandi: Companies A and B located inside a SEZ were authorised to manufacture and to trade in gold jewellery. This involved importing gold in either bullion form or as semi-finished jewellery from foreign jurisdictions. Generally, due to the special nature of SEZ there is no examination made by the authorities when the goods are imported or exported. These companies had opted for self-certification of the export goods as long as the activity met certain conditions.

Representatives of companies X and Y (mostly run by families) would travel abroad and select jewellery in demand in the Indian market. This jewellery would be paid for at the time of purchase in the foreign jurisdiction in which it was bought. It would then be imported into the SEZ by the companies operating there recorded as jewellery for either scrapping or further finishing.

After customs clearance the goods would be moved from the airport to SEZ (a distance of 20 km). On the way, either the employees of the relevant company or one of the directors replaced the sealed imported packets with certain other sealed packets containing brass, scrap metal or other imitation jewellery. The jewellery that had been imported was then taken and sold to customers in

legitimate gold markets.

The sealed packets containing the brass, scrap metal or other imitation jewellery was self-certified as gold and studded jewellery and subsequently exported. These exports were to their own related companies with remittances being received as required by law. This scheme was made possible due to the absence of even random checks on exports of jewellery from SEZ.

The Directors would charge their customers in INR 25 (Indian rupees) per gram of gold as a delivery charge and also offered commission of INR 5 per gram to the people coordinating the buyers in India.

Magnitude: During the investigation DRI (Directorate General of Revenue Intelligence, India) seized 79 kg of gold jewellery valued at approximately USD 3 million. Examination of intercepted export consignments declared to contain 190 kg gold jewellery with a value of USD 7 million were found to contain scrap metal. DRI seized cash close to USD 100 000. Further 30 kg gold jewellery belonging to a related company was seized valued at USD 1.2 million. A total volume of doubtful imports covered were USD 100-120 million. The total quantum of customs duty evasion amounted to USD 10 million in addition to evasion of other taxes.

Source: Enforcement Directorate of India

Case study 23. **international funds transfers in relation to gold business**

The Financial Intelligence Centre (FIC; the FIU of South Africa) obtained information that a subject, person A, received an inflow of USD 129 995.17 from the US in August 2012.

FIC investigations revealed that person A maintained four different accounts in one bank. All accounts were dormant prior to the transaction. Person A had established a company but could not provide evidence to support his gold business, although he alleged that he had been in the business for four years.

Person A claimed inflows were from his partners in the US who had jewellery shops in Europe. Person A indicated that he bought the gold from the black market and sent it to the USA. Web searches revealed person A to be among several foreign investors who had been duped by fake gold dealers. He was featured in a video filmed by Ana's Aremeyaw Anas (an Investigative Journalist) and broadcasted by Al-Jazeera.

Source: South Africa FIU

Case study 24. **Fraud relating to the export of gold jewellery**

A strategic consultant for jewellery making companies and senior employee of trading company A conspired to commit a fraud so that jewellery would be exported in the name of trading company A but other activities would be handled by the conspirators.

According to the agreement, 80% payment was to be made by trading company A to jewellery making companies after the jewellery was exported, and the remaining payment was to be made on realisation of the export proceeds which, as per terms of the agreement, was 170 days from the date of export.

In the first year of operation, all export payments were realised from overseas buyers. In the second year, while export turnover doubled, only 15% of exports proceeds were realised. On the export of the gold jewellery consignments, the conspirators would present the proof of export documents to trading company A, which paid 80% of the value of the exports immediately to the jewellery makers. In order to bridge the gap of 170 days credit, trading company A got the export bills discounted with a bank. Trading company A failed to get the export proceeds from the importers located abroad. The bank and trading company A had to thus bear the losses due to non-realisation of export proceeds. The conspirators in collusion and on behalf of jewellery makers defrauded the trading company A and the bank.

Investigation conducted by the Enforcement Directorate revealed that exports were made to companies abroad that were related to the jewellery makers. The jewellery exported by them, to related importers abroad, was sold for their gain. The advance payment received by the jewellery makers from trading company A was laundered into other businesses, such as real estate. The Enforcement Directorate traced and attached the laundered assets. The overseas investigations are in progress.

Source: Enforcement Directorate of India

Case study 25. **Ghanaian gold scam**

In August 2011, a lawyer and a self-styled traditional chief used the internet to lure a businessman from a country in the Middle East to Ghana with the offer of a supply of gold from a criminal syndicate. In this transaction, the lawyer represented both the buyer and the seller.

The buyer wired USD 3.5 million to an established bank in Ghana (bank A) and was subsequently cashed. As a result of the wire transfer, 1% of the agreed quantity of gold was supplied. When the buyer demanded the balance of the supply the criminal syndicate commenced intimidation and also solicited the help of corrupt police to chase the businessman out of the country.

The FIC commenced an investigation seeking particulars of suspects from various banks and information relating to the lawyer from other jurisdictions. This information was then disseminated to a law enforcement agency (LEA) who subsequently arrested the Lawyer and chief who were remanded in custody for two (2) weeks.

A review of the case by the office of the Attorney General found a number of flaws in the evidence which have not yet been resolved and the matter has not progressed.

Source: Ghana FIU

BIBLIOGRAPHY AND SOURCES

FATF (2013a), *Money Laundering and Terrorist Financing through Trade in Diamonds*, FATF, Paris, France, www.fatf-gafi.org/topics/methodsandtrends/documents/ml-tf-through-trade-in-diamonds.html

FATF (2013b), *The role of hawala and other similar service providers in money laundering and terrorist financing*, FATF, Paris, France, www.fatf-gafi.org/topics/methodsandtrends/documents/role-hawalas-in-ml-tf.html

FATF (2006), *Trade Based Money Laundering*, FATF, Paris, France www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

PricewaterhouseCoopers (2013), *The Direct Economic Impact of Gold* (referred to as the 'PWC Report'), PricewaterhouseCoopers LLP for World Gold Council, www.gold.org/research/direct-economic-impact-gold, accessed June 2015.

BJA and N.A.G. (2013), *The Gold Report* (referred to as the 'Gold Paper), British Jewellers' Association and the National Association of Goldsmith's of Federation House, Birmingham and London resp., United Kingdom, www.cibjo.org/download/gold_paper_feb2013_formatted.pdf, accessed June 2015.

PROJECT TEAM

Balesh KUMAR

Special Director
Enforcement Directorate,India
E-mail: balesh.kumar@nic.in

Nicholas McTAGGART

Detective Superintendent
Criminal Assets Confiscation Taskforce
Serious Organised Crime
Australian Federal Police
E-mail: nicholas.mctaggart@afp.gov.au

SPECIAL RECOGNITION

The Co-Leaders of the project would also like to extend a special thanks to Mr Anil Rawal Assistant (Director, Indian Enforcement Directorate, email: anilk.rawal@nic.in) who has provided valuable support and significant contribution to the Project in the area of statistical collection and analysis.

www.fatf-gafi.org | www.apgml.org

July 2015

This report identifies the features of gold and the gold trade that have made it an alternative means for criminals to transfer value and generate proceeds. Gold is anonymous, has a stable value and is easily transformable and transportable, which have made it an attractive alternative for criminals to store or move and generate value as regulators implement stronger anti-money laundering / counter terrorist financing (AML/CFT) measures to protect the formal financial sector from abuse.

This report provides a series of case studies and red flag indicators to raise awareness, particularly with AML/CFT practitioners and companies involved in the gold industry, of the key vulnerabilities of gold and the gold market.

Appendix XX:

FATF, *FATF Report: Money Laundering and Terrorist Financing Through Trade in Diamonds* (Paris: FATF, 2013)

FATF

EGMONT

FATF REPORT

MONEY LAUNDERING AND TERRORIST FINANCING THROUGH TRADE IN DIAMONDS

October 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

The goal of the Egmont Group of Financial Intelligence Units (Egmont Group) is to provide a forum for financial intelligence unites (FIUs) around the world to improve cooperation in the fight against money laundering and the financing of terrorism and to foster the implementation of domestic programs in this field.

For more information about the Egmont Group, please visit the website:

www.egmontgroup.org

Table of Contents

ACRONYMS

AML	Anti Money Laundering
ATA	*Admission Temporaire/*Temporary Admission
AWDC	Antwerp World Diamond Centre
CFT	Counter Financing of Terrorism
CTR	Currency Transaction Report
CDD	Customer Due diligence
DD	Diamond dealer
DDA	Designated Diamond Account
DNFBP	Designated Non-Financial Business and Professions
DPMS	Dealers in Precious Metals and Stones
EDD	Enhanced Due diligence
FC	Foreign Currency
FIU	Financial Intelligence Unit
FTZ	Free Trade Zone
HS	Harmonized Commodity Description and Coding System
JA	Jewellers of America
KP	Kimberley Process
KPCS	Kimberley Process Certification Scheme
KYC	Know Your Customer
ML	Money Laundering
MSB	Money Service Business
RTGS	Real Time Gross Settlements
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TF	Terrorist Financing
UAR	Unusual Activity Report
UTR	Unusual Transaction Report
WFDB	World Federation of Diamond Bourses

EXECUTIVE SUMMARY

This report, examining Money Laundering (ML) and Terrorist Financing (TF) vulnerabilities related to the trade in diamonds, began as an Egmont Operational Working Group project in February 2012. In June 2012, the project was also adopted by the Financial Action Task Force (FATF) and it became a joint FATF and Egmont typologies initiative. There were two main reasons for the Egmont Group of Financial Intelligence Units (FIUs) and FATF to commission typologies research into the diamond trade:

a) Neither FATF, Egmont Group nor any of the FSRBs had ever conducted an in-depth research of the diamond trade and its exposure to ML/TF risk.

b) During the last ten to fifteen years, Egmont and FATF delegations noted a number of indications that the diamonds trade was being exploited for ML/TF purposes.

Given the limited research into ML/TF through the trade in diamonds, the report provides a basic overview of the subject matter and then focuses on ML and TF issues. **Chapter 2** provides a general overview of the international trade in diamonds. The distinction between the use of diamonds themselves and the exploitation of the trade in diamonds which is conducted through financial institutions or alternative/internet payment mechanisms is important to note. Diamonds and the diamond trade can be used in all stages of ML (placement, layering and integration) and for the stages of TF (collection, transmission, and use).

The research conducted has brought to light evidence that the diamonds trade is subject to considerable vulnerabilities and risks, creating a challenge for both stakeholders within the industry and relevant national authorities for AML/CFT. The contributions from the project team and consultation with private sector have shown that the various entities within the diamond industry on both national and international level have made efforts to counter ML and TF risks.

The diamonds trade has existed for centuries. It has developed a unique culture and trade practices, which have their own characteristics and variations across countries and continents.

However, the international diamond trade has changed in the last few decades:

- De Beers no longer holds the same all inclusive diamonds monopoly.
- A number of smaller diamond dealers have entered the market.
- Distribution channels have become more diverse.
- New trade centres have emerged with billions of dollars' worth of diamonds, and financial transactions go in and out of newly founded bourses and their ancillary financial institutions.
- Cutting and polishing has shifted (except for the most valuable stones) from Belgium, Israel and the US mainly to India and China, with smaller cutting centres emerging.
- Cash transactions are still prevalent but the usage of cash is diminishing.

- The internet, as in all other facets of life, is rapidly taking its place as a diamonds trading platform.

These significant changes in the "diamonds pipeline" structure and processes raised the question of whether the risks and vulnerabilities remain the same and whether current AML/CFT standards and national regulations are sufficient to mitigate the different ML/TF risks and vulnerabilities identified in the research.

While the level of risk posed by the misuse of the diamond trade may not be accurately established within the scope of this report, the analysis conducted within the framework of the current research identifies issues affecting the level of risk posed by criminals seeking to misuse the trade. **Chapter 6** provides a detailed analysis of the risks and vulnerabilities, including

a) ***Global nature of trade*** - The trade in diamonds is transnational and complex, thus convenient for ML/TF transactions that are, in most cases, of international and multi-jurisdictional nature. This, in turn, may create difficulties for national law enforcement to conduct investigations and necessitates international cooperation between law enforcement agencies across countries in which the trade is taking place.

b) ***Use of diamonds as currency*** - The research noted criminals' use of diamonds as a form of currency[1] is a characteristic unique to the diamond trade[2]. Diamonds are difficult to trace and can provide anonymity in transactions.

c) ***Trade Based Money Laundering (TBML)*** - This is one of the most common methods used by criminals to launder illegally gained funds. The specific characteristics of diamonds as a commodity and the significant proportion of transactions related to international trade make the diamonds trade vulnerable to the different laundering techniques of TBML in general and over/under valuation in particular. This should be viewed in light of the significant world annual trade volume which includes rough diamonds, polished diamonds and diamond jewellery[3].

d) ***High amounts*** - cases show that the trade in diamonds can reach tens of millions to billions of US dollars. This has bearing on the potential to launder large amounts of money through the diamond trade and also on the level of risks of the diamonds trade.

e) ***Level of awareness of law enforcement and AML / CFT authorities*** (including FIU awareness) to potential ML/TF schemes through trade in diamonds is low in most countries. This can be seen in the trade statistics provided by the project team: there are almost no reports that were filed by precious stones dealers to FIUs and very few intelligence reports have been disseminated by FIUs to law enforcement agencies. The complexity of the diamonds trade requires particular study and expertise to analyse and evaluate the financial

---

1 For example, instances have been found where diamonds were used to pay for and to finance drug trafficking.

2 Within the regulated sectors according to the FATF recommendation, this is a characteristic of precious metals and stones in general.

3 In 2011 the rough trade in diamonds amounted to approximately USD 51 billion and the polished trade in diamonds amounted to USD 214 billion (see Figure 5, p. 33).

and trade transactions. The opaque and closed nature of the diamond industry are also obstacles to investigations of ML/TF by Law Enforcement Agencies, which in many cases are unaware of the benefit and the possibilities for ML which diamonds may allow.

f) There are cases, even though relatively few, indicating that the diamonds trade has also been used for TF during the last 10 to 15 years.

g) All this is conducted within an industry where, although efforts to reduce such trade practices have been made, the traditional ethics of trust are an integral part of the trade culture and record keeping is minimal.

Chapter 7. of the report provides red flags and indicators based on analysis of country contributions and red flags derived from submitted cases:

a) Red flags and indicators for regulated entities.

b) Red flags and indicators for diamond dealers and jewellers.

c) Red flags and indicators for customs.

Chapter 8 and **Chapter 9** provide an analysis of the different methods and techniques used for ML and TF. In total, 64 cases were received from team members or retrieved from open sources. From the cases collected, 38 cases were used in the report. Cases collected displayed links between the different stages of the diamonds trade and various predicate offences. These include drug trafficking, fraud, smuggling, theft and robbery, large scale tax offences, forgery and fictitious invoices among other offences. Drug trafficking and smuggling were found to be the most prevalent predicate offences.

Almost 50% of the cases concerned non-cash payment means. Cash as the sole method of payment was reported only in 10% of the cases. These figures echo one of the main conclusions of the report that the extent of cash usage in the trade is growing smaller. This has significance with respect to the FATF definition of *Dealers in Precious Stones* and the AML/CFT standards which apply to Diamond Dealers only when they engage in cash transactions with their customers. Taking into account the risk and vulnerabilities identified in the report which does not relate to cash usage the FATF definition of Dealers in Precious Stones is an issue to be further considered.

The vulnerabilities and risks of the diamonds trade noted in the report are made in general terms. However, it should also be stressed that since the trade in diamonds is dependent upon the trade characteristics pertaining to each jurisdiction in question, it is important to understand that there may be considerable differences in the level of risk between countries and a more country specific evaluation of risk is required. With respect to jurisdiction where diamond trade is a significant part of the economy or where trade volumes are high it should be considered by relevant national authorities to incorporate the diamonds trade as part of their national ML/TF risk assessment.

Generally speaking, international AML/CFT regulation must be as consistent as possible, in order to obstruct the laundering of proceeds of crimes and to prevent terror financiers to achieve their goals. Wherever loop holes exist in the AML/CFT standards, regulations or enforcement, criminals will tend to utilise them for their ML/TF transactions.

Other precious stones – Finally, the scope of the project was narrowed in February 2013 from ML and TF through trade in diamonds and other precious stones to the diamond trade only.

Information collected, before limiting the scope to diamonds, shows the use of gold and other precious stones for ML/TF purposes. The information is provided here without further analysis as an awareness raising step and as an indication that further research is required on this topic.

Important remarks - In this report, when reference to the diamond trade is made, this is taken to mean all the sectors noted in **Figure 1 – diamond pipeline diagram.** Where possible, the different parts of the industry will be distinguished: production, rough diamond sales, cutting and polishing, jewellery manufacturing and jewellery retailers.

The term diamond dealers refers, throughout the report, to a person dealing in rough or polished loose diamonds (mostly business to business). Unless otherwise specified, the term does not including diamond jewellers (mostly business to consumer).

CHAPTER 1.
INTRODUCTION

Banks and other financial services have traditionally been the preferred conduit for ML and often the ultimate destination for laundering proceeds of crime. Global efforts to mitigate the risks of ML/TF through financial services have reduced the likelihood of ML/TF through this sector. Through country specific legislation and international cooperation promoted by the FATF and Egmont Group, criminals have been challenged in their ML/TF activities. The implementation of AML/CFT measures has forced criminals to seek out other methods to launder the proceeds of their crimes. The ML aspect of the criminal enterprise has become more complex and sophisticated in order to conceal and disguise profits gained by their criminal activity and the origin of such profits. As a result, other business sectors have been targeted by criminals including the precious metals and precious stones industries, and specifically the trade in rough and polished diamonds and diamond jewellery.

The diamond sector as a Designated Non-Financial Business and Profession (DNFBP) is different in some respects from financial institutions and other DNFBPs. Diamonds are a commodity traded in international markets. The diamond trade is a dynamic international trading sector, where a significant amount of business is transacted through financial institutions. They are used not only for trade but also for investment purposes, although probably to a limited extent. Diamonds are traded mainly through dozens of bourses and cutting and polishing ('manufacturing') centres around the globe. As this research has discovered diamonds are also used as a form of currency, which distinguishes this industry from other trade based DNFBPs such as real estate agents and most trade based industries. The use of diamonds as a form of currency or as a means of payment is of significance from an AML/CFT perspective.

The FATF recognised that diamonds and other precious stones are vulnerable to ML/TF by including the diamonds and precious stones dealers under the definition of DNFBP when they engage in cash transactions with their customers above an applicable designated threshold. The FATF Report on Money Laundering Typologies 2002-2003[4] recognised the inherent risk that diamonds and other precious stones pose as a ML commodity.

This 2002–2003 typologies report identified cases where diamonds and the trade in diamonds have been exploited for ML and TF purposes. However, the team undertaking this project found that in many cases, Financial Intelligence Units (FIUs) and Law Enforcement agencies know little about diamond trade business practices, the methods of its utilisation for ML or TF and the typologies of the criminal exploitation of the diamonds trade, in comparison to their awareness of other types of ML/TF activities.

As will be detailed later in this report, the diamond trade was found to be linked to different predicate offences, including to offences conducted by organised crime, such as drug trafficking, illegal weapons trade and tax offences, as well as to ML offences. Additionally, one of the

4 FATF (2003)

complexities noted in the laundering activities that utilize diamonds is that diamonds can be both the vehicle to generate criminal profits as well as the vehicle to launder them.

Documented[5] cases of terrorist utilization of diamonds are few; however it should not automatically be assumed that terrorist utilization is uncommon because of the limited case examples that have been published. Often, law enforcement and intelligence organisations have documented the factual details that are not released to the public. Unless the use of diamonds leads to an arrest or criminal charges as the case may be, these details will not be made public. In addition, this knowledge may not be shared as willingly as criminal use of diamonds due to national security concerns.

Before the implementation of the *Kimberley Process*, researchhad shown that diamonds had been exploited extensively by war criminals in many African civil wars by a multitude of rebel and government forces, to exercise the acquisition of munitions. Some of the war lords and militia commanders had mastered the art of converting illicit diamonds into arms. Historically this may be the greatest example of terrorist or terrorist-like utilisation of diamonds.

The business practices prevalent in the diamonds trade are unique:

- Confidentiality of transactions.
- Agreements made by word of mouth.
- Deals conducted via a diamond bourse located in Free Trade Zones (FTZs)
- "memo" transactions.

Alongside, these factors, the diamonds trade is also characterised high value to mass ratio, million dollars' worth of diamonds may be carried across borders either legitimately through trade or illegally (*e.g.*, smuggling) with relative ease. These characteristics make diamonds a commodity vulnerable to exploitation by transnational criminal organisation and terrorist groups seeking to transfer value or legitimise illicit transactions and profits[6]. These characteristics, among others, also mean that the trade is difficult to monitor by regulators and law enforcement agencies.

The FATF definition of ML is based on the definitions included in the UN Vienna and Palermo Conventions. These definitions note that ML includes the acquisition, possession, concealment or disguising or conversion / transfer of property derived from criminal offences (listed as designated categories of offences by the FATF). Examining ML in its broadest sense, diamonds may be:

a) acquired as a "property of an offence" (theft of diamonds);

b) used to conceal or disguise "proceeds of crime" (as they are a high value/low mass good and relatively easy to hide from detection); and

c) converted into other financial instruments or conveyed or transferred relatively easily across borders and hold their value for a very long period of time. *I.e.,* diamonds are liquid assets.

5 See for example: GAO (2003); Global Witness (2003); and Douglas Farah (na).

6 FATF (2003), *pp.* 21- 24.

The flexibility of diamonds as a commodity that can generate profit, retain value and serve as means of payment, in conjunction with traditional ethics of trust and undocumented trade practices, indicate the potential for diamonds to be used as a laundering mechanism and why this industry is worthy of further examination by AML and CFT authorities.

I. REASONS FOR CONDUCTING THE RESEARCH

The FATF last conducted a typologies research on the topic of diamonds in 2002-2003. This typologies report was not dedicated fully to the topic of diamonds but rather covered several issues each in a very limited way. Diamonds as a topic for a typologies research has not been dealt with by the FATF nor by FATF-Style Regional Bodies (FSRBs) leaving the issue in need of attention. The purpose of this research is to create a better understanding of the diamond trade and in particular the "diamond pipeline", including the vulnerabilities and risks facing the trade.

The diamond industry (rough, polished and jewellery) is international in character, and demand for diamonds remains high. The whole industry "pipeline" needs to work so that rough diamonds can find their way from the earth as a rough diamond to a cut and polished diamond in someone's necklace, watch or ring. While the value of rough diamond production amounts to USD 14.06 billion[7] annually, the financial volumes of the trade on all its parts amount to hundreds of billions of dollars every year. In many countries the diamond industry has become an important economic factor.

Indications exist that point to the misuse of the legitimate diamond trade. NGOs such as Partnership Africa Canada, and government bodies, such as the US Government Accountability Office (GAO) have researched and published information revealing investigations involving the use of diamonds for ML. However, it remains an open question as to what extent the diamond industry itself has been exploited for ML/TF.

AML/CFT authorities recognise the potential risk of misuse of the diamond industry. The IMF has been engaged in Technical Assistance with African countries that produce and deal in diamond, gold, and precious metals to strengthen their defences against ML, smuggling, and TF. The IMF noted that: "the trade in precious minerals has been linked to illicit financial flows, corruption, drug trafficking, arms smuggling and the financing of terrorism[8].

II. AIM AND OBJECTIVES

The diamond trade is global in nature and can be highly complex. The characteristics of the trade vary along the supply chain and by location, whether it is African mining countries, diamond trading centres like Belgium, US, Israel and Dubai, or manufacturing centres such as India and China. For this reason this report aims at the outset to provide a general overview of the diamond industry, the way it works and the characteristics of diamonds as merchandise, through an AML and CFT lens. The aim is to provide the basic knowledge needed in order to have a better understanding of the

7 According to KPCS statistics for the year 2011.

8 IMF (2010).

manner in which the diamond trade / industry operates and the way this sector might be exploited for ML and TF purposes. This overview is provided in **Chapter 2** of the report.

In 2008 the FATF, in consultation with the private sector[9], published a ***Risk Based Approach (RBA) for dealers in precious metals and stones*** (DPMS). This document conducted an analysis of risks which may be considered by both dealers in precious metals and precious stones in the application of the risk-based approach to the dealers' activity. One of the main aims of this typologies project is to identify up-to-date ML and TF vulnerabilities along the different parts of the "diamond pipeline", with a specific focus on international trade and the unique characteristics of rough and polished diamonds that make them vulnerable to criminal activity, as well as an evaluation of the risks associated with the vulnerabilities of the trade. This may also assist concerned parties in enhancing their application of a RBA for precious stones with respect to the diamond trade.

Additionally, the typologies report also aims to:

a) Identify "red flags" and indicators which will enable financial institutions, diamond dealers and law enforcement to recognise cases of abuse of the diamond trade and increase unusual/suspicious activity reports to FIUs. Identifying "red flags" will also assist the relevant entities in assessing the risk of their own transactions.

b) Identify known and new typologies / case examples in the diamond industry based on case examples and open source information, and establish ML/TF trends in the global diamond trade. In particular, the project aims to contribute to a better understanding of the extent to which the diamond trade is used by criminals to launder proceeds generated in predicate offences and to what extent diamonds are used for this purpose.

c) The report also aims to outline relevant policy implications by:

   i. Examining the current FATF standards with respect to the diamond trade and identifying any need for further consideration, enhancement or amendment.

   ii. Identifying best practices for AML/CFT regulatory and supervisory approaches to the precious stones industries and specifying policy implications where needed. Furthermore, if required, develop a specific set of issues for consideration that may assist both the diamond and financial sectors and national competent authorities.

III. METHODOLOGY

The methodology adopted in this project deviated from the common practice of sending a questionnaire to all FATF/Egmont members to collect information. It was decided, rather, to create a diverse group of team members from countries of importance and/or relevance to all facets of the diamond trade to collect country-specific information and to take part in the report drafting. All countries where diamond centres or diamond mines are located were invited to take part in the

[9] The following diamond and jewellery industry representative bodies were consulted for the 2008 report: Antwerp World Diamond Centre (AWDC), International Precious Metals Institute, World Jewellery Confederation (CIBJ), Jewelers Vigilance Committee (JVC), World Federation of Diamond Bourses (WFDB), and the Canadian Jewellers Association.

project. The countries that joined the project included: Argentina, Australia, Belgium, Canada, India, Israel, Mexico, the Netherlands, Russia, South Africa, Switzerland and the US. Two FSRBs (GIABA and ESAAMLG) joined the project to serve as liaisons to African mining countries. The members represent a significant part of the international "diamond pipeline", namely: Mining[10] and production, trade and manufacturing centres, distribution and jewellers[11].

However, it is important to note that, the report would have benefitted from additional information from specific input of production countries and major trade centres. For example, United Arab Emirates, one of the world largest trading centres for diamonds (with trade volumes amounting to more than USD 40 billion). The lack of information from the United Arab Emirates leaves an intelligence gap which may cause an imbalance in the results of the research. This is also true for most of the African mining countries which supplied little or no information on the mining sector (*e.g.,* Botswana, Sierra Leone, Namibia and the Democratic Republic of Congo (DRC)).

A comprehensive collection plan was devised and distributed among team members. The objectives of the collection plan were as follows:

a) **Create a better understanding** of the manner in which the diamond trade is operating from mining of rough diamonds through trade and cutting centres to the retail level of jewellery shops where polished diamonds contained in jewellery are at the end of the value chain. This included information on customs, cross-border regulation, taxation and funding made available via financial institutions.

b) **Identify "red flags"** both in the trade of rough and polished diamonds to help diamond dealers and jewellers[12] recognise transactions which may be linked to ML or TF activities; these may also assist the financial sector providing services to the diamond sector. Red flags may also be used by FIUs and law enforcement while investigating cases involving the trade in diamonds.

c) **Diagnose the vulnerabilities** and **the level of risk** associated with different parts of the trade.

d) **Collect information on money flows** related to ML or TF from the different countries, in order to identify discrepancies between countries and indications for possible ML and/or TF activities.

e) **Collect information on sanitized and actual cases** from FIUs and law enforcement.

f) **Identify associated predicate offences** with the trade and financing of the trade in diamond.

---

10 There is a previous stage to mining which is the exploration stage whereby governments and specialized diamond companies such as Alrosa, De Beers and Rio Tinto search for new site of diamond mining. The report is not looking into this phase since it precedes the actual trade in diamonds.

11 Based on KP statistics for the year 2011 (rough diamonds only) the team members covered in terms of trade volume 95% of the mining sector and approximately 83% of the import and export of rough diamonds.

12 The FATF definition applies to dealers in precious metals and stones. The scope of the report is the diamond trade only; however, the identified red flags may also aid dealers in precious stones in general.

g) **Engage national players** relevant to the diamond trade in each member jurisdiction to facilitate the collection of information.

A limited collection plan was also sent to additional countries identified by the project team as relevant to the diamond trade. These included: China; Hong Kong, China; Singapore; Switzerland, Thailand; the United Arab Emirates; and the United Kingdom.

An open source survey for actual ML/TF cases involving diamonds was conducted and information on these cases was requested from the relevant countries (Australia; Belgium; Brazil; Hong Kong, China; Israel; South Africa; Switzerland; United Kingdom; United States; Zimbabwe[13]). These open source cases where also used in the typologies analysis section.

In November 2012, a typologies workshop was held in Dakar, Senegal within the GIABA/FATF joint expert meeting on typologies, produced relevant material to the report. Several presentations were given by the participants. Additionally, team meetings were held to discuss findings[14].

Several team meetings included consultations with the private sector aimed at better understanding the trade in diamonds and its vulnerabilities as perceived by the private sector and verifying the information previously collected. Consultations were conducted with Jewelers of America and the World Federation of Diamond Bourses (WFDB).

Additional private sector consultations took place during the end of August 2013 and the beginning of September 2013, just prior to the final project team review and submission of the report to the FATF and Egmont for approval, to verify the factual information regarding the diamond trade. The draft report was sent for comments to the following private sector representatives: WFDB, Jewellers of America, a consultant gemmologist to the crown in Canada, an expert from the UN Group of Experts on Côte d'Ivoire and a representative from Kimberley Process to review information on KP sections of the report.[15]

IV. SCOPE

The project was initially envisioned in two-phases, with the first stage focusing on ML / TF through the trade in diamonds and other precious stones and the second phase focusing on ML / TF through the use of precious metals. This was in accordance with the FATF definition of precious stones dealer as a sector included in the Designated Non-Financial Businesses and Professions (DNFBPs). The project was initiated at the first stage with an aim to conduct a typologies research to cover both diamond and other precious stones but would not cover precious metals.

---

13 As of 3 June responses had been received from Australia, Brazil, Israel, Switzerland, the United Kingdom and the United States.

14 Team meetings were held in July 2012 in St. Petersburg, Russia in the margins of the Egmont Own meeting; January 2013 in Ostend, Belgium in the margins of the Egmont OpWG meeting; February 2013 in Paris, France in the margins of the FATF WGTYP meeting; June 2013 in the margins of the FATF WGTYP held in Oslo, Norway a meeting which included consultation with private sector representatives.

15 The authors of the report noted that the same terminology was sometimes used differently by some private sector experts that contributed to this report. Every effort has been made to use the same terminology consistently.

During the team meetings in February 2013, the project team decided to narrow down the research to cover only diamonds. As the project progressed, and as more information became available giving a better picture of the scope of the issue, it became clear that the diamond trade alone is a vast area of research justifying a focused effort of its own. For the same reason, synthetic diamonds were also excluded from the scope of the research.

Since one of the objectives of this report is to create a better understanding of the misuse of the diamond trade for the purpose of ML or TF and to understand how the diamond trade is used by criminals to launder funds from illegal activities or to finance terrorism, the project team also decided that "conflict diamonds" would not be part of this research

Each part of the "diamond pipeline" has its own characteristics and different geographical locations. In many cases the "players" are different, and the vulnerabilities and risks correspond to the nature of each "pipeline" segment. The project team found that the collection of information on all of these parts, and the analysis of this information within the framework of AML/CFT vulnerabilities and risks, was a difficult and time-consuming task. Based on all the information collected, the project team identified vulnerabilities. However, since not all of the jurisdictions approached by the project team provided information, there are some intelligence gaps[16]. In order to stay within the timeframe allocated to this project, these intelligence gaps have not been included in the report, leaving the diamond trade in need of further research (particularly with reference to African mining countries and some trade centres like China, Panama and the United Arab Emirates).

Given that the diamond trade is very complex, involving numerous players spanning across continents, it would be difficult within the framework of this report to conduct a country by country analysis of the vulnerabilities and risks relevant to the diamond trade. As a result, the report speaks mainly in general terms with regard to vulnerabilities and risks associated with each part of the trade, and considers geographical vulnerabilities and risks where appropriate.

Finally, the quality of diamonds can be divided into *gem*, *near gem* and *industrial* grade categories. Industrial grade diamonds have different markets and are not used for the production of jewellery due to their low quality. According to the WFDB, 30 - 35% of the volume (less than 1% by value) of mined diamonds and a large proportion of synthetic diamonds are used for industrial purposes. Since the ML and TF vulnerabilities of industrial diamonds are lower than gem quality diamonds, industrial diamonds are not part of this research. When speaking about diamonds, this research is referencing only those diamonds which are eventually used for the manufacturing of jewellery, *i.e.,* gem and near gem quality.

[16] Some intelligence gaps remain since information was not received from all jurisdictions approached by the project team.

CHAPTER 2.
THE INTERNATIONAL TRADE IN DIAMONDS - OVERVIEW

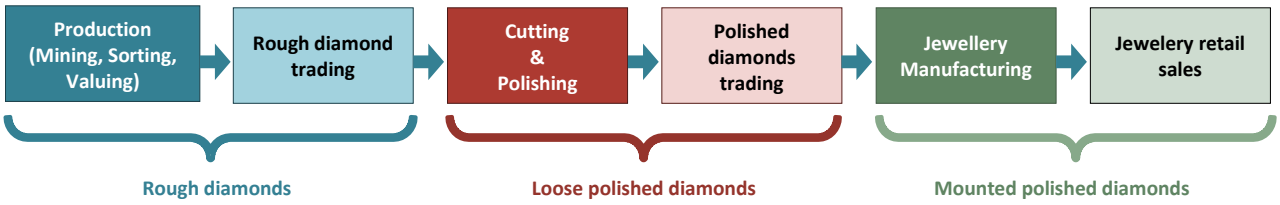
In order to understand the vulnerabilities of the diamonds trade throughout the various stages of the "diamond pipeline" and the risks associated with these vulnerabilities, it is required to understand how this unique and complex industry works, what are the processes bringing diamonds from the mine to the market, who are the "players" involved in the trade, what is the size of the industry, etc. While it is not the purpose of this report to provide a comprehensive analysis of the diamond industry, a synopsis of the sector from mining of rough diamonds to the retail level, is provided.

THE DIAMONDS PIPELINE

Bringing diamonds from production (mining) to the retail consumer involves several stages of processing and a variety of transactions (also known within the industry as the "diamond pipeline"). The stratification of the diamond industry is as follows:

- Production (including mining, sorting and valuing)[17]
- Rough diamond trading / sales
- Cutting and polishing
- Polished diamond sales
- Jewellery manufacturing
- Jewellery retail sales

Figure 1: **Diamond pipeline diagram**

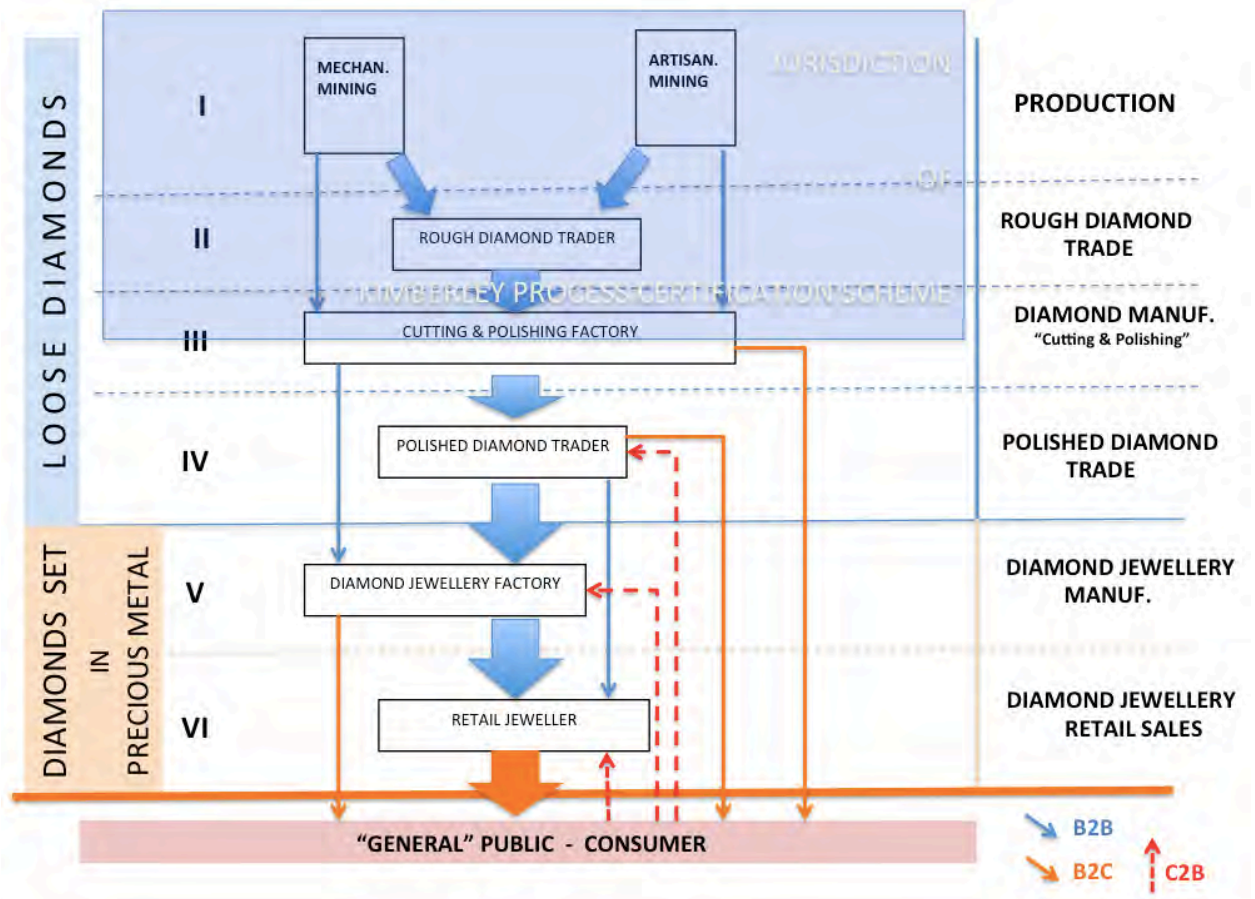


Note: This only represents this licit diamond trade.

A more complex version of the "diamond pipeline" from the post rough diamond sales step in the previous graphic, is the following version provided by industry organisations. However, even this is a far from comprehensive demonstration of the reality.

[17] There is a previous stage of exploration where diamond mines are searched for. This stage precedes the trade in diamonds and therefore it is not covered in the report.

Figure 2: **Diamonds distribution system**



Source: Information provided by industry organisations (2013)

Within this string of transactions and processes, the diamond industry has two distinct components[18]:

> **Mining and Manufacturing**, which is the segment of the industry that deals with rough diamonds and includes diamond mining through to rough diamond cutting and polishing.
>
> **Jewellery Manufacturing and Sales**, which is the segments that deals in finished (cut and polished) diamonds and includes polished diamond dealing on through to jewellery retailing.

Production - The diamond industry begins with the mining of diamonds in the production segment. Generally speaking there are a few primary locations for diamond mining the world over. These are **South, Central and West Africa, Russia, Australia and Canada**[19]. The diamond trade in most of the African mining countries is of high economic importance accounting for a large part of the GDP and export earnings.

---

18 In recent years this delineation has become, to some extent, less distinct due to vertical integration of diamond trading companies and branding of diamond jewellery. In some cases even rough diamonds companies are linked to jewellery companies.

19 There are also additional locations with a small mining sector in South America. India also produces rough diamonds worth several million dollars a year.

Diamonds occur in *kimberlitic* hard rock deposits or *alluvial*/fluvial deposits. Hard rock mines are those in which a kimberlitic pipe (and occasionally lamphorite), the host rock where diamonds are found in, is blasted from the surrounding rock and crushed to release the diamonds contained within it. *Alluvial* mining is the extraction of diamonds from river bed, sea floor, or beach deposits. They are referred to as secondary sources, since the diamonds in alluvial deposits were removed from kimberlitic mines (primary source) by natural erosion. Techniques used to collect the alluvial diamonds can be divided to industrial mechanized mining when specific conditions which make alluvial industrial mining economical are met or artisanal mining which involves diggers working in teams with simple implements such as picks, shovels and sieves. According to the literature review[20], contributions received from some of the mining countries (Australia, Botswana, Canada, Russia Sierra Leone and Zimbabwe) and discussions conducted in the workshop held in Dakar, kimberlitic mines are smaller in terms of geographical area and are much easier to secure than alluvial mines which may spread across huge geographical area which cannot be isolated. Kimberlitic mines are also highly mechanised with strict controls, while alluvial deposits (mainly artisanal) are more difficult to control because the diamonds can be extracted without large industrial machinery[21].

Loose / mounted diamonds

A distinction exists between *loose* and *mounted* diamonds.

Loose diamonds are cut and polished diamonds which have not yet been set in jewellery while mounted diamond is a polished diamond which was set in jewellery such as ring, watch necklace, etc. The regulation of loose and mounted diamonds are usually very different.

The next step of the production stage will be to sort and evaluate the diamonds and have them ready for sale. Sorting and valuation are done by dividing the diamonds into different groups according to their quality and value. This process will provide added value to the price of the rough diamonds. An important issue to understand is that when the report refers to diamonds, it covers a range of products. The price of a diamond, rough to polished, can vary from few tens of dollars per carat to tens of thousands of dollars per carat for a cut and polished diamond[22].

Rough Diamond Trading and Sales - Diamonds recovered from mining processes are purchased by rough diamond dealers through the global diamond markets. Purchases are usually arranged through diamond bourses (although there are different methods for the purchasing of rough diamonds) in countries such as **Belgium, UK, India, Israel, and the United Arab Emirates (Dubai)**. While many of these centres are located in countries that have no diamond production themselves, their rough diamond trading industry has evolved over decades or hundreds of years. A diamond bourse or exchange is a private commercial business with membership restricted to individuals only (not companies). The bourse provides a trading floor where members and buyers

20 For explanation on the difference between the two types of mines (kimberlitic and alluvial) please refer to World Diamond Council (nc). See also Diamonds A to Z (nc).

21 Comments from received from AWDC and information from World Diamond Council (nc).

22 See for example Pricescope (nc). See also, Evan-Zohar, C. (2004), *pp.* 97-98.

meet to trade in rough and polished diamonds[23]. Globally there are 29 diamond bourses affiliated with the World Federation of Diamond Bourses[24]. Other localised markets may exist in proximity to diamond mining locations, where street vendors purchase diamonds from artisanal miners. This is a vulnerable stage since it is very hard to control, as will be explained later. The diamonds are sold to regional dealers and then often to global diamond markets. The rough diamonds may be sold several times between rough diamond dealers and several diamond bourses before they are ultimately sold to a diamond cutter/polisher[25].

Rough Diamond Cutting and Polishing - The beauty of a diamond is realised through cutting, faceting and polishing. Cutting and polishing centres exist in several parts of the world, with major centres existing in **Belgium, India, Israel and China.** Once the diamonds are cut and polished they are ready for use in jewellery and are moved along the "pipeline" to be utilised in diamond jewellery manufacturing and sales. The transformation from a rough to a polished diamond is another vulnerable stage, as a diamond becomes much more difficult to track once it has been cut and polished[26]. Whilst it is possible to judge when certain diamonds were polished using antiquated techniques, for the vast majority of polished diamonds on the market it is virtually impossible to ascertain when they were polished. All diamonds one might view in a shop window might not be first hand goods.

Diamonds Dealers – Once the diamonds have been cut and polished, they are ready to be sold for use in jewellery and, to a very limited but growing market, as an investment product. Diamond dealers are the first merchants of diamonds after they have been cut and polished, and often handle hundreds of millions of dollars' worth of diamonds every year. These dealers usually operate from the major diamond dealing centres of the world including **Antwerp, London[27], New York, Tel Aviv** and in **Dubai, India** and **China**. Their clients include other diamond dealers, large diamond jewellery manufacturers and diamond wholesalers.

Diamond Wholesalers – This segment of the industry deals in smaller amounts of diamonds. They often deal with specific products, such as size or quality spectrums of diamonds or diamonds with fancy cuts or patented cut styles and they are often involved in branding their diamonds. This segment of the industry usually sells to jewellery retailers, but is increasingly selling directly to the consumer.

Diamond Jewellery Manufacturers – Structurally, organisationally, and operationally the jewellery sector is quite distinct from the diamond sector. The jewellery sector also deals in gold, other precious stones, silver, platinum and a range of other raw materials. The financing and capital structure are also entirely different. Some of the larger diamond jewellery manufacturing centres now exist in Asia (**China, Chinese Taipei and Indonesia**). Jewellery is manufactured and may be

23 Although most transactions today are conducted through diamond dealers' offices.

24 World Federation of Diamond Bourses (nc).

25 According to Chaim Even-Zohar the diamond goes through six to ten hands from the mine until it reaches the final customer, Evan-Zohar, C (2007b), pp 114.

26 The Kimberley Process Certification Scheme (KPCS) only covers rough diamonds.

27 In November 2013 De Beers will move its operations from London to Gaborone, Botswana.

sold to jewellery wholesalers and then on to jewellery retailers. Increasingly, the manufacturer is selling directly to jewellery retailers and consumers.

Jewellery Retailers – Diamond jewellery sales is the driver of the diamond industry and this occurs through retail jewellery sales. All of the processes that have previously occurred are in support of this segment of the industry. Diamond jewellery sales occur in virtually all countries of the world through brick and mortar vendors. Vendors exist as single independent stores or large corporate chains with hundreds of stores. Increasingly the internet is being utilised to market and directly sell diamonds and diamond jewellery to the consumer.

Pawn shops – polished diamonds and jewellery are also sold through pawn shops (*i.e.,* diamonds or diamond jewellery will be placed as collateral for loans extended, and only when the borrower defaults, the pawn shop owner takes possession of the collateral). Jewellery can then be resold to jewellery stores, pawn shops, lately to wholesalers, and at special fairs conducted for this purpose. Someone who wishes to sell his or her personal jewellery (in order to repay debts, sell jewellery from inheritance, etc.) can do so at these venues.

BUSINESS PRACTICES AND CHANGES IN THE DIAMOND TRADE

In many respects, the diamond and jewellery industry is not unlike any other trade industry but there are practices specific to the diamond trade. Some of these practices with relevance to AML/CFT considerations are detailed below.

Sightholders/tenders – *Sightholders*[28] are clients of De Beers who are authorised to buy bulk rough diamonds from the Diamond Trading Company (DTC) held by De Beers thus ensuring a steady supply of rough diamonds. Similar systems of rough diamond supply exist with other large mining diamond companies. The *tender* system is an alternative way to buy rough diamonds where bulk diamonds are offered for sale to diamond dealers through tenders. This system however is not limited to sightholders and large mining companies only; it allows 'smaller' rough diamond traders to sell their diamonds in a secure and controlled environment.[29]

Payment methods - Common to the diamond industry is a cash remittance system that is historically-based. Diamond sales at virtually all levels of the market function were made on cash purchases. Nonetheless, while acceptance of cash is still common, this practice has subsided in recent times and modern forms of remittance such as wired funds or credit systems are becoming more prevalent, even in cash based economies such as India and Namibia[30].

Trust – the diamond industry has always functioned on the basis of trust. Million dollar deals are sealed with a handshake. There is an accepted code of conduct and internal arbitration system. Rough or polished stones worth millions of dollars may be sent to another dealer for consignment without a written contract. For example, the owner of the stones will trust that a consignee will

[28] See Diamonds A to Z (nc).

[29] For example: Antwerp World Diamond Centre (nc).

[30] The limited use of cash in these jurisdictions is based on the reply to the collection plan submitted by India and Namibia.

transfer the correct payment upon selling or otherwise return the exact same stones. Consultations conducted with the WFDB revealed that a breach of this trust would ruin the diamond dealer's reputation[31] and consequently end his career.

Memo transactions - A practice that continues to be used in the diamond industry is the lending of a diamond or a mix of diamonds to others in the diamond industry so that they may have the opportunity to sell them – this is known as a "memo transaction." Under this arrangement, the conditions of the loan are specified, including for how long the diamond will be lent, the price of the diamond, and the terms of remittance to the owner if the diamond is sold. The vendor who has the diamond on memo may sell the diamond at a mark-up and then pay the owner in the time and amount specified by the memo. Sometimes the vendor that has the diamond on memo may lend it to another vendor on another memo. Some issues have arisen in the industry around the use of memos, including fraud. There have also been questions around who is responsible for reporting the sale of the diamond under ML reporting requirements (the owner or the seller). In addition, there have been cases in which the diamonds on memo have been sold, but the seller refuses to pay. This would be considered an outright conversion theft.

Related to the use of memos and ownership of diamonds is the variance in inventory practices at different levels of the industry and in different regions of the world. Generally speaking, while diamonds may be counted as individual units, they can also be accounted for by weight. For example, one carat of diamond could be a single one carat stone or 100 diamonds of 0.01 carat each (the per carat valuation is what will distinguish the two parcels in this case, as the one carat diamond may sell for USD 4 000/carat, whereas the 0.01 carat diamonds may only sell for USD 500/carat). While each stone has been weighed, the inventory, which has implications on the profit and hence on tax paid to the tax authority, may be registered differently, *i.e.,* some inventory practices may record diamonds by piece, others may do so by weight. This leaves room for manipulation and "playing" with tax reports, making it difficult for tax authorities to verify the level of inventory on the date of reporting, thus also allowing for manipulation of profit and income tax.

It is also common to negotiate a final price for a diamond. While there are industry suggested prices for a given quality of diamond they are in fact only guidelines, *i.e.,* a starting point from which the negotiation of the final price begins.

Special expertise - Training in gemmology requires a unique skill set, or, at the very least, industry experience. As a result those who enter the jewellery industry or trade are often those whose family is already in the industry, and through whom they can learn the business and garner the necessary experience to succeed. The independent jeweller must be a business person with savvy market-specific knowledge, keen gemmology skills (that need to be constantly upgraded), and, perhaps most importantly, industry contacts to acquire product to sell. Similarly, each level of the industry requires its own specific training, and this knowledge is only learnt through experience in the industry itself.[32]

---

[31] See Even-Zohar, C. (2004), *pp.* 35; and Siegel, D. (2009), *pp*. chapter 4.

[32] Rough diamond sorting and diamond grading of polished diamonds are regularly offered at specialized training institutes throughout the world. Well-known institutes include the Gemmological Institute of

This makes it very difficult for a person to enter the jewellery and diamond trade, as the experience required and practical market knowledge is not readily available[33]. For example, in order to become a diamond bourse member, it may be necessary to be in the business for several years and to be recommended by an existing bourse member[34]. These barriers to entry, including with regard to obtaining product from wholesalers, has made it possible for the diamond industry to protect itself from criminals infiltrating the trade. This is especially the case in countries where special 'license' needs to be obtained from the government in order to become a diamond dealer. In the past, one would receive a referral to a wholesaler from an established jeweller and then obtain an account with the wholesaler to purchase products. Once a few accounts had been set up and business arrangements with diamond/jewellery wholesalers made, these accounts could be leveraged to establish one's legitimacy as a jewellery business. However, without the initial referral from someone already in the business and the subsequently use of primary suppliers to obtain accounts with others, it was virtually impossible to become established.

Some families have been in the diamond business for several generations and have developed strong alliances and networks over time. The involvement of both religious and ethnic groups is very much a reflection of the industry's history, although, in recent times, there has been a shift in the geographic concentration of the diamond trade. This is more of a phenomenon of the finished diamond sector, particularly with respect to the wholesaler to the retailer end of the business.

So far, the overview of the diamond trade has discussed the various levels of the diamond market, presenting a simplified view of the supply chain from mine to consumer. It is important to understand that the processes of mining, the trading of rough diamonds, and even the processes of cutting and polishing diamonds may differ from country to country[35]. In addition, these processes have been subject to market forces and regulatory changes in the last 20 years that are creating new paths for bringing diamonds from mine to market.

While some of the market changes are having a dramatic effect on business practices the world over, these changes may be both positive for the relevant jurisdiction, but may also entail a shift in the level of risk posed by the diamonds industry. The following sections discuss changes in the diamond trade.

De Beers no longer holds a monopoly[36] - up until the 1980s, the rough diamond supply was controlled largely by De Beers through their African holdings. While there were a few other sources of diamonds, including from Russia, this control amounted to a market monopoly. With the emergence of a more open market for global rough diamond sales, a number of international

America in New York and Carlsbad (Calif.), the HRD Antwerp –Institute of Gemmology and the International Gemmological Institute in Antwerp, Hong Kong and Mumbai.

[33] See Even-Zohar, C. (2004), *pp.* 35 – "A closed industry guild with a high entry barriers".

[34] This is the one of the rules set up by the WFDB for all its members.

[35] Differences may lay in the type of mine (alluvial or kimberlitic, closed or open pit), in the manner in which the rough diamonds are distributed from the mine to the rough market, in the level of local beneficiation, in the level of regulation and control over the mining, rough or polished trade, etc.

[36] For a discussion on the change in the role of De Beers in the rough trade see Bain & Company (2011), *pp.* 11 "Expansion of rough-diamond sales channels".

diamond companies, such as Alrosa, BHP Billiton, Harry Winston, and Rio Tinto, increased their involvement, and Russia, Canada, and Australia have become major producers. In the past 20 - 30 years, many companies have chosen their own path for bringing rough diamonds to market instead of selling them to De Beers. It is expected that with the increasing diversity of supply, an equally diverse rough diamond trading market will follow. However, the more the market opens up for new actors, the greater the risk that money launderers will abuse the trade, potentially requiring greater oversight of the industry.

De Beers rough trade moves from London/Antwerp to Gaborone - Up to now, the rough diamond trade was mainly channelled through Europe where De Beers sorted and sold its rough diamonds from London. After an eight years transition period, from November 2013, all the sorting and selling of the global De Beers rough diamond production will have been relocated to Gaborone, Botswana, which is expected to become a major rough diamond "transit trading centre" and, in many respects, play the role hitherto played by Belgium and, to a lesser extent, Israel. Over a hundred rough diamond clients ("sightholders") of De Beers will now travel to Botswana to make their rough diamond purchases. The Botswana banking system may become recipient of some USD 6 billion of inward remittance from these sales alone. This is expected to draw new banking and trading actors to the diamond industry and the trading pattern may significantly change in the years ahead.

Beneficiation – Beneficiation covers the manufacturing of polished diamonds and the creation of diamond-set jewellery. In recent years, African mining countries have been focussing on local diamond beneficiation to sustain employment in the industry and to generate additional added values. As a result, traditional diamond producing countries are increasingly setting up domestic cutting and polishing centres to expand their involvement in the diamond supply chain[37]. The move of De Beers to Botswana means that a significant part of diamond beneficiation will move to southern Africa – mostly Botswana, South Africa, and Namibia. This is expected to have a spill over effect on neighbouring countries which are major diamond producers in their own right, such as Angola, Zimbabwe and the Democratic Republic of Congo (DRC) which may follow suit and develop their own beneficiation. This trend may have significance in terms of ML/TF which will be discussed further in the section referring to vulnerabilities of the rough trading stage.

New trading centres[38] - New diamond trading centres in **China, India, and the United Arab Emirates (Dubai)**, among others, have emerged alongside the traditional **trades centres** - The diversity in rough diamond dealers and increasing supply from multiple sources has afforded opportunity for new rough and finished diamond dealing centres to emerge and historical diamond centres are being challenged by these new diamond centres. The United Arab Emirates has become a 40 billion USD free trade zone trade market. India, and to a lesser extent China, became the major cutting and polishing centres with trade amounting to many billions of dollars. Smaller trade

[37] See for example De Beers (nc).

[38] For discussions on the new and traditional trade centres see Even-Zohar, C. (2007b), which provides an extensive survey of the different jurisdictions involved in the diamond trade. A short review of the trade centres of Antwerp (Belgium), Ramat-Gan (Israel) and Dubai (the United Arab Emirates) is provided in Siegel, D (2009), chapter 5.

centres like Panama, have also recently emerged with a view to serving South America. The emergence of these new centres is primarily a function of the aforementioned supply chain shift, and also reflects the changing tax and regulatory environments. In addition, increasing consumption of diamonds in some of these markets has drawn many diamond manufacturers (cutters / polishers) to these new centres. New trade centres should be aware of the ML/TF risks this shift might entail.

Industry regulation - *Kimberley process* - There have been some dramatic changes in the regulation of the industry in the past ten years, primarily through the implementation of the Kimberley Process Certification Scheme (KPCS) for rough diamonds. The Kimberley Process (KP) is a voluntary export/import control regime, supported by the United Nations, and focussed on stopping the illicit trade in rough diamonds to finance armed conflict (*i.e.,* the use of rough diamonds as an alternate currency used mainly to by weapons). It is not an international legally enforceable agreement, and its compliance flows from the national implementation legislation in participating countries. From an AML/CFT perspective what is important to note here is that the KPCS does not deal with ML or with TF activities and is limited to rough diamonds only. Thus polished diamonds are not covered by the KPCS as it is assumed that all polished diamonds come from KP Certificated rough diamonds.

The KP does not include all countries. Only 81 countries currently participate in the KP (including 28 countries of the EU).

AML/CFT legislation - In the last 10 – 15 years, diamonds and precious metals have been recognised as vehicles for laundering the proceeds of crime. To deal with this issue, Governments have implemented or amended their ML legislation to include diamonds. Some countries have been quick to implement AML/CFT regulatory controls on this commodity and industry.

Industry efforts - the various entities within the diamond industry on both national and international level have made efforts to counter ML and TF risks. This includes the issuance of AML guidance, participation in FATF consultative forums and industry seminars, establishing the Responsible Jewellers[39] Council, De Beers' publication of their Best Practice Principles (BPPs) which De Beers, their joint venture partners, contractors and Sightholders all subscribe to, and the industry's System of Warranties which seeks to complement the Kimberley Process Certification Scheme further down the value chain, including the trade in polished and the jewellery retail sector.

Use of the internet as a trade platform - On the wholesale and retail side of the diamond supply chain, the internet has been a driver for bringing dealers and sellers closer to consumers while squeezing out many intermediaries. In recent years there has been a flattening of the chain of participants that bring diamonds from the producer to the retailer. However, the greatest flattening has been observed in the polished diamond market, especially in the mid-market level involving diamond wholesalers. Diamond dealers who would traditionally sell their products through to diamond wholesalers are increasingly selling them through to the diamond retailer. Similarly, diamond wholesalers, who would traditionally sell diamonds to the retailer, are now offering them up direct to the consumer through the internet and by-passing the retailer. The practicality of

39 Responsible Jewellers Council (2009).

offering diamonds through the internet is enhanced by third-party diamond grading certification, as well as cost-effective and efficient courier services (such as FedEx and UPS).

The trade platforms on the internet web site are mainly *Business to Business* (B2B) but *Business to Customer* (B2C) websites also exist. Both ***rough*** and polished diamonds are offered for sale. Payment means vary from bank transfers and credit cards, as well as checks and money orders, to internet payment systems such as PayPal. Platforms like eBay also enable this direct trade in diamonds, which can amount to millions of USD for polished diamonds. These practices raise challenges for a diamond dealer selling his or her product (both rough and polished diamonds) on how to conduct *Know your customer/ Customer Due Diligence/Enhanced due diligence* procedures to either business or private customers. How are the ML/TF vulnerabilities of the trade mitigated when business is conducted through the internet? How is it possible to trade in rough stones via the internet? [40] How is a Kimberley certificate issued in this case and how can a buyer establish the value of a rough stone without physically verifying its value[41]?

Rough diamonds are offered regularly on the internet at discount prices. Several fraud cases reported by Belgium in their collection plan were conducted through the internet. The exchange of cash for fraudulent diamonds took place in a remote unpopulated place. Exchanges are often arranged in Africa or close to locations of the diamond trade in Europe, and the means of payment and the inspection of the goods take place under quite tight timelines and in remote places. Such deals may be accompanied by dubious certificates of origin, inaccurate evaluations or lack of evaluation by an expert and sometimes without proper documentation.

Recycled market - Recycling of diamonds that have been previous used in jewellery encompasses a huge secondary market estimated to be in the billions of dollars globally. This is a rather unique feature of this industry as the commodities do not need to undergo any preparation for return to the market; the diamonds may simply be inserted into new jewellery or sold as an investment diamond. The WFDB commented that it is estimated that the world probably has about 0.75 – 1 trillion USD of polished diamonds at current prices (or about 1 – 1.5 billion carats) in consumer hands[42]. About 40-50% of these would be held in America. Recycled diamonds are generally being recut to meet today's consumer preferences. This recutting is mostly done in the United States (for expensive goods), or India.

Investments in diamonds – One jurisdiction highlighted this activity as a growing phenomenon. Websites offering diamonds for sale as an investment demonstrate how the dramatic rise in the price of diamonds over the last decade has resulted in them becoming a possible investment tool.

---

[40] The fact that buying a rough diamond through the internet is problematic in terms of establishing the price was raised in a consultation conducted with the WFDB. In additional consultation with diamond experts it was stated that whilst it is possible to buy rough on the internet no diamond professional would purchase rough diamonds without seeing them first unless they were buying from an LSM (*i.e.,* De Beers, Rio Tinto, etc.) and often then a viewing will take place. If a seller over the internet is not known and offers rough stones that should be an immediate red flag.

[41] In 2010 and 2011, the KP discussed at length the problems associated with the internet-trading of rough diamonds. It became clear that most of this trade was B2C instead of B2B.

[42] Estimated by "Tacy Ltd".

While it is not possible to determine the amount of investment in the industry, the larger the investments, the easier it would be to commingle funds from non-trade sources.

Synthetic diamonds - Another important change to the diamond market has been the emergence of synthetic and treated diamonds on the retail diamond market. While these man-made cousins of natural diamonds were not included in the typology review, it is important to provide a brief overview of them here. Synthetic diamonds are made of the same composition as natural diamonds (aside from some slight atomic differentiations); the fundamental difference is that synthetic diamonds are made in a factory. The quality of the synthetic diamonds and number of methods to create them has improved tremendously over the past decade and they are being sold commercially within the diamond industry. In addition, diamonds that were once considered unsuitable for commercial jewellery use are now being treated with different processes to enhance their colour or clarity. While the project has not examined synthetic or treated diamonds in respect of laundering proceeds of crime, the use of these types of diamonds in cases of fraud has been recorded[43]. Moreover, the use of synthetics substituted for real diamonds in relation to commodity-based ML should not be underestimated. What further muddles this issue is that there is no common international nomenclature for synthetic or treated diamonds. Some legislation may refer to diamonds or natural diamonds without making distinctions between, or allocations for, synthetic or treated diamonds. Since the quality of synthetic diamonds has improved, it is important to keep in mind that the vulnerabilities and typologies identified for the trade in natural diamonds may also be relevant for synthetic ones. As the trade in synthetic diamonds expands the risks posed by the trade in this type of diamonds will grow. It was noted in the private sector consultations that as the number of diamonds available to be mined decreases, synthetic diamonds may become more of an issue. Also of importance is the fact that in most if not all cases synthetic diamonds are not part of AML/CFT legislation, although the vulnerabilities may be similar.

OVERVIEW OF DIAMONDS AND MONEY LAUNDERING AND TERRORIST FINANCING

That this report has highlighted the different and unique characteristics of diamonds and the diamond trade which make the industry vulnerable to ML and TF activities should not be taken to mean that the industry is more vulnerable relative to others. Nonetheless, it is important to keep in mind that the complexity of the international diamond trade means that the ML and TF vulnerabilities and risks may differ from one segment of the "pipeline" to another and from one jurisdiction to another.

Beyond more conventional cases of ML, including the laundering of the proceeds of crime and the generation of criminal profits, some research[44] has shed light on the use of diamonds and diamond jewellery as an alternate currency by criminals. This is particularly notable in the case of diamonds used by criminal enterprises engaged in drug trafficking, (*i.e.,* the trade of diamonds for drugs).

[43] See for example Flanders News (2012) where it was said that "The quality of synthetic or man-made diamonds is so good, that even experienced diamond dealers can't tell real from fake ones". See also JCK (2012).

[44] Nelson, D., Collins, L. & Gant, F. (2002).

Diamonds are also used by such criminals for wealth movement, storage and preservation, and use as a status symbol.

It is useful to make a distinction between ML through the diamonds trade and laundering diamond proceeds of crime. The first type of activity is where a criminal will launder cash or other payment means acquired through predicate offences he commits[45] by placing and layering through the diamonds trade. This can be done by conducting transactions with the proceeds of crime as if they were trade in diamonds where in fact the diamonds trade will only be used to transfer funds from one account to another, whether locally or internationally, or by purchasing diamonds with cash proceeds of crime and then selling the diamonds to obtain cash at a later date or a different location. The second type of activity is where illicit diamonds (e.g. stolen/robbed diamonds, or diamonds received as a form of payment for drugs) will be laundered by selling or trading the diamonds, by cutting/re-cutting and polishing the illicit diamonds etc.' so as to conceal their illicit source. In both cases the criminal has laundered proceeds of crime, but only in the former case we can formally speak about ML as such, i.e. money which is laundered through the trade. The diamond industry is a perfect example where both can occur.

This distinction may be lost among law enforcement practitioners, intelligence officers and industry representatives, who almost exclusively refer to ML as encompassing all processes related to the proceeds of crimes involving diamonds. However, with respect to the development of typologies, this distinction is very important, especially as it relates to the use of diamonds as alternate currencies and in remittance systems used by criminals. For example, Pablo Escobar laundering drug profits through jewellery stores in a massive ML scheme[46]. And in 2003, USD 150 million worth of diamonds were stolen from a central diamond vault in a single theft event[47]. In this case, selling the diamonds is profiting from the proceeds of crime. Both cases utilised the diamond market.

TF can involve the use of unlawfully and lawfully provided funds to finance terrorism activities. Diamonds could therefore be used to finance terrorism in a scenario where a donor or financier purchases diamonds legitimately, using lawfully derived funds, and then transfers the diamonds to a terrorist or terrorist organisation who use the diamonds in exchange for equipment or cash intending to finance terrorist activities.

Buying and selling diamonds within rough and polished diamond markets is critical to understanding the vulnerabilities of the criminal use of diamonds, it is important to discuss the diamond and jewellery cycles. Diamonds are often reintroduced to the diamond market to be resold. The sale and resale of diamonds within the national and international diamond industry is a function of the diamond and jewellery cycle, which in turn provides an opportunity for laundering proceeds of crime. Illicit funds that are generated can be hidden, moved and entered into financial institutions or traded for other tangible assets within the diamond and jewellery cycle. The

45 These may be predicate offences not connected to the diamond trade, i.e., drug trafficking, fraud, weapons trade, etc.'.

46 Robinson, J. (2003).

47 See The New York Times (2013).

diamond industry may be a stepping stone for criminals who utilize these commodities to enter illicit funds into the banking system, whether in their own or in an offshore jurisdiction.

This cycle is rather unique for commodities (although it also applies to precious metals and gemstones, to some extent), especially as the diamond remains in the same form from the time that it first enters the market after being cut and polished. The simplicity and ease with which diamonds can be purchased and sold, and the special characteristics of these precious stones, provides tremendous opportunity to exploit the commodity and the industry with regard to the laundering of the proceeds of crime.

In summary, the diamond supply chain at all of its stages, from production to consumption, can be the gateway to profitability, for laundering proceeds of crime, for ML or TF and for moving proceeds of crime into the financial system.

THE DIAMOND TRADE IN NUMBERS

The purpose of this section of the report is to give the reader unfamiliar with the diamond trade information on all its facets a rough idea as to the volume of the different parts of the trade (rough, polished and jewellery manufacturing levels) and to draw some inferences from available trade data.

ROUGH DIAMOND TRADE

The KP publishes annual statistics on the rough diamond trade, which include the annual volume in carat and the annual value in USD. The information is published on the KP website with respect to each of the member countries and includes data on: rough diamond production, import and export; the average price per carat[48] for both import and export; and the number of certificates issued within each jurisdiction[49]. These statistics provide a very general picture of the leading countries at each level of the rough "diamond pipeline" and the overall volume and value of the global rough diamond trade.

What is important to remember is that The KP data does not capture the entire global production. These figures exclude trade within the EU (*i.e.,* between the United Kingdom and Belgium for which no certificates are required) or internal trades on local markets. There are some suspended or sanctioned countries whose production is not recorded. In quite a few instances the production values are not correctly reported. Smuggling is still taking place, and those diamonds do somehow end up in the diamond pipeline. The Kimberley system figures should be viewed as indicative only.

The KPCS was not designed to curb ML/TF activity; it was designed to put an end to the trade in conflict diamonds. While it is not possible to draw firm conclusions based on these statistics some

48 The average price per carat is also published for each member state on the KP web site.

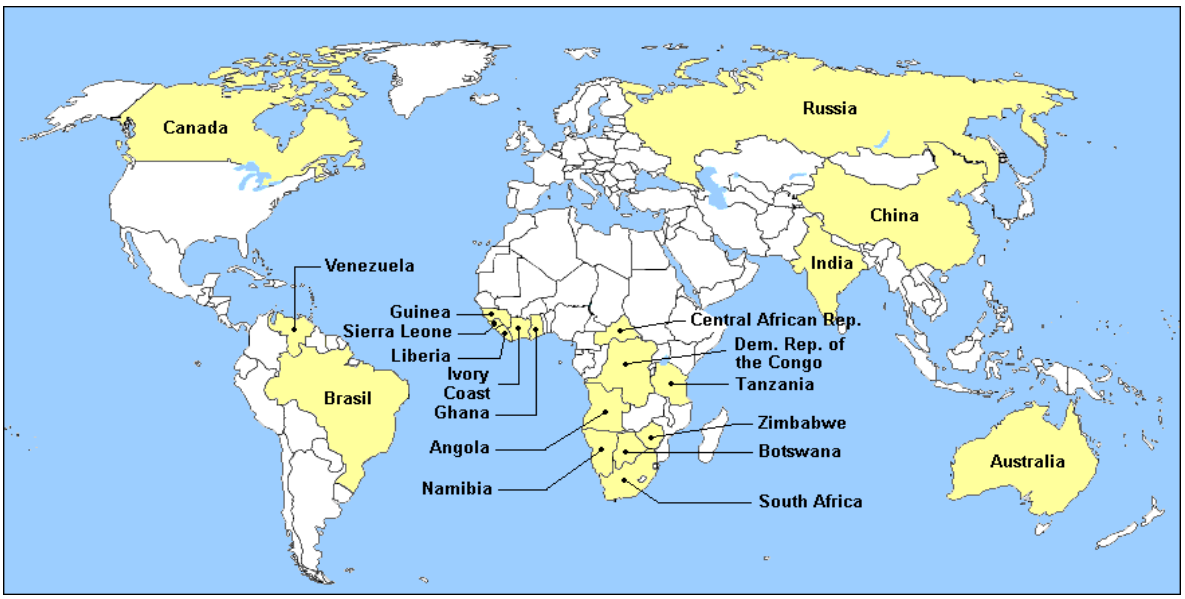
49 KPCS rough diamond public statistics area, https://kimberleyprocessstatistics.org/public_statistics. Additional statistics as to the country to country rough diamond trade are not published, but may provide a more deeper understanding of the rough diamond trade and may point to additional ML/TF issues and concerns.

indication of ML/TF activity related to rough diamond trade are provided by this information which should be addressed by participants of the KP.

DIAMOND PRODUCTION COUNTRIES

Mining activity takes place across different geographic areas around the world. The figures below provide some information on mining countries at the first level of the "diamond pipeline", i.e. supplying rough diamonds which will eventually be manufactured into jewellery. Rough diamond production is spread across different geographical areas around the world but almost 80% of the total rough diamond production is concentrated in 5 countries.

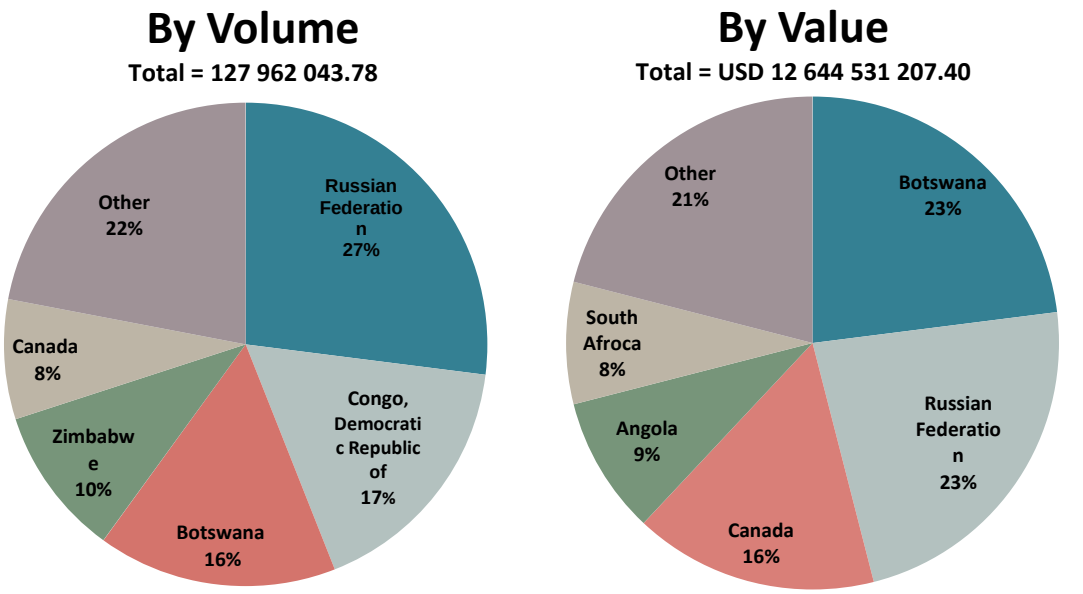
Figure 3: **Countries of rough diamond production**



Source: www.info-diamond.com[50]
Note: Lesotho, Guyana, Togo, Cameroon, Congo (Brazzaville) and Indonesia are also producers of rough diamonds. At the moment there is a total UN embargo on the import of diamonds from Côte d'Ivoire, and a KPCS "embargo" on diamonds from Venezuela and Central African Republic.

50 www.info-diamond.com/rough/map.html#prettyPhoto/0/.

Figure 4: **Countries of rough diamond production – 2012 Production**



Source: Kimberly Process Certification Scheme

According to the KP statistics for 2012, the total volume of production of rough diamonds was close to 128 million[51] carats, amounting to a total value was over USD 12.6 billion[52]. However, imports and exports of rough diamonds have reached USD 50.92 billion and USD 50.27 billion respectively. The volume of export and imports are much higher than the volume of production since rough diamonds go through many several "industry actors" in several trade and polishing centres before they are cut and polished. Mining countries may also stockpile production. The production, export and import figures of the major diamond producing countries (in terms of volume and value) are included in table below:

51 127 962 043.78 carats.

52 USD 12 644 531 207.40.

Table 1: **Production, Exports and Import of rough diamonds in major Producing countries – 2012**

	Production		Import		Export	
Country name	Volume (Carats, Carat (Millions)	Value (Billions of USD)	Volume (Carats, Carat (Millions)	Value (Billions of USD)	Volume (Carats, Carat (Millions)	Value (Billions of USD)
Botswana	20.55	2.98	7.49	2.14	23.35	3.99
Russian Federation	34.93	2.87	0.14	0.15	29.81	3.90
Canada	10.45	2.01	0.76	0.16	11.12	2.16
Angola	8.33	1.11	0	0	9.20	1.15
South Africa	7.08	1.03	11.47	1.08	8.01	1.36
Namibia	1.60	0.90	0.13	0.16	1.68	0.98
Zimbabwe	12.06	0.64	0	0	14.96	0.74
DRC	21.52	0.18	0	0	19.56	0.26

Source: KP statistics[53]

As can be seen in the table above, Botswana is currently the largest producing country in terms of value, (USD) and the Russian federation is the biggest producer in terms of volume (carat). Most of the production is exported to trading centres and then onwards to polishing and cutting centres. Botswana and South Africa are also significant importers of rough diamonds of very high volumes. The Russian Federation's exports amount to almost a billion dollars more than the value of its production. This raises a question as to the source of the diamonds exported. Since the volume in terms of carat is almost the same, this means that the average price of diamonds exported is much higher than those which were mined.

There are additional countries producing from just a few million dollars to several hundred millions dollars in diamonds (Australia, Brazil, Central African Republic, Congo, Ghana, Guinea, Guyana, India, Lesotho, Liberia, Sierra Leone and Tanzania). The Democratic Republic of Congo is the second largest producer in terms of volume (carat). Diamond mines also exist is Venezuela, but according to the KP statistics, the country has voluntarily suspended exports and imports of rough diamonds in 2008 and until further notice. However, reports exist that suggest that mining in Venezuela continues and the rough diamonds are smuggled out of the country[54].

53 Data from KP web site for the year 2012 (statistics are provided on the web site from year 2004) - Kimberly Process (2012).

54 See Time (2012).

DIAMOND TRADE CENTRES

Table 2: **Production, Exports and Import of rough diamonds in major trade centres – 2012**

	Production		Import		Export	
Country name	Volume (Carats, Carat (Millions)	Value (Billions of USD)	Volume (Carats, Carat (Millions)	Value (Billions of USD)	Volume (Carats, Carat (Millions)	Value (Billions of USD)
European community	0	0	124.80	16.79	126.80	17.81
Israel	0	0	13.27	4.66	13.79	3.61
Switzerland	0	0	8.68	1.99	8.88	2.29
United Arab Emirates	0	0	59.74	4.56	60.44	6.82
United States	0	0	3.49	0.48	1.45	0.40

Source: KP statistics[55]

In 2012 the main trade centres for rough diamond were Belgium, Israel, Switzerland and the United Arab Emirates. Belgium is the largest trade centre with a USD 34.6 billion rough diamond industry followed by the United Arab Emirates (USD 11.38 billion) and Israel (USD 8.27 billion). The role of rough diamonds trade centres is to provide the link between mining countries and polishing centres and provide the supply needed by cutters and polishers who produce polished diamonds. What stands out from the figures in the table above is the role played by the United Arab Emirates, and its significance in terms of the world-wide trade. The volumes (carat) imported to and exported from the United Arab Emirates are almost the same and stand at around 60 million carats. However the value of the exported rough diamond and the average price per carat is almost 50% higher than the value of imported rough diamonds. For 2011, the average price per carat for export in the United Arab Emirates is 74% higher than the average price per carat on import. These are the same rough stones going in and out only they are sold at a much higher price, an increase that perhaps includes more than the entire production chain mark-up. A small part of the difference may be explained by 'sorting' which may produce 10–15 % mark up. Since the United Arab Emirates is not a polishing centre the added value for the diamonds going in and out of the country is unclear and would merit further investigation[56].

55 Kimberly Process (2012)

56 Earlier research has been done on the situation in Dubai. See Even-Zohar, C. (2004), chapter six, for a discussion on transfer pricing with reference to Dubai and FTZs. In particular Even-Zohar states that "*In essence, diamond multinationals will channel their rough diamond purchases … through Dubai. Often, the parcels are not even opened and, after re-invoicing, are shipped to the final destination, often Belgium, India or far-east cutting centres. The invoice will inevitably provide a higher figure … As a result, the local company produces a profit – which is a purely paper profit, because it generally remain a transaction between affiliated companies*" (*Ibid, pp.* 101).

CUTTING & POLISHING CENTRES

Table 3: **Production, Exports and Import in major cutting & polishing countries – 2012**

	Production		Import		Export	
Country name	Carat (Millions)	Volume (Billions of USD)	Carat (Millions)	Volume (Billions of USD)	Carat (Millions)	Volume (Billions of USD)
India	0	0	151.87	14.88	34.44	1.80
China	0	0	21.14	2.73	15.00	1.66
Thailand	0	0	0.87	0.40	0.40	0.15

Source: KP statistics[57]

Most of the cutting and polishing is done today in India[58]. China has also become in recent years a major cutting and polishing centre. The traditional polishing centres were Belgium, Israel and the US (see KP data in the tables above), much of the polishing and cutting has recently moved to the Far East. Additionally, African countries such as Botswana and South Africa have invested in developing the local beneficiation industry and are becoming to some extent cutting and polishing centres. Smaller manufacturing operations are located in Angola, Armenia, Brazil, Democratic Republic of Congo, Mauritius, Namibia, Russia, Sri Lanka and Thailand.

Changes in export/import to production ratio – in the last 5 years the ratio between the volumes in USD of rough diamonds export to rough diamond production[59] has risen by 33%. During the same period of time the rate of export to production in terms of volume (carat) has gone up by 27.3%. Compared to 2008, the same stones are exported and then re-exported more times than five years ago and at a higher price per carat than the price of carat at the production level. The diamonds are going through additional "hands". In terms of ML/TF this may be an indication that there are more "circular transactions" in diamonds (and correspondently in financial transactions conducted through financial institutions supporting the trade, mainly banks) which might be a result from ML or TF activity. It is not within the scope of this project to analyse the reasons for this additional circular trade, but this should be a reason for concern for importing and exporting countries.

57 Kimberly Process (2012)

58 According to open source information India accounts today for more than 90% of cutting and polishing of rough diamonds (by volume), e.g., Bain & Company (2011), *pp*. 45, "*Before the recent recession, Indian craftspeople cut 14 out of 15 diamonds worldwide*" and Even-Zohar, C. (2013).

59 The export and import are almost identical in terms of both value in USD and volume in carat since the same diamonds which are exported are also imported in another KP member state.

Table 4: **Rough diamonds export/import to production ration for 2008 - 2012**

	2008	2009	2010	2011	2012
Export/import ratio (value, USD)	3.04	3.03	3.29	3.63	4.02
Export/import ratio (volume, carat)	2.49	2.64	3.22	3.14	3.17

Based on KP statistics

Illegal trade – the KP statistics account only for the legitimate trade between KP member states. While team members have indicated that illegal trade is taking place, there is no source of data to evaluate the extent of such trade making it hard to establish the overall global volumes of rough diamond trading. Cases provided by team members or from open source show that **smuggling accounts for a large portion of the illegal activity**, indicating that the illegal trade in diamonds is very significant. The following countries have either provided cases involving smuggling and/or indicated that smuggling of diamonds occur within their jurisdiction: Belgium, Canada, Israel, Netherland, Russia, South Africa, Sierra Leone, United Kingdom, and United States of America.

The illegal diamond trade can be divided as follows:

1. **Illegal mining** which takes place in mining countries. The illicit diamonds will then be either inserted to the trade of a local mine or smuggled to a neighbouring country with a mining industry and then commingled with the produce of a legal mine.
2. **Stolen diamonds** which are inserted to the legal trade as a laundering method (for example, it is estimated by DeBeers that USD 100 million is stolen from them annually).

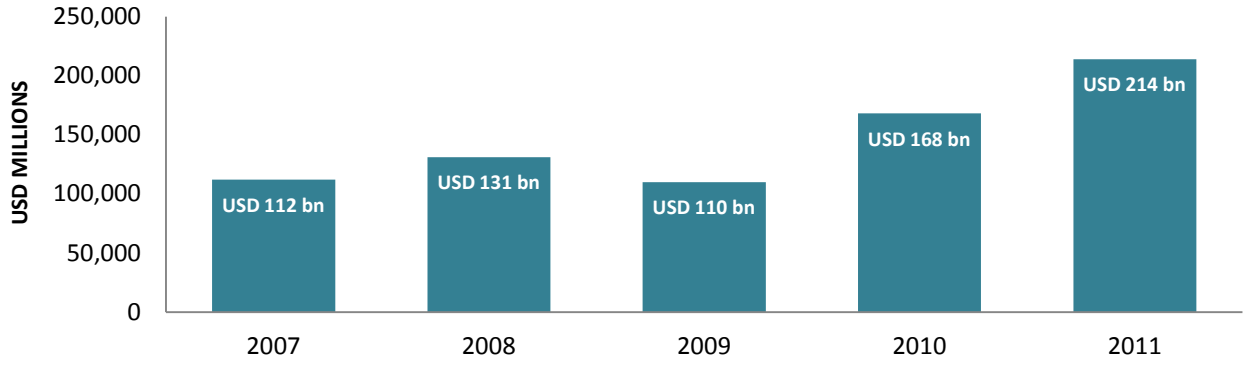
From an AML/CFT perspective the illegal diamond trade may also be used for ML/TF purposes.

POLISHED DIAMOND TRADE

In order to further understand the volume of the diamond trade and the leading countries involved in it, one must also look at the trade in polished diamonds. The polished diamond trade refers to trade in *loose* diamonds after they have been transformed from rough diamonds through cutting and polishing. As the chart below shows, the volume of trade in polished stones is much larger than the trade in rough stones amounting to approximately USD 214 Billion[60].

60 These figures include also movement of diamonds, such as memo transactions where in many instances the diamonds do not change ownership and are returned to the diamond dealer or when the diamonds are sent for appraisal.

Figure 5: **World Polished Diamonds Trade**



Source: www.diamondshades.com

The charts show a significant development in the traded value of diamonds during 2007-2011. There is one exception, the financial crisis in 2008-2009 which resulted in a shortage of rough stones as the volume in carat weight declined sharply. The general trend is a development of the extracted value by strides and jumps. There appears to be a significantly disproportionate ratio between the turnover of polished diamonds and the traded turnover of rough diamonds. This may be attributed to higher prices of polished diamonds, since the real added value in the phase of the transfer of diamonds from rough and uncut stones to polished gems is relatively small. Although not indicated, this may also be attributed to an inclusion of return shipments of polished diamonds, where polished diamonds are sent for inspection by a customer while some of the diamonds are returned to the diamond dealer.

The US is today the largest consumer market for diamond jewellery. There is also a significant polished diamond trade in China; Hong-Kong, China; India; Japan and the Persian Gulf. Trade centres such as Belgium, Israel and the United Arab Emirates also see high volumes of trade in polished diamonds with turnover reaching USD 28.67 billion in Belgium, USD 12.88 billion in Israel and USD 29.73 billion in the United Arab Emirates (for the year 2011). Finally, cutting and polishing centres also account for a large portion of the trade, with USD 47.25 billion in India and USD 4.7 billion in China[61].

JEWELLERY MANUFACTURING

At the last stage, jewellery manufacturing hold an additional large portion of the trade in volumes amounting to tens of billions of USD anually. The US is considered to be the largest consumer market for diamond jewellery with volumes amounting to billions of USD. India is one of the major manufacturing countries of diamond jewellery with volumes reaching a few tens of billions of USD. Jewellery manufacturing is also conducted in countries like China, Thailand and in western Europe. Some of the manufacturing is made by large international chain store companies where manufacturing can reach several billion USD.

61 For statistics see Diamond Shades (n.c.).

CHAPTER 3.
REGULATION AND LEGISLATION RELATING TO DIAMOND DEALERS AND CROSS-BORDER TRANSPORTATION OF DIAMONDS AND CURRENCY RELATED TO THE TRADE IN DIAMONDS

FATF STANDARDS

FATF STANDARDS RELATED TO DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

In 2008, FATF adopted a Risk-Based Approach Guidance document for dealers in precious metals and stones[62]. The guidance supported the development of a common understanding of what a risk-based approach involves, to outline the high-level principles involved in applying a risk-based approach and to indicate good practice in the design and implementation of an effective risk-based approach. In the guidance, the term 'dealer' encompasses a wide range of persons engaged in these businesses:

- Those who produce precious metals or precious stones at mining operations.
- Intermediate buyers and brokers.
- Precious stone cutters and polishers and precious metal refiners.
- Jewellery manufacturers who use precious metals and precious stones.
- Retail sellers to the public, and buyers and sellers in the secondary and scrap markets.

In addition to financial institutions, the FATF Recommendations[63] also cover a number of Designated Non-Financial Businesses and Professions (DNFBPs). DNFBPs cover dealers in precious stones, including diamond dealers. No further explanation of definition on dealers in precious stones is provided by FATF.

The following FATF Recommendations are applicable to diamond dealers.

- **Recommendation 22** mandates that customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17 apply to dealers in precious stones when they engage in any *cash transaction* with a *customer* equal to or above the applicable designated threshold (USD/EUR 15 000).

62 FATF (2008a).

63 FATF (2012).

- **Recommendation 23** indicates that the requirements set out in FATF Recommendations 18 to 21, regarding measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, internal AML/CFT controls and the reporting of suspicious transactions, apply to dealers in precious stones when they engage in any *cash transaction* with a *customer* equal to or above the applicable designated threshold (USD/EUR 15 000).
- **Recommendation 28** requires that dealers in precious stones be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which should be performed on a risk-sensitive basis by a supervisor or by an appropriate self-regulatory body.

FATF STANDARDS RELATED TO CASH COURIERS

With regard to **Recommendation 32** on Cash couriers and its interpretative note, precious stones ***are not included***, despite their high liquidity and use in certain situations as a means of exchange or storing and transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of precious stones, it should consider notifying, as appropriate, the customs service or other competent authorities of the countries from which these items originated and/or to which they are destined. The country should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward taking appropriate action. Countries are not required to have measures in place to detect the physical cross-border transportation of diamonds through a declaration/disclosure system.

NATIONAL AML/CFT REGULATION/LEGISLATION IN DIAMOND TRADING COUNTRIES

As part of the project, countries were asked if they have national AML/CFT regulation applicable to diamond dealers in place, and, if so, what the reporting and record -keeping duties contained and how registration and supervision of the sector was carried out. Information was also gathered about the regulation of the cross-border transportation of diamonds, and currency related to the trade in diamonds.

It is important to note that the definition of a diamond dealer differs from country to country. For example in the US a retailer can be under certain conditions seen as a diamond dealer. However, in most countries a diamond dealer is only dealing in rough or polished loose diamonds. Further information on difference in regulation and legislation can be found in **Chapter 5**.

NATIONAL AML/CFT REGULATION ON DIAMOND DEALERS, REPORTING DUTIES AND RECORD KEEPING DUTIES

With regard to current international AML/CFT legislation, several countries do not have AML/CFT regulations pertaining to diamond dealers. As a result, businesses that buy and sell diamonds are

not obliged to implement due diligence procedures or report[64] transactions to an FIU (STRs[65], and / or CTRs)[66] or undertake AML/CFT risk assessments.

In some cases, countries without national AML/CFT regulations pertaining to diamond dealers have other legislation for the regulation of the sector. For example, legislation making it illegal to trade in rough diamonds - or are in the process of enacting an AML/CFT regime for diamond dealers.

- **South Africa** does not have industry-specific AML/CFT regulations directed at diamond traders. Diamonds are only covered under the Diamond Act, which deals with the regulation of the diamond industry as a whole.
- **Israel** indicated that, in 2012, parliament approved an amendment to the AML/CFT law to include dealers in precious stones. In the near future, diamond dealers will be regulated and supervised for AML/CFT by a supervisor and they will become subject to Administrative Sanctions for non-compliance.
- In **Mexico**, an AML/CFT law applicable to the trading in diamonds, among other non-financial businesses, entered into force on July 17, 2013. Through this law, both individuals and legal entities trading in diamonds and other precious stones and metals are subject to AML/CFT compliance measures, such as CDD and filing of transaction reports.
- The **Australian government** has also proposed amendments to its AML/CFT Act to include diamond dealers.
- Although **Switzerland** has no specific AML/CFT regulations specifically applicable to diamond dealers, it does have a reporting obligation in place for instances in which dealers are considered financial intermediaries.

In most of countries that contributed to the report, however, diamond dealers are subject to a national AML/CFT regime. Depending on the country, this includes implementing an AML/CFT programme designed to prevent the dealer from being used to facilitate ML or TF, and usually entails designating a compliance officer, providing on-going education and training, customer identification, and a customer acceptance policy, as well as record-keeping requirements, Know Your Customer (KYC) procedures, reporting requirements and a risk-based approach. De Beers provides training and awareness to law enforcement, *e.g.,* Interpol and customs.

The customer identification and identity verification range from remote identification, the identification of the ultimate beneficiaries, to the identification of the clients and sometimes identification of the suppliers. In Belgium, the identification and identity verification of clients is a legal obligation when establishing a business relation, when entering an occasional relationship for

---

65 While The FATF uses the term Suspicious Transactions Reports there are other types of reports such as SAR (Suspicious Activity Report), UTR (Unusual Transaction Report) and UAR (Unusual Activity Report) which are the legal requirement in different team member jurisdictions.

66 More details on the countries and numbers can be found in the chapter on statistics.

a transaction exceeding EUR 10 000, or generally when there is a risk or suspicion of ML or TF. Furthermore, it is required to identify such diamond suppliers for which purchasing transactions lead to payments that are wholly or partly, directly or indirectly, carried out by other means than by transfer to bank accounts held with credit institutions.

When AML/CFT legislation is applicable to diamond dealers, they are obliged to submit Suspicious Transaction Reports (STRs) / Suspicious Activity Reports (SARs) to the FIU and establish different procedures and policies for AML/CFT prevention. The statistics show that half of the countries that participated in the project received some or several STRs/SARs from diamond dealers. The reporting duties depend on the country but several of them have set a threshold (from USD 6 500 to USD 65 500) with regard to cash transactions in the diamond trade or business. In The Netherlands, consistent with the limitations set out in the European Union, diamond dealers are obligated to report cash transactions above a threshold of EUR 15 000 and on suspicion of ML.

In most countries, diamond dealers have the obligation to maintain verifiable records of all activities for a period of five years. In Argentina, diamond dealers keep documents for ten years in such a way that enables the reconstruction of transactions and allows such documents to be used as evidence in any ML and TF investigation. In general, diamond dealers need to keep, protect, safeguard and prevent the destruction or concealment of information and documentation supporting trade practices (invoices, KP certificates), as well as the information used to identify their clients. Depending on the country, diamond dealers also have to submit an annual declaration about the stocks and activities, put in place a written AML/CFT policy or keep a copy of every suspicious transaction report that they forward to the FIU.

The overall self-assessment of those countries that provided information was that the level of AML/CTF compliance of the diamond sector as medium.[67] In Canada, deficiencies related to entities' compliance programmes have been primarily identified (e.g. policies and procedures, training, risk-based assessment, etc.). Canada's AML/CTF regime for diamond dealers is more comprehensive on other elements, such as appointment of a compliance officer, record-keeping and client identification. In Belgium, an extra focus on compliance was put forward by the sector representative with an AML/CFT and Compliance Helpdesk assisting diamond dealers with their regulatory and compliance obligations and the introduction of Compliance as the 5th "c" of diamonds (next to Cut, Clarity, Carat and Colour).

LICENCE REGIME AND SUPERVISION OF THE SECTOR

Only in a few countries are licences and registration required for business activity in the diamond trade. This can be with the FIU or another licensing authority. In Belgium, all diamond dealers need to be registered with the Federal Public Service Economy for business activity in the diamond trade and a licence is required for the import and export of diamonds coming from or going to non-EU countries. By contrast, in the United States, diamond dealers are not required to register or be licensed for AML/CFT purposes. The strictest rules apply in South Africa and Namibia, where it is illegal for any unlicensed person to be in possession of or trade in uncut diamonds.

67 There were some outliners. One country assessed their level of compliance as low and one medium to high.

Compliance with the regulations imposed on diamond dealers is checked by an independent authority or the FIU (depending on the country). These regulators/controlling bodies have the authority to issue administrative fines and, in some cases, criminal penalties (monetary and imprisonment) to diamond dealers who are non-compliant with their AML/CFT obligations or to revoke the license of a diamond dealer. In the USA, some warning letters regarding the lack of a required AML/CFT programme were issued. Nonetheless, in most countries no fines have been imposed on diamond dealers, and no AML/CFT civil enforcement actions have taken place over the last two years. In Namibia, the diamond sector has not been assessed for AML/CFT compliance as of yet, thus no enforcement has taken place. Consequently, no sanctions were imposed in the last two years. This is a clear indication that the level of AML/CFT enforcement of the sector in most team members' jurisdictions is low, perhaps apart from the mining sector of some kimberlitic mines jurisdiction where level of control over the risk of theft is considered to be high. During the FATF/GIABA expert workshop held in Dakar, some participants noted that there is a need for strong enforcement on the sector and that the low level of enforcement, particularly in some African mining countries, poses a problem in terms of AML/CFT supervision.

NATIONAL AML/CFT REGULATION ON CROSS-BORDER TRANSPORTATION OF DIAMONDS AND CURRENCY RELATED TO THE TRADE IN DIAMONDS

There are several ways of transporting diamonds, via parcel or mail, courier service or by personal transport. Lower value shipments may enter by way of FedEx/UPS, whereas Brinks, G4S or other secure or armoured car services (Malca Amit) are in most cases used for the highest value shipments and bulk rough diamonds. In most cases, diamonds enter a country as paid parcels and taxes are incurred, less frequently the diamonds are entered on Memo and also under ATA Carnet[68] (tax-free – for display/show purposes). In Israel, the courier service will also deal with the documentation and transmit the information of the shipment to the customs. According to the Israeli contribution, the courier service company does not verify if the content of the shipment corresponds with the diamond dealer declaration. All Kimberley Process (KP) members have implemented domestic legislation that requires rough diamonds be exported in tamper-resistant containers.

Within the Kimberley Process Certification Scheme (KPCS), rough diamonds can only be traded between KP participants, and all imports and exports of rough diamonds must be accompanied by a KP Certificate.[69] In Russia, diamonds are transported in boxes that contain a mixture of diamonds of given types, collected in compliance with the adopted structure. The certified (validated) copy of the KP certificate and the shipping documents are enclosed with the parcel within the tamper-resistant plastic bag, the KP certificate is visible through a transparent window in the bag. The number of the KP certificate is indicated on the bag and in the shipping documents.

68 ATA Carnet cannot be used for sending rough diamonds.

69 Although it is illegal for KP participant countries to ship rough diamonds to non-KP participant, KPCS is not an international binding treaty and therefore it is not illegal for non-KP participating countries to trade in rough between themselves.

There are some major differences between countries with regard to customs control, especially on polished stones. For example, in Israel all rough diamonds imported to or exported from Israel are examined and assessed in order to collect due taxes and receive proper documentation by a special diamonds customs station located within the diamond exchange operated by three diamond and gem specialists. Similarly, the value of polished diamonds is randomly checked. In Belgium, every shipment that goes in or out is checked, verified and cleared by sworn experts, while each step is carefully monitored by the government (triple control). In Russia, customs clearance of diamonds is performed exclusively at the special customs station, where they undergo clearance and government inspection. In South Africa, where a levy is payable whenever a registered person imports or exports diamonds into or out of the country, all diamonds are transported in parcels sealed by the diamond regulator after evaluation so that the exporter cannot change the content of the parcel after evaluation.[70]

In most of the other countries there are no specific import /export customs controls on diamonds. The imported and exported diamonds fall under the same provisions as any other goods imported or exported and only have a *Harmonised Commodity Description and Coding System* code to indicate the category of diamonds (*i.e.,* rough sorted or unsorted, polished, etc.). For example, in the UK, Customs require a declaration for all imported or exported goods (including diamonds) for customs duty and or VAT purposes and there are no further controls by Border Force (Customs) on polished diamonds. In Canada and the USA, diamonds are classified using the Harmonized Tariff classification system. In Canada, imports/exports do not necessarily specify the four Cs of diamond valuation or the number of pieces, and therefore valuation exploitation can occur. This is more often the case for diamond parcels rather than single diamonds. In Namibia, diamonds are classified for shipment purposes as polished or rough diamonds and the carats are taken into consideration.

Even though all countries have either specific or general Custom regulations in place regarding the import and export of diamonds, all team members indicated that no specific AML/CFT requirements are in place to declare diamonds while entering/leaving the country. The AML/CFT requirement to declare cross-border transportation of currency related to the trade in diamonds often falls under a more general requirement for cross-border transportation of currency. For example, there is no specific legislation in Switzerland for the declaration of cross-border transportation of currency related to the trade in diamonds. This is regulated by federal legislation and is applicable to any kind of cross-border transportation of currency. In Russia, natural persons who exit or enter the country are obliged to declare cash in amounts equal to or exceeding USD 10 000. Origin of currency is indicated in the customs declaration. However, the customs authorities do not use this information, but instead file it with law enforcement agencies, including the FIU, for further use within the scope of powers vested in them. In Belgium, Israel, and the Netherlands, the FIUs received several currency Cross-Border Reports related to diamonds. In the Belgium, the Netherlands, and the UK, all movements of EUR 10 000 (or equivalent) or more entering or leaving the European Union must be declared. Some of these declarations may relate to the trade in diamonds. The declaration requests details of the owner, origin and use of the cash. Border Force

[70] Which is a general KPCS requirement valid in all KP countries.

agents may also detain cash found on a person at the border where the cash has been concealed and they believe it to be the proceeds of crime. In Namibia and the USA, there is a general requirement for diamond dealers to declare currency and monetary instruments that are being transported internationally.

Diamond are covered for AML/CFT in some countries as part of a list of precious stones (Canada, Israel, Mexico, United States, etc.) where if a certain precious stone is not included in the list than the law does not apply to trade in that specific precious stone.

CHAPTER 4.
FUNDING THE DIAMOND TRADE

In many countries, the diamond trade is funded (primarily) by financial institutions such as banks, although the participants may finance a part of the trade solely with their own equity. Some countries have specialised diamond banks or banks with designated divisions or branches that diamond dealers use for doing business and/or that provide financial services to them. In Israel where these special branches within banks exist, the financial services are only provided to licensed diamond buyers, sellers or manufacturers, where they manage a diamond designated account (DDA) in USD. Without a license, the bank will not open a DDA. specialised banks themselves hold a diamond dealer license. In those countries that do not have specialised diamond banks or designated diamond divisions/branches, financial services to the diamond industry are provided just as to any other trade. This means that many, though not necessarily all, of the following financial services are most commonly provided: bank guarantees, loans, use of diamonds as collateral, receipt and remittance of money. Israel indicated that when diamonds are used as collateral the bank will evaluate the diamonds with its specialist and after providing a loan, the bank will keep the diamond as the collateral. This is not a common practice but rather, represents exceptional cases where the account is problematic. The banks specialised in diamond trade offer a wide range of tailor-made financial services. Diamond dealers are usually treated as any other customer when providing credit, meaning that the same collateral will be requested in order to secure the loan. Vulnerabilities arise when diamond trade credit is extended at concessionary terms, thus making it more attractive in comparison to rates of credits in other sectors.

In most countries, the banks and credit institutions do not apply special Know Your Customer (KYC) or Customer Due Diligence (CDD) procedures to diamond dealers. This means that the same normal or enhanced due diligence procedures apply whether it is a diamond dealer or any other client (depending on the designated risk of the customer). However, some banks and credit institutions may consider the business as such higher risk or may take additional due diligence measures if their client is a diamond dealer. These measures can include extensive monitoring (including monitoring of transactions, site visits, etc.). Some banks or credit institutions may even have employees with a specialised technical knowledge of the industry. The diamond banks, like traditional banks, have policies and procedures for preventing ML and TF and their own monitoring and prevention systems. The specialised diamond banks perform an extensive compliance check of all diamond dealers before granting a loan. In one country, a special diamond office acts as a neutral party, verifying the copies of trading documents handed in by diamond dealers to the banks. This is because the bank works only on the basis of the documents and customer declarations and has no information on the actual diamond deal, thus making it difficult to evaluate the transactions.

The main methods of payment used by diamond dealers are *wire transfers* or *electronic funds transfer*. Cheque and cash are also used. In one country, the use of informal promissory notes for trade between diamond dealers is also accepted. These notes are generally tradable and notes that are not "crossed" are treated like ordinary cash. In many countries the use of cash is on the decline and not being used very commonly anymore. One country stated that cash is not used at all. However, cash may still be commonly used at the retail stage where small payments are sometimes

made in cash or used by smaller dealers. The use of cash is still a common method of payment in the diamond business in countries where cash is widely used such as in African and Latin American mining centres, or in trade centres like Hong Kong, China.

The prevalence of consignment agreements (or "memo" transactions) to purchase diamonds varies from country to country. A consignment is a private contractual arrangement as explained previously (see page 21). This necessitates the identification of the same diamonds by the consignor. Although consignment agreements are a very common trade method in some jurisdictions, especially in international trade, they may bear some ML/TF risks. These risks would be elaborated in the trade financing vulnerabilities.

CHAPTER 5.
STATISTICS (REPORTING, INVESTIGATIONS, INDICTMENTS ETC.)

A sample of **17** countries submitted contributions from team members and a few additional jurisdictions approached by the project team. While these jurisdictions do not include the entire diamonds industry, as mentioned previously team members represent a significant part of the international "diamond pipeline" (mining and production, trade and manufacturing centres, distribution and jewellers[71]). Not all project-participants were able to submit relevant **statistical data** in regard to the reporting and dissemination of STRs (suspicious transactions reports) by Dealers in Precious Metals and Stones (DPMS). In some cases, countries do not (yet) have reporting obligation for DPMS, thus no information concerning DPMS-reports could be submitted. This section aims to create an overview of the available information, by summarizing the project team member's input and by identifying common denominators in countries' individual AMC/CFT reporting obligations.

Based on team members contributions the following issues were looked at: is there a reporting obligation for DPMS and if so what is the reporting threshold for CTRs; what is the number of reports received from DPMS; what is the total number of reports related to DPMS (i.e. reports filed by DPMS or by other reporting entities relating to DPMS); number of reports disseminated to law enforcement authorities.

The table below presents the most important information provided by the 17 sample countries.

Table 5: **Overview DPMS reporting obligation and its results**

Co	Reporting obligation DPMS?	CTR Threshold (USD)	Number of reports from DPSM	Total number of reports related to precious stones (incl. DPSM)	Reports DPMS disseminated	Total number of reports disseminated related to precious stones (incl. DPMS)	Analysis period
1	No	n/a	n/a	n/a	n/a	n/a	n/a
2	No	n/a	n/a	n/a	n/a	n/a	n/a
3	Yes	9 600	112 STRs	n/a	23	23	2010-2012 (2 years)
4	No	n/a	n/a	n/a	n/a	n/a	n/a
5	No	n/a	n/a	n/a	n/a	n/a	n/a
6	Yes	63 600	11 836 CTRs 3 STRs	n/a	n/a	n/a	2012-2013 (1 year)

71 See footnote 11 for the percentage of rough diamond trade covered by team members.

Co	Reporting obligation DPMS?	CTR Threshold (USD)	Number of reports from DPSM	Total number of reports related to precious stones (incl. DPSM)	Reports DPMS disseminated	Total number of reports disseminated related to precious stones (incl. DPMS)	Analysis period
7	Yes	20 000	10 179 CTRs STRs – n/a	n/a	0	0 [1]	2009-2012 (2 ¾ years)
8	Yes	10 000	0 STRs	1 524 STRs	n/a	0	2012 - 2013 (1½ years)
9	Yes	No	10	115	3	139	Reporting period: 2005 – 2012 (8 years). Dissemination period: 2000 – 2012 (13 years)
10	No	No	n/a	5 820 UARs	n/a	23	Reporting period: 2007 – 2012 (6 years). Dissemination period: 2011-2012 (2 years)
11	Yes	2 500	36	n/a	n/a		2009-2012 (4 years)
12	Yes	8 550	2 UTRs	110	0	18	2008-2012 (5 years)
13	Yes	n/a	90 CTRs 24 STRs	n/a	n/a	n/a	n/a
14	Under implementation	n/a	n/a	n/a	n/a	n/a	n/a
15	No	n/a	n/a	20 STRs	n/a	n/a	n/a
16	No	n/a	n/a	n/a	n/a	n/a	n/a
17	Yes	No	0 STRs	n/a	0	0	n/a
TOTAL	Yes: 9 Under implementation: 1, No: 7	Yes: 7; range from 2 500 to 65 600, No: 3 n/a: 7	If yes (7), range from 0 to 112 for STRs; range from 490 to 11 839 for CTRs.	If yes (5), range from 20 to 5 820	In the case of filed reports (3), range from 3 to 23	In the case of filed reports (4), range from 18 to 139	

Note 1 : According to the contribution received, a total of 335 criminal cases related to the trafficking of precious stones have been opened in 20 different country regions since 2010 (based on law enforcement officials).

Reporting obligation DPMS: Out of the **17** countries that have submitted relevant data, 9 countries have a legal reporting obligation in place for DPMS to report STRs to the FIU (some

countries have also CTR reporting obligations). In **7** countries, AML/CFT legislation has led to CTR or STR reports by DPMS (between 0 to 112 STRs for periods which vary from one to five years). Several countries indicated that they receive reports concerning diamonds and/or other precious stones from other sectors then DPMS (mostly banks and customs). In one country, a large number of reports emanate from the banking sector (5 686 reports). In all, the information collected over the periods of time specified show low level of STRs reported by DPMS in the relevant countries.

Dissemination of reports to law enforcement: Only **2** out of **7** countries that have received reports from DPMS indicated that transactions related to diamonds and precious stones have been disseminated to investigative authorities. Two (**2**) additional countries have disseminated reports based on reports filed by reporting institutions other than DPMS. This information also show low level of FIU reporting to law enforcement and may be an indication of low awareness level of FIUs with regard to the diamonds industry.

CHAPTER 6.
THREATS[72] AND RISKS[73] RELATED TO VULNERABILITIES[74] IN THE TRADE IN DIAMONDS

Diamonds have the ability to earn, move and store value. They are a liquid and transferable asset. These are some of the features that make diamonds appealing to criminals[75] seeking to move, conceal and store the proceeds of crime. Diamonds have unique physical and commercial properties which carry value in small, easily transportable quantities.

The worldwide trade varies from modern international transactions conducted through the financial system, to localised informal markets. Dealers range from very poor individuals in some of the most remote and troubled places on the planet, to the wealthiest individuals, to large multinational companies working in major financial centres through specific unique trade mechanisms and diamond bourses. Transaction methods also range from anonymous exchanges of handfuls of stones for cash, to exchange-based government-regulated deals. A single one carat polished diamond can be worth more than USD 15 000, and, unlike cash, diamonds are often not required to be reported when transported or sent across borders.

This section of the report is based both on literature review conducted by the team members, the specific country contribution addressing the vulnerabilities and risks of their respective countries, and consultation conducted with the private sector at the national and international level.

PRODUCT VULNERABILITIES

Diamonds can be vulnerable for misuse for ML/TF purposes because they can transfer value and ownership quickly, often, with a minimal audit trail. They provide flexibility and an easy transportation of value.

A 2003 Report[76] assessed various alternative financing mechanisms that could be used to facilitate ML and/or TF. Trading in commodities, remittance systems, and currency were assessed on each of

72 A threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.

73 Risk can be seen as a function of three factors: threat, vulnerability and consequence. An ML/TF risk assessment is a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand ML/TF risks and serves as a first step in addressing them.

74 The concept of vulnerabilities as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threat means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.

75 GOA (2003), p 10.

76 GAO (2003).

their abilities to earn, be moved, and store value. Diamonds were the only alternative financial device that fit into all of these assessment criteria.

Diamonds possess several characteristics which make them vulnerable to ML/TF. These include[77]:

- **Very high value** – diamonds can store very high value. The higher the value, the more vulnerable a commodity is to ML/TF.
- **Low weight/mass and relatively small size – high value to mass ratio (easy to transport/smuggle)** – diamonds are easy to move and conceal, which makes them susceptible to smuggling. The transfer of value between countries is in many cases part of a ML/TF scheme and diamonds allow for the transfer of very high value.
- **High durability with stable pricing and an ability to retain value over long periods of time** – this makes them good for investment purposes (origin of money may be outside the industry). Also, it may attract criminals as they can distance the funds from their origin by transferring proceeds of crime into diamonds with minimum risk of confiscation and low risk of loss of value.
- **Ability to go undetected** (non-metallic and odourless) – diamonds will show on x-ray but because of the low density to x-rays they remain 'difficult' to detect.
- **Untraceable** - once the items change hands and enter the licit market they are difficult to trace, in terms of both their original ownership and value. Additionally, once the diamonds have gone through the beneficiation process and the rough diamonds are cut and polished, it becomes almost impossible to determine the origin of a stone, since Kimberley process only applies to rough diamonds.
- **Easily bought and sold outside the formal banking system** – AML/CFT measures are higher in the formal banking systems, but diamond transactions can be conducted outside this system and the value is carried between countries without having to go through the KYC procedures in the banking sector. Also, diamonds can be bought and sold in all parts of the world at almost any jewellery or pawn shop.
- **Unmarked** - It is virtually impossible to distinguish between rough diamonds that were illegally obtained and those that were legally obtained. Technology allows for the marking of diamonds so it would be possible to follow the trail of the diamonds, i.e. who is involved in the sale/purchase of the diamonds, however, most diamonds are unmarked. Diamonds are also

77 See for example Farah, Douglas (2005), which relates to some of the characteristics making diamond vulnerable to ML/TF: "Gemstones are ideal for several reasons: they hold their value; they are easy to transport; they do not set off metal detectors in airports; and they can be easily converted to cash when necessary".

easily disguised as other stones of much lesser value; the use of diamond simulants and synthetics can be used to commit frauds (predicate offence). Diamond marking can mitigate the risk of ML/TF the more it comes into practice and if documentation of the transactions include this data.

- **Evaluation of price -** The subjectivity of valuation of diamonds is a significant vulnerability. There are no official or agreed tariffs for rough or polished stones. The per-carat price of a diamond can vary considerably based on the crystalline shape, the carat weight, the colour and the clarity, i.e. the four (4) C's. Each qualifier imparts an individual measure of a diamond while also affecting the valuation of the other qualifiers; each measure is subjective and cannot be precisely stated (except carat weight). For rough diamonds there may be thousands of prices which are published by companies such as De Beers and Rio Tinto[78]. As stated previously, what is important to understand is that *diamonds are not one product*. From rough to cut and polished diamonds, *the price per carat can vary from few tens of USD to tens of thousands of USD*, based on the 4C's and the specific evaluation of the gemmologist or evaluator. Different professional evaluators may provide two reasonably and considerably different evaluations to the same diamond. This is one of the features enabling the manipulation of price for any specific deal (see also vulnerabilities of trade based ML/TF,). This may also cause difficulties in investigation and in judicial proceedings since it will be difficult to establish the price of a diamond where there is no true and unique value. On the other hand, it is just as difficult for criminals as for law enforcement to determine the value of diamonds.
- **Changeability** - From rough to polished, changing the dimensions of illegally gained diamonds make identification virtually impossible and can inhibit law enforcement from pursuing criminal charges.
- Readily exchangeable for other commodities or forms of currency (separate section broadens this issue below).
- **Susceptible to fraud** - The ease with which diamonds and other precious stones can be substituted for inferior or fake stones makes fraud more possible (see also vulnerabilities of the retail level). Diamonds are also susceptible for investment fraud.

These distinctive characteristics create not only vulnerabilities for ML/TF, but also for other criminal activity, including theft, smuggling and fraud. A vulnerability analysis of the diamond

78 Even-Zohar Chaim (2004), *pp.* 97, "the De Beers' Diamond Trading Company, for example sort them … into some 14 000 different categories". In the Hebrew addition it is stated that Rio Tinto sort the rough diamonds to 7 000 categories, *Ibid pp.* 113.

sector with regard to organised crime[79] awarded great vulnerability to 'the nature of the economic product'. The following properties/indicators were discussed.

- **Stability of the product**: As diamonds do not have an expiry date, no restrictions are imposed on criminal strategies by the physical nature of the product itself.
- **Mobility**: This indicator was awarded very great vulnerability since diamonds are very easy to be transported covertly.
- **Compatibility/flexibility**: Diamonds offer the criminal a lot of possibilities for setting up and continuing an extremely flexible organisation and activity.
- **Product differentiation**: diamonds, as a 'white product' cannot be individually identified or traced at any time, apart from marked diamonds. The laser inscription on marked diamonds can always be removed by a laser but this will still leave a mark of an inscription.
- **Elasticity:** Diamonds are extremely interesting as a means of payment or investment, also in relation to criminal activities of fraudulent entrepreneurs.

Certain product properties, such as the degree of mobility, as well as compatibility and flexibility, ensure that diamonds can be fit neatly into the illegal strategies of criminal groups, without a structural link to the diamond sector being necessary.

USE OF DIAMONDS AS CURRENCY

Diamonds display a high value-to-weight ratio, retain their value and are not affected by inflation or exchange rates, and are easily exchanged for other commodities or forms of currency. Diamonds can have similar characteristics as cash[80].

"Conflict diamonds" are not within the scope of this report. However, in conflict areas, diamonds were frequently used to finance wars by way of buying weapons. The KPCS was initiated to prevent the actual use of diamonds as hard currency in such a manner. These characteristics can be also used for ML/TF.

In practice, diamonds are being used as an alternate currency by criminals who use them to acquire other goods such as tobacco, guns, and, most commonly, drugs. Some countries (Australia, Belgium, Canada, Israel, USA) indicated that diamonds can or have been used as a form of currency. Canada noted that diamonds are also used by criminals for payment of debt, usually for drug debt.

79 Research carried out from 2001 to 2003. Cuyvers, L.; De Ruyver, B. & Vander Beken, T. (2004)

80 See also Even-Zohar, C. (2004), *pp*. 26 ("The easily concealable, readily transportable, high value nature of diamonds represent another factor which makes diamonds the currency par excellence for those motivated to avoid the use of "real" money").

In terms of ML/TF vulnerabilities, this is a particularly important feature since diamonds are not included in the concept of cash/currency or a bearer negotiable instrument (FATF recommendation 32)[81] even though it is possible to both launder with diamonds themselves and use diamonds as a means of payment to finance criminal activity, e.g. for the purpose of buying drugs or paying for illegal arms. The use of diamonds as a form of currency was also supported in the case studies submitted by team members. This will be illustrated below in the section analysing cases and STRs.

TRADE BASED ML

The typology of trade based ML (TBML) is defined quite clearly and was dealt with extensively by the FATF and FSRBs in recent years. In 2008 the FATF published a best practices paper on TBML[82]. The first section of the report states that:

> *"The Financial Action Task Force (FATF) has recognised misuse of the trade system as one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. As the anti-money laundering (AML) and counter-terrorist financing (CFT) standards that have been applied to other ML techniques have become increasingly effective, such abuse of the trade system is expected to become increasingly attractive".*

This statement is very relevant to the trade in diamonds. In 2006, the FATF published a typologies report on TBML[83] and in 2012 the APG updated and extended the FATF report[84]. Both reports included TBML cases relating to the trade in diamonds, exposing the vulnerabilities of the trade to TBML. Moreover, the APG report indicated that there are goods which are more susceptible to TBML due to the difficulty in identifying the true value of the goods, especially where the goods are subjected to higher taxes/duties or where the goods are of high turnover/value. Diamonds were amongst the goods identified[85].

One of the main methods through which TBML is conducted is by way of over or under valuation. The diamond industry is tremendously vulnerable to TBML primarily because of the high subjectivity in the valuation of diamonds[86], the ability of diamonds to change their form, the trade-

---

81 "For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action." (Interpretive Note to Recommendations, 32 paragraph 8).

82 See FATF (2008b), section 5 for a TBML definition.

83 FATF (2008b).

84 APG (2012).

85 *Ibid*, page 36, section 139.

86 See previous section on product vulnerabilities and the discussion on price evaluation.

based and global nature of the diamond market, and the long production chain involving many actors.

To compound the problem, there is no commodity or market price or "price list" for diamonds since there is no specific product[87]. With respect to parcels of bulk diamonds, which may include different diamonds of different size and quality, it is impossible and impractical for the evaluator to examine each and every diamond that is set for export and thus can be easily overvalued or undervalued to facilitate TBML schemes.

Transactions conducted by diamond dealers can amount to millions and even tens of millions of USD. This makes it easier to launder very high sums through the trade by over or under valuing the shipment by 5 to 10 per cent In the day to day trade, this will not be taken as unusual and will not alert customs official or banking institutions funding the trade and facilitating the transactions. Under these circumstances, Customs officers, who in many cases lack the expertise to evaluate a shipment, particularly bulk shipments, have no choice but to accept the shipper's self-assessment of the value of the goods. An inspection by an expert gemmologist on behalf of customs[88] may improve the situation and narrow the room for price manipulation based on expertise evaluation.

Tariff for customs declarations based on only carat - not only diamonds are hard to evaluate it is also, in many if not all countries, not necessary. Several team members stated that the declaration provided by the diamond dealer to customs as to the value of the diamonds is based only on carat, which is easier to verify since it is possible to weigh the diamonds. However, as previously explained, the price of diamonds is based on all 4 Cs and may change considerably with variation of Colour, Cut and Clarity. For example, the US has stated that the Harmonized Tariff Schedule (HTS)[89] is the primary recourse for determining tariff classifications for imports into the United States. The HTS classifies a good/commodity based on its name, use and/or the material used in its construction. US customs authorities believe that the HTS may aid in price manipulation, because the only valuation criterion it uses for diamonds is weight. In the US there are only two HTS subheadings for nonindustrial diamonds, worked but not mounted or set:

1. Weighing not over 0.5 carats each;
2. Weighing over 0.5 carats each

This means that only one of the 4 Cs (carat) is used to assess the value of a consignment of diamonds.

This is a gap built within the export/import systems which may also be easily exploited for over/under valuation while making it hard to establish whether there is an infringement of customs laws and regulation.

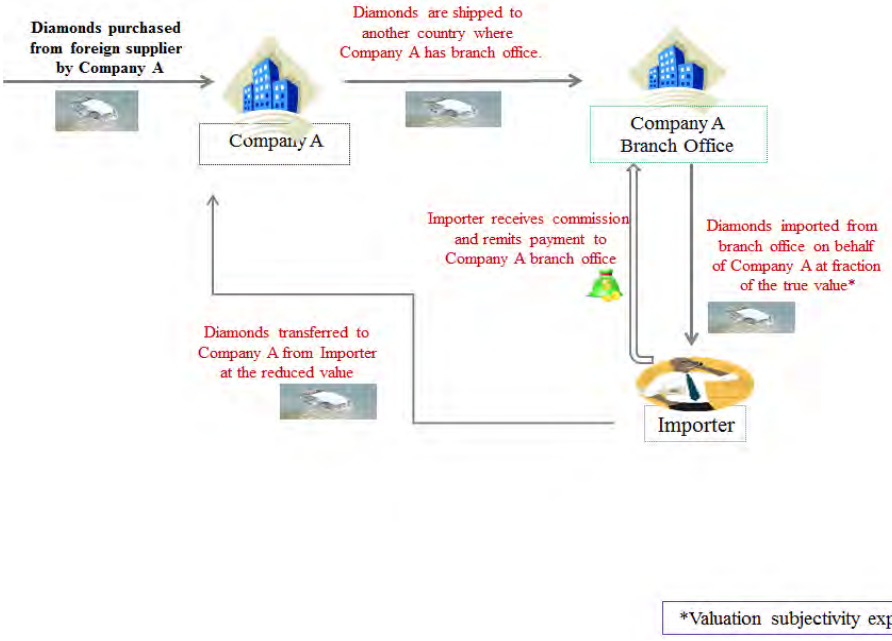
87 Every diamond has to be evaluated on its own merit. See also footnote 22.

88 Customs valuation of diamonds is subjected to the GATT 1994 Rules on Customs Valuation (Cascade system off 6 steps).

89 All members of the WTO/WCO apply the Harmonized Commodity Description and Coding System (or HS). In US it is named HTS, in EU GN, etc.

Thus, diamonds sold may be shipped from one jurisdiction to another and be assigned low value to minimize inland revenue or export duty, then traded in the other jurisdiction or re-exported from it with a much higher "price tag". The value generated from the final sale of the diamonds will be much higher than their original stated value, but no real value will be added along the trade path, except for the "mark-up" by the traders. According to KP statistics, some trade centre's show considerable differences between the average price per carat coming into the jurisdiction compared with the average per carat price leaving the jurisdiction. As previously detailed this difference can be explained to a certain extent by sorting and valuation of the diamonds which may produce an added value of between 10 to 15 per cent[90]. But, it can also provide an indication of tax evasion schemes, or ML/TF trade-based activities.

Figure 6: **Trade Based Money Laundering / Tax Evasion**



REGULATION OF DIAMOND DEALERS

FATF Recommendations on dealers in precious stones - Recommendation 22 only applies to dealers in precious stones when they engage in any cash transaction with a customer equal to or above the applicable designated threshold. Analysis showed that the extent of cash usage seems to be diminishing and that most of the transactions are not conducted in cash. There is no obligation for customer due diligence or record-keeping requirements when dealers in precious stones use wire transfers or other means of payment. This makes the sector more vulnerable to ML/TF, particularly because precious stones including diamonds can be used as a form of currency/payment.

90 Price increases between import and export are largely due to sorting and valuation activities, an essential element in the diamond pipeline. Sorting diamonds into different sizes &grades is time consuming, requires very specific know-how and is a value adding activity along the supply chain. This is an essential stage in the diamond dealing process.

Since the AML/CFT duties are only relevant to cash transactions, it is possible to establish the method of payment only when the payment is received, which can be a long time after the deal has been made and the diamonds have already changed hands. Again, this is important since it is possible to launder with diamonds, as they are themselves of intrinsic value and a form of currency.

National AML/CFT regulation of the industry - There are still several countries where diamond dealers are not subject to AML/CFT legislation and therefore have no reporting responsibilities. These businesses that buy and sell diamonds are not obliged to undertake AML/CFT risk assessments, implement due diligence procedures or report transactions to the national FIU.

The issue here is the KYC, which is neither legally required nor ordinarily carried out by the traders in diamonds who are not under an AML/CFT regulation. For diamond dealers, the risk of being involved in or being used for ML or TF is not limited to the customers (subjects to whom they sell diamonds). There is also a risk when establishing a business relationship with diamond suppliers, when purchasing transactions give rise to payments that are wholly or partially, directly or indirectly carried out by other means than by transfer to bank accounts held with referred credit institutions. Payment by other means than by transfer to bank accounts is considered a high-risk situation for illicit trafficking, which always has to be taken in account.

In order to deal with these high-risk situations, the identification requirement not only needs to be obligatory for diamond dealers, but also needs to extend to suppliers in diamonds when the delivery of diamonds results in cash payment.

AML/CFT regulation applicable according to precious stones lists - Even though the project is focusing on the trade of diamonds, it was established during the collection of information from the relevant countries that the definition of a precious stones dealer is in many cases based on a list of precious stones (Canada, Israel, US) which cover only part of the market, leaving other parts of the precious stones sector uncovered by AML/CFT regulation. This creates a ML/TF vulnerability since a money launderer or a terrorism financier can make transactions of high value without being covered by AML/CFT legislation (no KYC, no reporting, etc. will be conducted).

Record-keeping - As noted above, there are very limited AML/CFT record-keeping obligations for dealers in precious stones. Some countries reported that, due to specific business practices where the diamond trade is based on trust and verbal agreements, diamond dealers may not fully record transactions in cases where they know each other. Vague and inconsistent records within the industry complicate financial investigations for law enforcement.

False records and invoices and, more importantly, lack of detail on records precipitate laundering with these commodities. The lack of detail is important to note: while false invoice is definitively criminal, lack of detail on an invoice is not. However, without sufficient detail, law enforcement has difficulty determining the extent of criminal activity, if any, and then may not be able to articulate such in court. Additionally, lack of details may prevent banking institutions from reporting transaction to FIUs with all required information.

Physical cross-border transportation of diamonds and currency - Although diamonds can be used as a currency and to store value, they are not included in the concept of cash/currency or a

bearer negotiable instrument (FATF Recommendation 32)[91]. Countries are not obliged to have measures in place to detect the physical cross-border transportation of diamonds through a declaration/disclosure system. The Customs declarations on cross-border transportation of cash that an FIU receives do not include diamonds.

Loose vs. mounted diamonds – in general terms the legislation applying to loose diamonds is different from that which applies to mounted diamonds.

Compliance of the sector - Although the AML/CFT legislation applies to diamond dealers, FIUs have not yet received many disclosures. This may be an indication that there is not enough awareness in the sector of the importance of combating ML and TF within the diamond sector and that diamond dealers are not sufficiently aware that their sector is being misused by criminal organisations to launder their proceeds. Improved awareness of the AML/CFT legislation could result in a diminished restraint to report.

SUPERVISION, CONTROL AND ENFORCEMENT VULNERABILITIES

SUPERVISION

Registration and licenses - Only in a few countries are licences and registration required for business activity in the diamond trade. This has a major impact on supervision of the sector and this makes the KYC procedure for diamond dealers and financial institutions handling diamond dealer accounts very difficult.

Fines and penalties on non-compliance - Due to the lack of AML/CFT obligations in several countries, few AML compliance assessments on diamond dealers have been carried out. Although the overall compliance of the sector is assessed as medium in those countries with AML/CFT obligations, no fines have been issued to diamond dealers and no other AML/CFT civil enforcement actions have taken place over the last two years.

CONTROL

Customs Control and over - and under-valuation - In several countries there is no separate set of guidelines or procedures for monitoring the import/ export of diamonds by the Customs Department. The import and export of diamonds are dealt with in the same manner as those of any other article or commodity. Given the specifics of diamonds (high value in small size and not detectable by specialised equipment), effective and specific control by customs is necessary.

---

91 "For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action." (Interpretive note to recommendation 32 paragraph 8).

Furthermore, the size of the industry makes it extremely difficult to verify each and every diamond consignment set for import or export. Additionally, it is sometimes not possible for customs to identify the correct value of the consignments (a lot of under- and overvaluation of diamonds takes place). Shortage of expertise in gemmologists makes it difficult for customs to assure the real value of every shipment of diamonds or other precious stones against invoices and freight documents.

Issues related to KP certificates - Since the implementation of the Kimberley Process Certification Scheme (KPCS), no conflict diamonds can enter a KP member country in a legal manner. All shipments of rough diamonds require a certificate specifying the origin of mining, volume and value, and are checked and confiscated immediately when no certificate is available. All trading countries are required to submit data on production, import and export of rough diamonds. The risk is situated in the fact that current enforcement efforts related to diamonds are directed more at ensuring compliance with the KPCS rather than preventing smuggling, fraud, or ML. Therefore, the primary legal and regulatory focus regarding diamond smuggling is on rough, rather than cut and polished diamonds. While important, it does little to prevent the use of finished diamonds in TBML schemes.

The KPCS lacks transparency for controlling officers at the border. There are specific requirements for KP certificates to have certain security features in place and known certificate forgeries and examples of certificates and authorised signatures are shared between KP members. Due to the lack of a universal standard for the format and/or specifications of a Kimberley Certificate (KC), it is almost impossible for customs officers not experienced in the diamond trade to intervene or recognize forgeries. This also applies to official certificates of origin and invoices of certain countries. The validity period of the Kimberley Certificate is often too long, opening up the possibility of misusing the certificate for more than one shipment[92]. The section on the KC where the weight (carat) of the diamonds needs to be filled in is sometimes not appropriate for adding numbers, which is why it is easy to manipulate the total weight (carat). This also applies to changes made on a KC - these need to be officially confirmed by means of a signature and official stamp.

Issuing new KPC also raises questions. According to the KPCS the KPC that come with imported diamonds are kept in a country and not sent with the following export of the diamonds. The rough diamonds that leave the country for export receive a new certificate issued by the responsible authority in the exporting country. This legitimate procedure may be exploited by criminals and is one of the major vulnerabilities of the KPCS whereby the actual origin of the rough diamonds is often concealed and practically impossible to retrieve[93] by moving the rough diamonds through trade centres for the purpose of issuing a new KPC. When exported from the mining country the KPC will include the country where the diamonds were mined. In a later phase, since the shipment of rough diamonds may include diamonds from several mining countries, the exported diamonds receive a certificate indicating that the diamonds originate from more than one country without

92 Legally it is not possible to use the same certificate twice.

93 The KP is not a certificate of origin and therefore the origin cannot be traced by it. This leaves the ML/TF vulnerability uncovered, not even by the KPCS.

specifying which countries[94]. This is mandatory according to the KPCS and a common trade practice; however it may create an opportunity to for criminals to misuse this practice. Information received from one jurisdiction indicated that this practice has taken place.

It should be noted that the KPCS does not regulate the movement of cut and polished stones but only focuses on rough diamonds.

ENFORCEMENT

Limited awareness - Enforcement of the diamond sector is exposed to a degree of vulnerability due to the limited number of skilled experts to appropriately enforce the regulations applicable to the sector. All enforcement of legislation and rules relevant to this industry is only enforceable through the right set of skills. The skills needed for valuing diamonds are quite rare and expensive to obtain; this makes it difficult for governments to provide the necessary investment. Most law enforcement professionals do not possess the necessary skills to identify a diamond, let alone to evaluate it. Few countries possess a specific diamond squad within their police department to tackle these cases. There is little specific enforcement of any crimes related to diamonds. Law enforcement looks at these crimes/commodities the same as all others and does not relegate specific resources towards it. In general, law enforcement has little knowledge about crimes and criminal activity involving these commodities/industry.

Collection of evidence - The diamond sector has refrained from proper documentation and book keeping for almost 90 years. As a result, there is hardly any evidence of the terms of agreements made by diamond industry representatives. The only evidence of transactions is the invoice and shipping documents presented to customs. The strict confidentiality practiced by the actors in the trade imposes secrecy even in conflict situations, breach of contract, fraud attempt, etc. There are also many unknown factors in law enforcement about what evidence is even available and then how to collect it/use it.

International police cooperation - The bottleneck in effective law enforcement remains international cooperation and confirming the relation with TF. In order to address the problem of fraud in the diamond sector, international awareness and cooperation in harmonizing and implementing legislation needs to be established. The diamond trade is characterised by international financial flows, and also by flows of goods. In order to have a successful police investigation and have the criminal assets confiscated, international cooperation of the authorities is a prerequisite. In particular, the countries **involved** in the different stages of the trade be it mining countries, trade centres, cutting and polishing centres or retail centres, such as the Lebanon, Switzerland, the United Arab Emirates and countries on the African continent. A deficiency in the information exchange could seriously undermine the investigation and the success of a conviction. The police stated with regard to one of the billion dollar trade centres that even though it is a full participant of the KP Process, it refuses to share basic KP information such as statistics on import

[94] Only if positive proof exists that the goods in the shipment consist of rough diamonds from one (KP) production country only will that be mentioned, in all other cases "*****" must be filled out on the KP Certificate.

and export of companies. The inflexible position of such jurisdiction within the trading route creates issues for other partners seeking to investigate ML and TF.

Judicial follow-up – Few examples were found of cases that were reported to judicial authorities or brought before court. Also, statistics are not available. Many files concerning ML from illicit trafficking in diamonds from the FIU reported to the judicial authorities are dismissed. The non-punishment of diamond trade-related offences is a major vulnerability in the prevention of ML/TF.

VULNERABILITIES IN THE DIFFERENT STAGES OF THE TRADE[95]

As detailed previously, the diamond industry has a very long chain of production from the mining to the final customer, known in the industry as the "diamond pipeline". This "pipeline" involves practically all parts of the globe when taking into account the retail level, including internet trading platforms. On top of the vulnerabilities of each jurisdiction in terms of the regulation, supervision and enforcement, there are vulnerabilities associated with each level of the trade where the level of risk may change from jurisdiction to jurisdiction (in light of the specific characteristics of the trade in the jurisdiction). Some vulnerabilities are relevant for all stages of the trade (e.g. theft, commingling).

MINING

Vulnerabilities of alluvial *vs.* kimberlitic mines – Kimberlitic and alluvial mines differ in their level of their vulnerability to ML/TF. The vulnerability of the mining stage is dependent on the level of supervision and control put in place by the relevant national authorities[96]. In general, the vulnerabilities of the mining stage are those associated with *illegal mining*, *commingling* of illicit diamonds and *theft*. Since kimberlitic mines are usually much easier to secure and control, they are less vulnerable and less exposed to these risks. In contrast, since alluvial deposits are much harder to secure and, as previously detailed, since mining may span over very large geographical areas, conducted to a large extent by artisanal and "informal" miners by hand, the risk of abusing these vulnerabilities is much higher. Thus, countries where alluvial, particularly artisanal mining[97], are more prevalent are more vulnerable to ML/TF activity.

Sierra Leone indicated that the diamond trade in Sierra Leone has been, and will remain to be, a major flashpoint for criminality and a high risk sector for ML and TF and has pointed to a link which can be made between ML **and** trade in diamonds to the trade in conflict diamonds. During the workshop in Dakar it was indicated that there are people coming to the country from abroad with cash and then fly out with diamonds.

---

95 For a short discussion on some of the vulnerabilities in the different stages of the diamonds pipeline, see Siegel, Dina. (2009), *pp*. 160-161.

96 See previous discussion on the characteristics of kimberlitic and alluvial mines on page 17.

97 See World Diamond Council (n.c.) - "Prevalence of small-scale alluvial diamond digging is highest in Angola and the Democratic Republic of Congo (DRC) but also takes place, on a smaller scale, in the Central African Republic, Cote d'Ivoire, Guinea, Ghana, Liberia, Sierra Leone, Tanzania and Togo. It is estimated that 1.3 million people in Africa work in this sector".

Canada indicated **that** despite the highly controlled mining and security environment, increased diamond flows will provide more opportunity for attempts by criminal groups to infiltrate diamond mining and trading.

Illegal mining – This is one of the major issues for mining countries. South Africa indicated that there is a trend of illegal mining in the country that is becoming more prevalent. The trend is facilitated by the fact that some of these illegal miners are either mine workers or former employees who know the workings of the mines they target. Because of their size, diamonds are smuggled out of the mine premises without detection as they can be slipped under fingernails or by being swallowed; the use of homing pigeons was even noted. There are unfortunately certain players in the industry who are willing to buy illegal diamonds without questioning their origin. It was also indicated that the issue is that once the illegal diamonds have entered the industry it is impossible to track them. The diamond will be presented as if they were mined legally, and afterward they will be sold to diamond dealers who would export the diamond with a KP certificate issued by the appropriate authorities. This method of commingling illegally mined diamonds is also conducted when diamonds are mined in neighbouring countries, smuggled across the border and then inserted into the legitimate trade. The problem of illegal mining and smuggling was brought up by two additional African mining countries in the 2012 FATF / GIABA Typologies workshop.

ROUGH TRADING

The product vulnerabilities discussed above are characteristics of the trade in rough diamonds. There are additional vulnerabilities with respect to the KP certificate which should also be noted.

Kimberley certificate is required only on import and export – According to section II (a) of the Kimberley Process Certification Scheme *"Each Participant should ensure that: (a) a Kimberley Process Certificate (hereafter referred to as the Certificate) accompanies each shipment of rough diamonds on export*[98]*".* When a rough diamonds is traded locally there is no need for a Kimberley certificate. Thus, it is possible to cut an illegally mined or otherwise illegally gained rough diamond, polish it locally in order to conceal its source and export the polished diamond without the need to issue or present a KP certificate[99]. While a change in the scale of beneficiation has a positive side, the more mining countries, particularly African countries, expand their beneficiation process the risk of cutting and polishing the rough diamonds locally and avoid the need for a KP certificate, as a ML/TF tool, may increase. This may also mean that the risk of rough diamonds being smuggled and then cut and polished as a mean to conceal their illegal source may also increase. For example, it would be easier to conceal rough diamonds bought with cash proceeds of crime by cutting and polishing the stones locally and exporting the polished diamonds without the need to issue a KP certificate.

Kimberley certificate and ML/TF – the KPCS was established for the purpose of curbing the trade in "conflict diamonds". While there may be some bearing on ML/TF activities in that the predicate

98 See Kimberly Process (nc), page 5.

99 For this reason the World Diamond Council has created the WDC System of Warranties, by adding a warranty stating the conflict free nature on each invoice.

offence may be committed by those who are involved in the trade in "conflict diamonds" (such as smuggling), this is not ML or TF per se. However, when a shipment of rough diamonds is accompanied by a KP certificate, this may give legitimacy to the shipment to customs officials and bank employees.

TRADE CENTRES (ROUGH/POLISHED)

Transfer pricing – transfer pricing can take place at a variety of stages of the trade, but FTZ centres are most vulnerable. As mentioned, the diamond trade is international in nature. The diamond industry includes multinational companies with operations spanning across many countries, serving as trade centres of rough and polished diamonds. The term 'transfer pricing' is usually used in the context of tax regimes where related companies (subsidiaries, affiliates) conduct international transaction between themselves[100]. Such practices are also prevalent in the diamond industry. While transfer pricing may be conducted in a legitimate fashion (i.e. in accordance with relevant tax regimes), it opens up the possibility to commit tax fraud and ML. Diamond trade centres like Dubai, which operate as FTZ are susceptible to vulnerabilities as specified in the FATF report regarding the ML vulnerabilities of FTZ.[101] This, in combination with the specific vulnerabilities of the diamond trade and the mechanism of transfer pricing, creates a significant vulnerability for ML and TF activities. By way of over or under invoicing with affiliate diamond companies located in FTZ, it is possible to illegitimately shift profits from diamond companies in high tax rate countries to FTZs and thus avoid taxes[102]. It is also possible to use the same scheme for ML/TF purposes. The combination of a lack of transparency in the diamond trade with a lack of transparency in a FTZ provides an excellent atmosphere to conduct large volume transactions without being detected.

Transfer pricing can occur during different stages of the trade, such as rough diamond trading from African mining countries to diamond trade centres where by African countries will be losing huge amounts of due tax to FTZs. One African mining jurisdiction indicated that the risk of transfer pricing is ever eminent. It can also occur as stated above between two trade centres of both rough and polished diamonds where one jurisdiction will have high tax rates and the other jurisdiction will be a FTZ or have very low tax rate.

Issuing of new KP to conceal the source of diamonds - Belgian investigators have noticed that shipments are being diverted to one of the billion dollars trade centres where the original certificate and invoice were, still in accordance with the rules of the Kimberley Certificate, turned into a new KP certificate (origin: mixed or unknown) **with a higher price** and sent further to a trading centre. Although each member state of Kimberley is obliged to make a new Certificate, the police suspect

100 For a definition of transfer pricing see TP Analytics (n.c.).

101 In March 2010 the FATF published a typologies report – *Money Laundering Vulnerabilities of Free Trade Zones*. The documents illustrates the vulnerabilities associated with FTZ particularly TBML including over and under invoicing. According to the report a FTZ provides among other things a relaxed oversight and lack of transparency. The report also states that "The existence of vulnerabilities in a system makes it attractive for money launderers and terrorist financers".

that this trade centre is used as a transit country that produces "new" documents to hide the origin of the diamonds and facilitate the diversion of payments.

The full purchase price, as mentioned on the invoice, is transferred and channelled to different accounts all over the world, private accounts or accounts of individuals. In the accounting, all transfers are recorded on the supplier situated in this particular trade centre. The relation between the beneficiaries of the funds and the supplier in the trade centre is unclear. Police investigations showed a strong relationship between the final buyers and the companies in the trade centre. Once a supplier was identified by the police, the relationship ended and the trade went on through another supplier.

Facilitating corruption - From a trading centre perspective - through under-invoicing of the rough diamonds in mining countries, acquired margins may be created to facilitate payments to PEPs, military or other invisible stakeholders in the transaction.

CUTTING AND POLISHING

Diamonds are not bound by any certification requirements to identify origin once cut and polished – This is another feature which makes diamonds very easy to move and conceal high value, and is also what lends polished diamonds similar characteristics as those of cash. This means that it is easy to move the diamond up the supply chain through trade centres for polished diamonds without an ability to verify the origin of the diamond; the larger and less supervised the market is, the easier to move the stones. Moreover, as there is no requirement to document the origin of the diamond while conducting a business transaction in polished diamonds, it may be impossible to verify who the previous sellers were, i.e. it is easy to lose the polished diamond trail. However, there are technologies in place which enable diamond marking. This technique allows a polished diamond to be traced to its origin and facilitates a better documentation of transactions by including the details of the diamond as part of the documents accompanying the transaction. However, marking is not done on all diamonds and is not documented on all transactions, leaving the possibility to lose the "diamond trail".

Untraceable diamonds - Cutting and polishing is often an important part of illicit diamond trading. A diamond's size and form can be significantly altered, making it more difficult to trace the stone back to its origin as illicit rough. It is also possible to further cut an illicit polished stone so as to avoid the identifying of the polished stone which was illegally gained (E.g., recut a stolen polished diamond). Thus, one part of disguising the origin of an illegally gained rough or polished stone can be to cut or recut it, polish the diamond and then sell it within the local or international market. It should be noted that whilst there is an increasing trend for diamonds to be cut and polished in the country of origin (beneficiation), the vast majority of diamonds continue to be processed in the 'cutting centres' that are outside of the producing nations. There have been suspicions that clandestine diamond operators in some producing nations, particularly African alluvial, have been cutting and polishing. Whist this might be true on a very limited scale there is a continued lack of evidence to support the notion of any scaled up polishing being carried out. Consequently the main focus should remain on rough diamonds.

RETAIL LEVEL

The retail level is perhaps the largest part of the diamond trade chain. It includes jewellery shops, pawn shops, trade fairs and wholesalers of jewellery, and encompasses both new products as well as the recycled market. While mining and trade centres are located in specific countries, it is estimated that there are more than a quarter-million retailers who sell jewellery to consumers around the world[103]. The entire jewellery manufacturing and retail market are too great for the scope of this report, but they may be touched upon based on the analysis conducted on the different stages of the trade and the vulnerabilities identified by team members. The following vulnerabilities were identified:

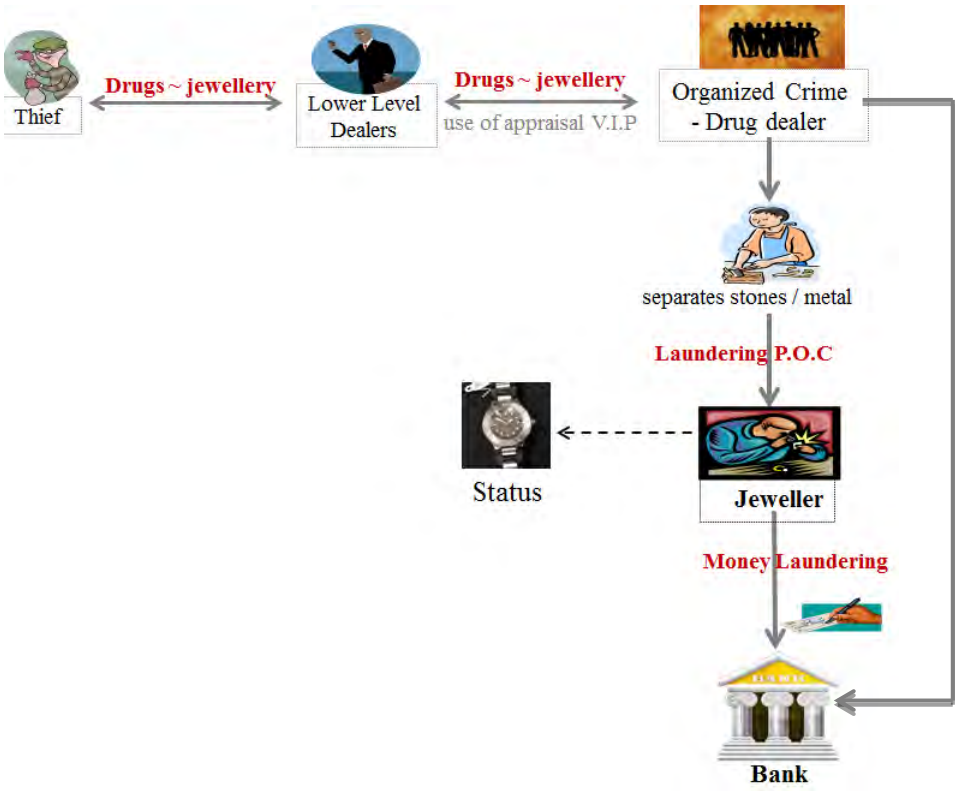
Supervision and enforcement are difficult - due to the extent of the sector it was indicated that it is very hard to conduct supervision and enforcement. Jewellery retailers can vary from very small individual jewellery shops up to worldwide chains with hundreds of outlets. Some jewellers do not have enough capacity or are not legally required to dedicate resources to AML/CFT campaigns or reporting. They may also be less wary of AML/CFT in general and could be a target for criminals to launder goods.

Use of cash - It was noted by Canada that further down the supply chain, i.e. the jewellery/retail level, the trade becomes more cash -based. Large cash deposits provide an opportunity for jewellers to introduce illicit funds into the legitimate economy disguised as proceeds of cash sales from diamonds.

Laundering of stolen jewellery/drug proceeds – this is perhaps the main vulnerability identified, particularly through actual cases submitted by team members where the retail level was used to launder funds or illicit diamonds. Second-hand jewellery shops and pawn shops were identified as vulnerable by allowing stolen diamonds or diamonds which were used to pay for the purchase of drugs to be re-entered into the market by selling the goods at the retail level, in many cases as accomplices of the criminals. As mentioned above some of the cases emphasised this vulnerability of the retail level by showing how laundering is taking place in actual means. The US indicated that small jewellery shops may deal with extremely large amounts of sales (millions of dollars annually). This provides the possibility to launder very large sums of money. This vulnerability is basically not different from that which characterises other parts of the trade, i.e. *commingling* of illicit diamonds. Commingling can be done at each and every part of the trade chain.

103 Bain & Company (2011), pp 50.

Figure 7: **Criminal Organisation Importing / Producing with several lower level syndicate dealers**



KYC/CDD measures – retailers will buy polished diamonds either from a local wholesaler or from foreign wholesalers. Conducting CDD procedures with foreign suppliers/customers can be difficult as it is not always possible to establish the identity of the beneficial owners of the foreign company and to verify that the information provided is genuine. It is often easier to conduct KYC/CDD procedures with local retailers or wholesalers since identifying information is more available.

As reported by authorities, in consultation with the relevant private sector in each country, KYC or CDD requirements for dealers in diamonds are usually not legally required for two main reasons:

- there is an informal knowledge of the actual and potential customers due to the recurring business activities and transactions conducted, or
- these requirements are covered by other reporting and registry obligations, mainly related to taxes or accounting.

While this is true for B2B transactions, the situation is different with retail transactions or sales directly to the customer.

Fraud - One jurisdiction indicated that the main vulnerability of the retail level is fraud which can be divided into several types:

a) False grading – where a stone's true grade is not reflected in the nominated grading.

b) False certificates – where a grading certificate has been counterfeited, subject to unauthorised amendment, duplicated and attached to stones of varying quality.

c) Misrepresentation of stone – where other stones are passed off as diamonds.

d) Non-disclosure of type – where synthetic diamonds and fracture-filled diamonds are not declared as such and are passed off as undamaged, naturally-mined diamonds.

e) Valuation fraud – where a stone is undervalued to avoid customs duty and/or tax.

Theft/Robbery – as other sectors of the trade, it is susceptible to theft and robbery (see also below vulnerabilities related to all stages of the trade).

VULNERABILITIES IN THE USE OF THE INTERNET

The internet has been for many years now a trading platform for goods and services of every kind, and this includes the diamond and jewellery trade. In the United States, such trade sites began operation mostly during the last decade. While the average retail sale on the internet is under USD 10 000, internet sites have become celebrated by both large and small buyers for its "price quotes". These sites give buyers across the country access to New York wholesale market prices for diamonds. Since it has no advertising overhead and gets customers through word of mouth, it may save consumers up to 40% from retail prices. This relatively new trade platform also brings with it vulnerabilities which may be applicable to all sales and purchases on the internet, including buying of rough and polished stones and diamond jewellery. A quick survey on the internet reveals that the largest diamond companies offer online platforms (De Beers, Alrosa, Rio Tinto and BHP Billiton), with a very developed international online market of diamond dealers of every size.

KYC/CDD measures – internet trading platforms allow for both B2B and B2C transactions. Conducting transactions over the internet allow for increased anonymity of the customer, making it harder to conduct KYC/CDD procedures. For example, it is possible for a customer situated in one part of the world to buy diamonds which will be sent from another part of the world via courier services such as FedEx without the diamond dealer and the customer ever meeting. The price of the diamond can be very high (for example, the price of 12.01 Carat D-IF Excellent Cut GIA Certified Round Diamond 14.69-14.73x9.13mm, up for sale on EBay, has reached 2.725 million USD, see Figure 5). When speaking about a sector which is not regulated as well as financial institutions, it is hard to enforce on diamond dealers the application of AML/CFT regulation, including KYC/CDD measures.

However, and perhaps of more importance, since the FATF definition of dealers in precious stones includes only cash transactions, the internet trading platform for diamond dealers is not covered by the AML/CFT standards[104], since payment is facilitated almost entirely through banking and credit institutions or internet payment means. While these financial institutions may perform their KYC duties based on the applicable regulation of the jurisdiction, it will be performed on the party transferring the funds only and not necessarily on the customer buying the diamond over the internet.

[104] There may be instances when national legislation goes beyond the FATF Recommendations and may cover this activity.

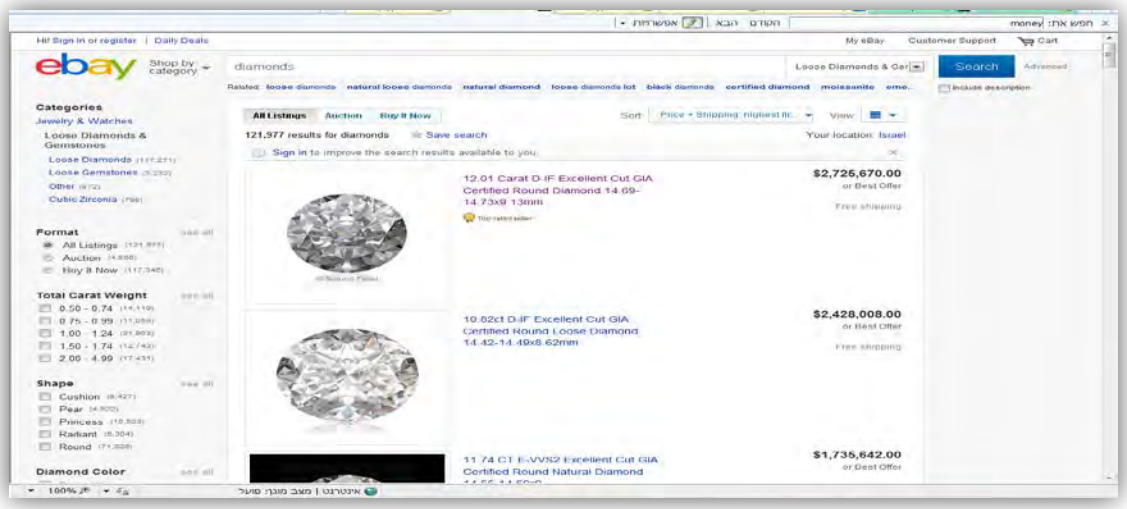
Checks conducted by the project team located trading sites providing a platform for buyers to meet sellers, conducting tens of thousands of gem stones auctions, including rough and polished diamonds, where in registration all that is required is a username password and email to verify registration:

> "*In order to participate in the auctions … you must first register to become a member. First, you must* select *a username, which is the name you will be known by while you're on our site. Please note your Username will be viewable by all … members. You will also be asked for a password to secure your account. Please note that once you've chosen a username, you will not be able to change it.*
>
> *You must provide valid contact information and a valid e-mail address. This is required so that buyers and* sellers *will be able to contact one another once an auction closes*"
>
> "*After you submit your registration, you will receive a confirmation e-mail message … You may begin bidding* immediately"

This registration procedure of minimal identifying requirements is similar to some internet payment means which in the past facilitated ML activity (*e.g.,* E-gold[105]).

This means that trading platforms may be used to easily move very high value stones internationally without either establishing the identity of the buyer or the identity of the seller.

Figure 8: **Example of eBay online trading site – cut & polished diamonds worth millions of USD**



Source: Internet screen shot July 2013

Rough diamond online sales – as mentioned above, it is also possible to buy and sell rough diamonds via the internet. This may also be done globally using international courier services. It is not clear in all websites whether a Kimberley certificate is attached to the shipments in these transactions. One web site indicated that "*all international shipments will receive a UN "Kimberley*

105 See US Department of Justice (2007).

Certificate". All domestic shipments come with the appropriate guarantees that they are non-conflict diamonds as laid out by the United Nations[106]".

In a consultation with WFDB it was noted that it would be difficult to buy rough diamonds online since it is necessary to physically examine the stone in order to evaluate the price. Online sites offer a refund in case a customer is not 100% satisfied; however, this is vulnerable to fraud[107].

Internet payment systems – in 2010, the FATF published a typology report on "Money Laundering Using New Payment Methods" (NPMs)[108]. The report identified the vulnerabilities associated with NPMs, including anonymity and the global access to cash through ATMs, but also stated that "where NPM providers are subject to AML/CFT obligations and appropriately supervised for AML/CFT purposes, NPMs can make payment transactions more transparent and help prevent corruption or other abuses". This is because a transaction via NPMs leaves an "electronic record". The vulnerabilities that were identified in the above mentioned report create risks to the trade in diamonds over the internet, in light of the previously discussed characteristics of the product and the fact that diamond dealers are not routinely subjected to AML/CFT obligations for the majority of their transactions over the internet. However, to the extent that AML/CFT obligations apply to both NPMs and diamond dealers on the internet, the "electronic records" may serve as a mitigating factor by providing an audit trail.

Trading platform as a mean to launder funds – it is relatively easy for a criminal or money launderer/terrorism financier to establish a diamond trading platform online to disguise the source of funds.

Fraud – a customer buying a diamond via an internet trading platform is exposed to the risk of fraud. Fraud -related vulnerabilities were previously specified with regard to the retail level of the trade (false grading, false certificate, misrepresentation of the stone, non-disclosure of type and valuation fraud). All of these vulnerabilities also apply to the online trading platform. However, there is an additional vulnerability of no supply, where a customer pays in advance but does not receive the stones he or she paid for. There are payment and delivery methods whereby a customer can avoid such an occurrence. For example, a diamond may be shipped to the customer for inspection and payment is made only after the customer has examined the stones and the documentation to his or her satisfaction. The stones are shipped upon proof of payment to the secure courier service. According to the consultation conducted with the Jewellers of America, in most cases the customer will see a diamond prior to purchasing it.

Laundering stolen diamonds via the "Darknet" –In spite of not being a common activity, Silk Road offers jewellery with diamonds of unknown origin. It can be purchased and paid in Bitcoins. It is delivered by Fedex or any other courier service in a plain envelope without a description of the goods inside.

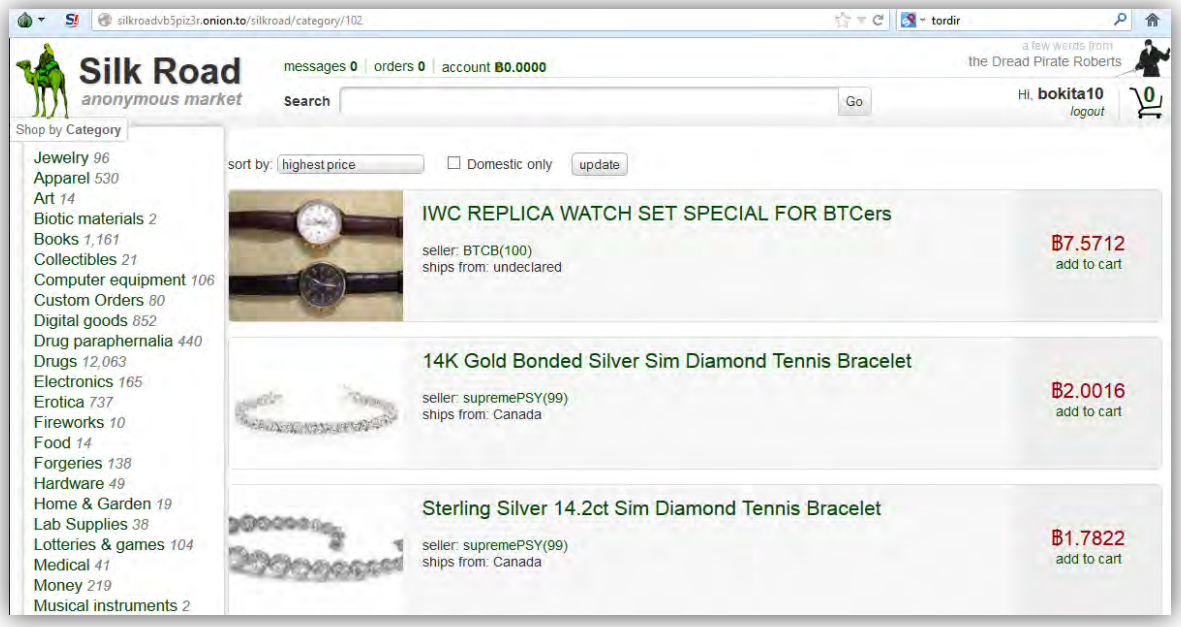
---

106 While the UN indeed supports the KP, it doesn't have any formal/legal relationship with the KP (indeed, the KP itself is not a legal entity). In other words, KP certificates have nothing to do with the UN.

107 This is not unique to online diamond trading platforms.

108 FATF (2010).

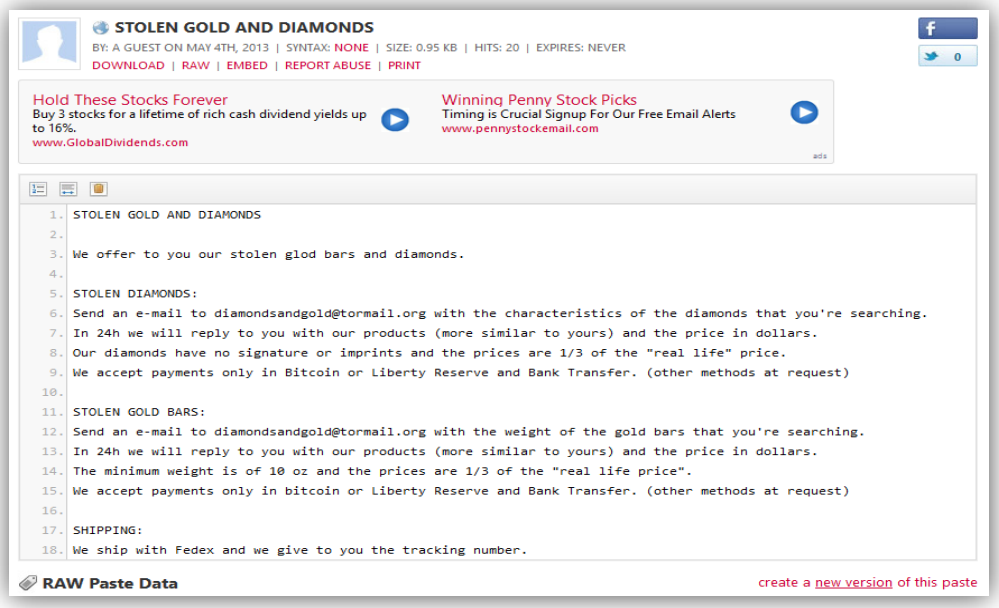
Figure 9: **Jewellery with diamonds offered for sale on "Silk Road"**



Source: Internet screen shot July 2013, Exchange Rate: 1 Bitcoin = 98 USD

There are sites that offer stolen gold and diamonds that can be pre-ordered according to customer preferences. The payment is made in Bitcoins or bank transfers and shipped by Fedex. Liberty reserve was also accepted. This illustrates one of the venues by which stolen diamonds are offered for sale and laundered using Bitcoins.

Figure 10: **Stolen gold and diamonds for sale**



Source: Internet screen shot July 2013

VULNERABILITIES RELATING TO ALL STAGES

Theft/Robbery – Theft or robberies of diamonds can occur at all stages of the trade. Since diamonds are of very high value, they are targeted by artisanal miners, employees of diamond companies, and criminals including criminal organisations. Several countries pointed to theft as being one of the most prevalent risks of the trade. This can be seen by the cases[109] submitted by team members and also by open source information on cases of theft or robbery of diamonds in values which can reach many tens of millions of US dollars.

Heists of diamonds have probably occurred in all times, but the value and volume of diamonds' heists in the last decade has developed in leaps and bounds. In the first half of 2013 alone two robberies of very high value took place in Brussels Airport[110] and in the French Riviera[111]. The theft of diamonds and jewels owned by Israeli billionaire Lev Leviev could be the largest jewellery heist in years, the worth of the stolen jewels was estimated at USD 136 million.

The recovery rate of stolen diamonds is usually very low. Open source cases show that stolen diamonds / jewellery are usually not found. Since diamonds are laundered in many cases through the trade, this is an indication of the ease with which very high -value diamonds can be laundered without a trace. Some cases showed that criminals used diamond dealers/jewellers to dispose of the illicit diamonds in their possession.

What is interesting here from a ML/TF perspective is that since the case is that, even for such extremely high amounts, the diamonds simply disappear then the same may be said with regard to ML/TF schemes through the diamond industry – the possibility today to trace such schemes where proceeds of crime are traded for diamond and then laundered through the trade is very low[112].

However, Australia noted that there is a misconception that theft is a key vulnerability at the jewellery manufacture and retail stage. While the jewellery retailers are often targets of theft, these robberies (generally 'smash and grab' jobs where quality jewellery is not necessarily targeted) account for only a small percentage of Australian thefts.

Australia also noted that theft in the diamond industry is more likely to occur in transit than at any of the six stages of the diamond pipeline. Diamonds in transit are particularly vulnerable to third party and opportunistic theft. Many diamond industry participants view transit as their largest risk.

According to the WFDB, most of the kimberlitic mining process of the mining stage is mechanised and is laser sorted. This has reduced considerably the risk of theft from kimberlitic mines. There are indications that in general, the frequency of theft has gone down significantly.

Smuggling - Despite controls put in place by authorities and mining companies, the smuggling of diamonds remains a problem. According to the information collected by the project team, it is

109 See for example case no. 8 and case no. 16.

110 See CNN (2013).

111 See Jewish Daily Forward (2013).

112 Dina Siegel looks at the largest robberies of the 21st century in which diamonds worth many tens of millions of euros where stolen and never recovered. She provides six different ways in which the diamonds could have been laundered. See Siegel Dina (2009), *pp*. 173 - 178.

difficult to ascertain the extent of the smuggling and that of the illicit market in illegally-obtained diamonds. South Africa has indicated that once the smuggled stones have entered or left a country, they are virtually impossible to trace.

Instances of smuggling were noted in the contributions of Australia, Canada, Israel, Namibia, Netherland, Sierra Leone, South Africa, Russia and USA. The cases in the United States concerned smuggling of uncut rough stones on the body of couriers, via commercial flights. The operations were linked to a "ML organisation". The organisation provided contact points for a broker and facilitated the payments for the smuggled stones. There were indications that the stones originated from conflict areas or that they were illegally obtained. The insertion of such smuggled stones into the legitimate market is accomplished by the "ML organisation", in cooperation with local dealers and through trade shows.

Nearly all rough diamonds found in the world today are controlled by a relatively small number of governments and private mine owners and conglomerates. There are some smugglers who pilfer from the concessions of those who control the rough diamonds from both government and private mines. Another country indicated that diamond smuggling is usually perpetrated by the employees of those companies.

The larger the extent of smuggling of diamonds, the easier it is for criminals to use smuggling for ML/TF purposes, *i.e.,* buying illegal diamonds with cash, smuggling the diamonds to a different jurisdiction and inserting them into the legitimate trade with almost no possibility for the diamonds to be traced. South Africa noted that there have been cases where criminals have been found trying to smuggle diamonds into/out of the country, especially through the airport, most of these destined for Europe.

In 2007[113], an assessment by an independent diamond expert provided information on several countries where smuggling took place:

- It is stated that with regard to Brazil that most of the diamonds mined in the country are smuggled out. Locals estimate that production may reach **USD 550 million annually** where formal production is several million USD;
- With regard to Central African Republic it is argued that the total export from Central African Republic is reportedly at least twice the official export data.
- A large part of the production in Sierra Leone is smuggled through Guinea, Liberia and other countries[114].

Commingling - Once diamonds are stolen, whether rough or polished, loose or mounted diamonds, in most cases, the offender will have to reinsert them into the legitimate trade in order to receive a pay-off. The same is true for illegally mined diamonds, which, in many cases, will be reinserted into the trade through another diamond mine. Thus commingling of diamonds is actually part of the ML/TF process and every stage of the "diamond pipeline" is vulnerable to commingling.

113. Even- Zohar, C. (2007).

114 *Ibid*, *pp*. 125, 197, 234.

South Africa identified a risk whereby small-scale operators may be tempted to buy illegal diamonds from other countries and try to pass them as legally mined diamonds. This in fact is an example of commingling through the mining sector.

TRADE FINANCING VULNERABILITIES

Use of cash - In order to better understand the extent of cash use in the trade of diamonds, it must be divided into two categories: wholesale and retail.

In general terms, the trade of diamonds through wholesale or other large dealers and brokers is **becoming less dependent on cash transactions, with wire transfers becoming the preferred method of payment**. While an overall decrease in the use of cash was reported, including in cash-based economies, by financial institutions and by team members, it is difficult to assess whether the level of risk generated by the use of cash being used remain significant. Analysis of the cases provided by team members show numerous cases involving cash transactions, including some cases where by cash proceeds of crime are placed, as part of a laundering scheme, in the diamond industry by means of buying diamonds with cash or depositing cash into diamond dealers accounts. Thus, it is possible to infer that even though cash is diminishing, cash usage still poses a risk for ML/TF in the diamond trade.

There are risks involved with the use of cash in large-scale transactions. A number of African or Latin American countries, some of them being diamond producers, still have a cash based economy. This makes cash the main payment method to conclude business with such countries. There are cases in which these transactions lack documental support, thus making them a very attractive means for ML and financing of terrorism. Moreover, as reported by one of the countries, depending on the local regulations, companies or individuals are able to conduct business in cash with foreign diamond bourses or fairs without the requirement for them to file a corresponding report. Therefore, we can conclude that, while most countries agree that the use of cash for large scale business to business (B2B) is being used less frequently, there are still transactions concluded this way that create a vulnerability within the AML/CFT regime.

At the retail level, transactions are typically smaller (when compared to the acquisition of bulk diamonds), and they can be conducted using cash more easily. Smaller diamond dealers, retail shops and even pawn shops can sell finished pieces of jewellery or even separate diamonds with cash as the payment method. Trends point to a decrease in the use of cash, mainly due to the introduction in some countries of legislation restricting the use of cash to purchase high value goods, such as jewellery and diamonds. However, not all countries have retail outlets or pawn shops among their catalogue of reporting entities, which means that transaction reports may not be received for sales of diamonds in all cases.

Uses of "IOUs" or promissory notes - promissory notes are used to cover debts related to the trade of diamonds (especially in bulk) by miners, dealers, brokers, cutters and polishers. They are negotiable instruments – as opposed to IOUs, which are non-negotiable instruments – and can be treated in the same way as cash (i.e. transferrable to a third party). The free and unrecorded circulation of these mostly honoured IOUs creates an unofficial and unmonitored "banking system", that provides financing for traders, outside the official banking system. Furthermore, in most

circumstances, the circulation of the promissory notes is totally "in house" within the "guild" of diamonds. The actual financial risk of a diamond dealer is "under the radar" of the official banking creditors and regulators.

The unrecorded circulation of IOUs facilitates the transfer of high value assets, without a trace in the monitored financial system. Thus, it is possible to cause the transfer of large scale funds, just by word of mouth among two persons who are members of Diamonds exchanges in different and remote locations.

The vulnerability of these cash like mechanism lays also in that it is possible to pay for the purchase of diamonds with an IOU, even with a 3rd party IOU, with no AML/CFT duties applying since only cash transactions fall under the standard and the AML/CFT legislation in most countries. This means that through the use of an IOU it is possible to avoid KYC procedures and reporting to the FIU with no audit trail of the transaction. While cross-referencing of these negotiable instruments may be useful, it is uncertain whether or not this is common practice for notes exchanged for diamond trade. Participant countries sent limited information regarding this issue, so further research is **recommended** to better assess the extent of the use of IOUs between diamond dealers and the risks entailed by such practice.

Use of diamonds as a collateral currency - Diamonds are an attractive alternative for criminals and terrorists to transport and transfer value physically, as diamonds are relatively small in size and are high value goods. The latter has also made diamonds a feasible alternative to currency, which is used in some countries by criminal or terrorist groups to buy supplies, drugs, weapons, or pay for drug-trafficking related debts.

This is relevant considering that diamonds could be **stolen** pieces, "conflict diamonds" or diamonds used to pay for drugs or weapons. Forged Kimberley Certificates can allow them to pass as recently and legally extracted stones, those bought as investments or as used diamonds removed from pieces of jewellery.

This is particularly important to financial institution providing loans against diamonds as collateral. Without the ability to verify the source of diamonds either for rough diamonds where a KP certificate is available or for loose polished diamonds where there is no certificate, there is a risk of such loans being part of a ML/TF scheme.

Memo transactions – As mentioned, memo transactions may bear some vulnerability to misuse in terms of ML/TF. These vulnerabilities are linked to possible variation of the prices of the diamonds evaluated, over or undervalued, and to the possibility of fraud committed by the consignee. For example, a potential buyer may review a parcel of diamonds and select some of the stones while returning the unsold diamonds to the consignor. The original shipment may occur at a certain stated value while the unsold return is made at another value (potentially over or undervalued). This flexible gap of value is common and may not be considered unusual or suspicious by the financial institution. But, it may also be used for ML purposes. The difference in price also raises the question whether the stones returned were all included in the shipment in the beginning. It has to be noted that the percentage of returns of polished diamonds is high. Consignment transactions may be considered by some countries to be high-risk deals with stricter rules for financing by the banks. In certain cases that involve familiar and reliable diamond dealer account holders, some banks do transfer funds or accept funds as advance payment without any document agreement

(save for a statement by the diamond dealer account holder), and then monitor the advance payment. The bank may be limited in the ability to verify that the financial transactions correspond to the terms of the memo and the value of the diamonds. The other risk linked to memo transactions is the possibility for fraud, when the consignee does not return the diamonds consigned.

"Advance payment" – some of the accepted **financial** practices by diamond dealers may also serve as conduit to ML or TF. For one, it is an accepted practice to transfer funds as an advanced payment for the stones. These are payments conducted without sending the precious stones. In many cases the advanced payment is returned back to the customer/diamond dealer. These transactions may be used to send back money from a 3rd party.

"Return shipments" – another accepted practice which create a ML/TF vulnerability is the return of shipments (partial or hole). In transaction such as memo transactions, stones are sent to the customer for his review and in case the customer is not satisfied with the stones he will send some or all the stones back to the diamond dealer. This in many cases would be accompanied with a return of funds already paid. Banks financing the trade should be aware that the funds should be returned from the same party to which the funds were initially transferred to and also with the same value. This may also be relevant to the diamond dealer where his customer is asking to transfer or transferring such funds to a third party.

"Fork Transactions" – in general these are transactions where funds are sent/received to/from other parties then those appearing in the documents as customer/supplier. As illustrated later, several cases illustrate such transactions conducted via diamond dealers' accounts.

Date of sale vs. date of payment – while conducting a transaction, the diamond dealer and its customer (which may also be a diamond dealer) will negotiate the terms of the deal including terms of payment. In most cases the diamonds will be provided close to the date of the sale and before the payment is received. The date of payment may be upon delivery of the diamonds but may also be several month later.

According to Recommendation 22 of the FATF (customer due diligence for DNFBPs) CDD measures apply for Dealers in precious metals and dealers in precious stones: "*when they engage in any **cash** transaction with a customer equal to or above the applicable designated threshold*".

The same applies to Recommendation 23 with regard to reporting duties of DNFBPs which states that dealers in precious metals and dealers in precious stones "*should be required to report suspicious transactions when they engage in any **cash** transaction with a customer equal to or above the applicable designated threshold*"

In many cases, the form of payment will determine the AML/CFT duties, it may be the case that the KYC and reporting duties will be conducted long after transaction took place and the diamonds have been delivered to the customer. Since, diamonds are a form of currency and may be used themselves for ML/TF purposes, this creates a vulnerability in which the ML/TF process may have taken place long before the details of the customer were verified and a report was sent to the relevant FIU.

Deficiencies in KYC / CDD procedures - In a number countries, diamond dealers and brokers are not accustomed to performing KYC or CDD procedures, as the industry is fairly closed to a limited

number of persons, involved in the business even for generations, who generally know each other. According to industry sources, it is difficult for a new and unknown individual to get involved in the trade of diamonds without being referred or introduced by an already established dealer[115]. In these cases, identification and cross-referencing of information may be used, however it is not mandatory.

The procedures to identify customers that purchase diamonds at the retail level are not the same in every jurisdiction, mainly because some countries do not consider dealers in diamonds, jewellers or retail outlets, including pawn shops, as reporting entities. Depending on the jurisdiction, sales outlets or even large-scale, wholesale transactions may be subject to reporting duties for large cash transactions or suspicious transactions.

The main difficulties to perform due diligence on customers arise from the international nature of the trade. The risk of these transactions is further increased when at least one of the parties conducts business through brokers, in which case the seller and buyer may not know each other. The trade of diamonds through the internet has become both a feasible and lucrative activity. However, the online trade in diamonds lacks sufficient – or, in some cases, any – procedures to identify customers and perform due diligence on potential buyers or sellers. This provides a level of anonymity that makes this market attractive for trade of diamonds with the purpose of concealing the illicit origin of resources or financing terrorist activities. KYC will be challenging to the banking institution receiving the payment from the buyer, since if the diamond dealer selling the diamonds does not fully know who his customer is then this is even more so for his bank.

One jurisdiction identified the lack of a central and up -to -date database with information on all registered individuals and legal entities dealing with diamonds – mining, exporting, importing, cutting, polishing or sales – worldwide as a deficiency on implementing KYC measures. This can prove helpful for assessing B2B transactions, but would still have little effect on retail level transactions, which have been linked by most countries to most risks.

The WFDB indicated that someone who is not a diamond bourse member cannot walk in to another diamond bourse and trade with the local members. It is required to present a letter from the bourse where he is a member, to the bourse where he intends to trade.

Screening of transactions - Reporting duties of transactions involving diamonds and other precious stones are, for most countries, in line with reporting duties established for other activities and businesses, both financial and non-financial, with the requirement to file reports before the relevant authorities when said transaction is above the established threshold or the characteristics of the transaction could raise suspicion.

Countries have recognised that information regarding the common practice involving transactions at various market levels is far from sufficient. Also, one of the countries reported that banks usually have limited ability to confirm that the parties to a transaction are, in fact, involved in the formal production and trade of diamonds. This may be one of the explanations for the low level of reporting as evident from statistics provided by team members.

115 This is sometimes required by law. In the consultation with the WFDB it was said that this is a requirement from all bourses of the WFDB.

CHAPTER 7.
RED FLAGS AND INDICATORS OF ML/TF[116]

There are many avenues in which diamond and jewellery may be bought:

- trade centres and diamond bourses;
- precious stones fairs in HK, Thailand, Switzerland and USA;
- Tenders;
- Sights;
- internet platforms;
- jewellers/jewelleries;
- Pawn shops.

Each stage of the trade may have its own red flags and indicators on top of red flags and indicators which are general and apply to all stages of the trade.

The 2008 FATF RBA guidance paper for dealers in precious metals and stones lays the foundation for an analysis of the risks which dealers in precious metals and stones, among other relevant players, are facing while conducting their business and provides the "*criteria to assess potential money laundering and terrorist financing risks*[117]". These criteria are reflected in some of the indicators below and may assist relevant players to identify specific possible ML/TF activity.

The following indicators have been identified from an analysis of the responses and cases collected by the project team. The existence of a single indicator does not necessarily indicate illicit activity, but should encourage further monitoring and examination. In most cases, it is the existence of multiple indicators which raises suspicion of potential criminal activity. These red flags and indicators may also assist in performing more general ML/TF risk-analysis in the diamond industry.

At the onset a clear distinction should be made between two different categories of red flags:

- red flags to **financial institutions**, mainly to banking corporations, referring to financial transactions carried out by entities involved in the diamond trade; and
- red flags or indicators referring to the **entities involved in the trade of diamonds** being one sector of the DNFBPs.

The first category of indicators is much more familiar and covers many indicators which would perhaps be relevant to other types of financial activities. The second category, the trade in a

116 The following member countries provided direct responses to the Collection Plan topic on red flags/indicators – Australia, Canada, Israel, The Netherlands and the United States. The red flags and indicators provided by the Netherlands were derived from Customs related case studies. There applicability is limited to import and export situations.

117 FATF (2008a).

commodity, is somewhat different and requires knowledge of the regular patterns and characteristics of the diamond trade throughout the "diamond pipeline". This second category is targeted more to diamond dealers themselves.

Further analysis of member responses identified four categories of indicators.

a) Red flags and indicators for regulated entities

b) Indicators related to the trade in diamonds

c) Indicators for the diamond industry at each stage of trade

d) Indicators specific to customs cases involving the import/export of diamonds

All categories have been included to provide the Egmont/FATF Project Team with a strong foundation to inform this chapter of the report.

Some member responses related specifically to one or some the above categories. Where possible the stage of trade is highlighted in brackets at the end of the indicator. For example:

- Israel provided indicators which are related to the trade in diamonds (category 2 above)
- The Netherlands provided customs cases from which indicators were drawn.
- Canada reported that it provides guidance to dealers in the precious metals and stones sector. This guidance includes red flags for possible suspicious transactions. Canada also reported that many indicators from diamond-related ML/TF cases were generally consistent with common ML indicators. Canada also identified red flags specific to the diamond industry at each stage of the trade.

It is also important to emphasize that while some general indicators have been identified, they are only partial and are not a replacement of general ML/TF red flags and indicators for reporting bodies.

Important remark: for the purpose of this section *only* the term Diamond Dealer will refer to all actors along the different parts of the trade from the mining sector to through dealers in rough or polished diamonds to jewellery retailers and pawn shops (unless the stage of the trade is specifically indicated).

RED FLAGS AND INDICATORS FOR REGULATED ENTITIES

The following indicators may assist regulated entities to identify potential ML/TF activity through the trade in diamonds and diamond jewellery. In most cases, these are general indictors serving to identify ML/TF activity of customers which are diamond dealers conducting their business in other

sectors than the trade in diamonds[118]. In some cases these are specific indicators relating to the trade in diamonds or diamond jewellery.

Red flags and indicators relating to trade practices

- Profit is unlikely with respect to the investment of a diamond dealer.
- Diamonds originate from a country where there is limited production or no diamond mines at all.
- Trade in large volumes conducted with countries which are not part of the "diamond pipeline".
- An increase of the volume of the activity in a diamond dealer's account despite a significant decrease in the industry-wide volume.
- Selling or buying diamonds between two local companies through an intermediary located abroad (lack of business justification. uncertainty as to actual passage of goods between the companies).
- Volume of purchases and/or imports that grossly exceed the expected sales amount
- Sale of gold bars, coins, and loose diamonds from a jewellery store (retail).
- Payments related to the appearance of rare or unique diamonds in the international market outside of known trading procedures (e.g. Argyle's rare pink diamond appearing in the international marketplace outside of the annual tender process). This to the best knowledge of the financial institution.
- A single bank account is used by multiple businesses.

Red flags and indicators related to transactions/financing of diamond trade

- Unusual *forms of payment* in the diamond trade, for example, use of travellers cheques (all stages according to the accepted forms of payments).
- *Date of payment* not customary in the trade, (e.g. receiving/sending funds for a diamond deal conducted a very long time ago (outside accepted payment terms). Or, a customer paying upfront where the customary payment date is within a 120 days term.
- *Financial activity* is inconsistent with practices in the diamond trade. For example,

118 This is not an exhaustive list. Red flags related to financial activity in general (e.g., structuring of transactions below the reporting threshold, transactions in high risk areas, etc.) are also applicable to the activity of diamond dealers.

  - Foreign currency deposits followed by currency conversion and cash withdrawal in local currency.
  - Cheque deposits followed by immediate cash withdrawals in slightly lower amounts (possible use of the diamond dealer account for cheques discounting).
  - Transfers of foreign currency and/or foreign currency cheques deposits, followed by currency conversion and immediate withdrawal from the account (possible use of the diamond dealer account for exchange services).
- No economic rationale for transactions involving an individual or company in the diamond industry.
- Deposits immediately followed by withdrawals, atypical of practices in the diamond trade, including but not limited to:
  - Circular transaction related to import/export of diamonds.
  - Circular transactions related to local trade (between local bank accounts).
  - Circular financial transactions between a diamond company's account and the private account of the company's shareholder/director, without business or economic reason.
  - High turnover of funds through an account with a low end of day balance.
- Deposits or transfers to a diamond dealer's account from foreign companies followed by immediate transfer of similar amounts to another jurisdiction.
- Immediately after a diamond dealer's related account is opened, high-volume and high-value account activity is observed.
- Transactions between accounts of different companies which are affiliated with the same customer, particularly to or from Free Trade Zones or countries with tax leniencies [119] (may be an indication of transfer pricing or trade mispricing).
- Open export[120] is settled by offsetting to, and receiving payment from, a third party.
- Open export is settled abroad by offset in front of the importer.
- Settling an open export invoice with unrelated companies that engage in diamonds and not through value/return from abroad or return of goods to the diamond merchant.

119 These transactions should be closely monitored since they may facilitate ML/TF activity and tax evasion through transfer pricing.

120 An export of diamonds where a payment was not yet received and the sale was not cancelled.

- Details of the transaction are different from the details of the commercial invoice presented by the diamond dealer to the bank (name of importer/exporter, sum, place etc.)[121].
- High-value funds deposited or transferred to an account described as short term loans with no transactions showing repayment of loans.
- Early repayment of diamond dealer's loan (a loan for 25 years is repaid after five month) with no reasonable explanation.
- Sale of diamonds and jewellery at small incremental amounts (retail).
- Multiple cheques drawn on the same diamond dealer's account on the same day.
- Origin/destination of funds is different from the destination/origin of the diamonds.
- Diamond dealer account is credited by transactions with no evidence of diamonds sales.
- Numerous returns of advanced payments.

Customer-related red flags and indicators

- Activity does not match KYC, for example:
  - Actual trade volumes are significantly larger than the expected volume.
  - Customers and/or suppliers of the customer do not correspond to the stage of the trade initially declared.
- Diamond dealer is not familiar with trade practices.
- Diamond dealer maintains high level of secrecy.
- Diamond dealer conducting activity in a branch not specializing in diamonds (where such branches exist).
- Use of a bank account in the name of a *charity*[122] to transfer funds to/from diamond dealers.
- Frequent changes in company name and contact person for a business in the diamond industry (mainly wholesale).

121 This may indicate a false/fictitious invoice which might constitute a predicate offence.

122 In the particular case provided by Australia from which the indicator was derived the charity was not a registered charity, company and/or business name. This is an additional general indication not related to trade in diamonds.

Red flags and indicators related to the use of third parties

- Customer consults a third party while conducting transactions.
- Receiving/transferring funds for import/export activity to/from entities that are not known to be involved in the diamonds trade (either an individual or a legal entity).
- Return of an advanced payment from a third party.
- Receiving/transferring funds for import/export where the ordering customer/beneficiary is an MSB.
- Use of third parties to deposit funds into single or multiple diamond dealers' accounts.
- Return of an advanced payment from a third party.
- Name of sender in the payment transfer to the diamond dealer is not the importer/buyer (mainly rough and polished trade).
- Name of receiver in the payment from the diamond dealer is not the exporter/supplier.
- A single bank account with multiple deposit handlers (retail and wholesale).

Red flags and indicators relating to the use of missing/suspicious/falsified documents

- KP certificate is or seems to be forged.
- Long validity of a KP certificate[123].
- Transfers of funds or an attempt to transfer funds through a diamond company's account without producing appropriate documentation.
- Diamond dealer claims funds received/transferred are an advanced payment without producing any appropriate export/import invoice to support it.
- Transfers between a diamond company and a private account that are reported to the bank as diamond transactions, without presenting appropriate documentation.
- Invoice presented by the diamond dealer appears to the bank as unreliable/fake.

[123] The Kimberley Certificate has a maximum two month-validity: KP certificates have a maximum validity of two months following their issuance. A "good for one entry-only" policy, a unique serial certificate number, and by the mandatory "import confirmation" from the importing KP Authority to the KP Export Authority of the exporting KP is intended to create a closed loop.

- Failing to provide a customs declaration in relation to a foreign currency cash deposit resulting from selling precious stones abroad.

RED FLAGS AND INDICATORS FOR DIAMOND DEALERS

For each of the following red flags and indicators, the relevant level of trade is indicated in brackets.

Customer or supplier related red flags and indicators

- Purchases or sales which are unusual for customer or supplier (all stages of the trade).
- From what the diamond dealer knows about the customer or supplier, the transaction appears to him to be illogical from a business or economic point of view (all stages of the trade).
- Customer or supplier does not hold a position within a company they claim to represent (all stages of the trade).
- Customer or supplier is not familiar with trade practices (all stages of the trade).
- Customer or supplier maintains high level of secrecy (all stages of the trade).
- Customer or supplier known for their *involvement in trafficking conflict diamonds* (mainly rough trade. Could apply to diamond dealer who is involved in both rough trade and polished trade)
- Customer indiscriminately purchases merchandise without regard for value/price, size or colour (all stages of the trade).
- Sale of illicit goods from a jewellery store, such as counterfeit jewellery (retail and wholesale).
- Sale of gold bars, coins, and loose diamonds from a jewellery store (retail).

Red flags related to the sale or purchase of diamonds (transaction)

- Purchases or sales that are not in conformity with standard industry practice (all stages of the trade).
- Origin/destination of funds differs from the destination/origin of the diamonds (mainly rough trade and polished trade).
- Diamonds are not accompanied by a valid KP certificate[124].

[124] Every shipment of rough diamonds at import and export needs to be accompanied by a valid and validated KP Certificate. For transactions of rough diamonds within the jurisdiction of the same KP country no KP certificate is required, but the commercial invoice must contain the WDC system warranties declaring the shipment to be conflict free. This allows the overseeing authority of the KP country to follow the transactions from import to re-export.

- Diamond cutters receiving unwashed and uncut diamonds where the source of the diamonds is unknown or questionable (rough trade).
- The appearance of rare diamonds in the international market outside of known trading procedures (e.g., Argyle's rare pink diamond appearing in the international marketplace outside of the annual tender process. (rough trade, cutting and polishing).
- Selling or buying diamonds between two local companies through an intermediary located abroad (lack of business justification. uncertainty as to actual passage of goods between the companies).
- Purchase of diamonds with a credit card issued in a country which is not the buyer's country (where credit cards are used, mainly retail).
- Regular interval purchases, rather than seasonal purchases from foreign wholesaler (retail especially, less so with diamond dealers and wholesalers).
- Buying of diamonds or jewellery and reselling even at wholesale price (retail).
- Customer is known to purchase of diamonds off the street (retail).

Red flags and indicators related to the use of third parties

- Use of third parties to sell diamonds jewellery where this is not acceptable in terms of trade practices (all stages).
- Use of third parties including relatives to conduct transactions/receive payments where this is not acceptable in terms of trade practices (all stages).
- Customer or supplier consults a third party while conducting transactions (all stages of the trade).
- Purchase of diamond or jewellery from a company abroad (funds are sent to the selling company) and receiving the diamonds from a third company (rough trade, polished trade, jewellery).

Red flags and indicators relating to the use of suspected/falsified documents

- KP certificate is or seems to be forged.
- Long validity of a KP certificate

Red flags and indicators relating to the method of payment

- High-value cash purchases of diamonds particularly in non-cash jurisdiction and/or non-cash stage of trade (all stages and depending on jurisdiction).

- A customer paying for high-priced jewellery with cash only (mainly retail).
- Unusual *means of payment* in the diamond trade, for example, use of traveller's cheques, cashier's cheques or money orders. Higher risk where they are sequentially numbered (all stages of the trade).
- Customer or supplier appears to be indifferent to the *date of payment* (all stages of the trade).
- Paying for diamonds with cheque and noting on the cheque the payment is for something else (retail and wholesale).
- Customer attempt to use a third party cheque or a third party credit card.

Red flags and indicators related to geographic location/country

- The customer or supplier appears to be related to a *high-risk jurisdiction* (all stages of the trade).

RED FLAGS AND INDICATORS FOR CUSTOMS

The Netherlands provided customs-related case studies. These cases yielded indicators related to the import and export of diamonds. The following indicators were used to detect the cases highlighted in the Netherlands' response.

Red flags related to export/import (documentation and entities involved)

- Origin of diamonds seems to be fictitious.
- The long validity period of the KP Certificate opens up possibilities for reuse and setting up a carousel[125].
- Low invoice amount.
- Overvaluation of imported good.
- The consignee doesn't specify a permanent address on the airway bill but makes use of a hotel, or other temporary accommodation, to receive the shipment, complicating the audit trail.
- The consignee specified on the airway bill is a known diamond dealer, but a different delivery address is provided.
- The diamond appears to have been shipped as a form of payment.

[125] For countries participating in the Kimberley Process Certification Scheme, international shipments of rough diamonds must be accompanied by a Kimberley Process certificate to guarantee that they are conflict-free. See Kimberly Process (n.c).

CHAPTER 8.
MONEY LAUNDERING SANITISED CASES THROUGH TRADE IN DIAMONDS[126]

Methodological remarks - This section of the report looks at case studies which illustrate the ML/TF methods and techniques which are used in the diamond industry throughout its various stages. All the cases were provided by countries that completed the collection plan[127] or through open source analysis. The case studies included in this chapter are real cases but in most instances the real names have been omitted. For the purpose of this analysis, clear distinction should be made between two methods of ML/TF through the trade in diamonds which were already outlined in the short overview of the international diamond trade provided in the beginning of this report.

- The first method is the conduct of ML through the use of diamonds as vehicles of intrinsic high value which may often be the proceeds of crime in cases of theft or robbery.
- The second method is the abuse of the financial trade in diamonds to launder illegally gained funds generated from other predicate offences such as drug trafficking and fraud.

Other precious stones - even though the project team decided to exclude other precious stones from the scope of this report, team members provided several cases where precious stones other than diamonds were used in money laundering schemes. This information has been provided in this report to emphasize the ML/TF vulnerability and risk that concerns precious stones and to highlight the importance of AML/CFT counter measures required to mitigate such risks. These cases also point to the need to conduct further research on the use of other precious stones for ML/TF purposes.

ML methods and techniques - The analysis of the cases collected identified seven ML method. Each method may be carried out through different techniques. Many cases entail the use of more than one method or technique of ML. The methods identified are:

a) Use of diamonds as currency.

b) Acquisition of diamonds with proceeds of crime as a means to store wealth.

c) Laundering through stages of the diamonds trade (either ML of proceeds generated via offences not related to the diamond trade or laundering the proceeds of diamonds related crime such as theft or robbery of diamonds).

d) TBML and customs infractions.

e) Use of financial hubs and FTZs.

126 FIU sanitized cases, Law enforcement, open source cases / investigation.

127 Including the limited collection plan.

f) Smuggling of diamonds and cash.

g) Link with or use of gold and/or other precious stones trade.

The methods identified above correspond to a large extent to the vulnerabilities identified in the previous section dealing with the vulnerabilities of the diamonds trade. The previous discussion of the diamonds trade identified certain vulnerabilities, based on the unique characteristics of diamonds:

- the possibility to use the diamonds as currency and as a mean to store wealth,
- the different vulnerabilities entailed in each stage of the trade from mining to retail level,
- the vulnerability to large scale TBML (e.g. via under or over valuation),
- and a vulnerability to smuggling resulting from these characteristics.

These cases show that criminals and professional money launderers take advantage of the identified vulnerabilities.

The analysis show that the ML/TF methods are closely related to the nature of the diamond trade conducted within specific jurisdictions or to the stage of the "pipeline" each case is referring to. Thus, for example, Belgium and Israel have significant cases relating to diamond dealers and diamond trading companies, whereas the US identified as a retail market show more laundering through jewellers. Several intelligence gaps still remain due to the lack of cases from several African mining counties and financial hubs such as the United Arab Emirates. This raises questions about the actual AML/CFT investigations in the sector.

Case structure – since the project is dealing with a trade-related DNFBP, the project team found it important to indicate for each case, where information was available, the characteristics of the trade and the financial activity related to the trade. For each case, the associated predicate offences were specified and also the ML stage (*placement*, *layering* or *integration*). Since the cases show very large scale ML activity, the sum involved in the case was also specified. Finally, the source of information (country contribution, open source or both) was also indicated.

General remarks –

a) **Large scale ML** - many cases show very large scale predicate offences or ML activity conducted through the diamond trade. One of the vulnerabilities identified was the ability to launder large sums of money, since the transaction performed in the various stages of the trade may amount to tens of millions of USD. These cases provide an indication that this vulnerability is used in ML schemes.

b) **Common predicate offences** – the most common predicate offences identified in these cases are smuggling and tax offences, including large scale tax fraud. Tax fraud, particularly when conducted through financial hubs and trade centers such as Dubai, Switzerland, Belgium and Israel, are an indication of the use of transfer prices for the purpose of avoiding tax regimes.

c) **Third party transactions** – one important issue which surfaced from different countries is an extensive use of the diamonds trade to transfer funds to or from entities which are not related to the diamond industry.

METHOD 1: USE OF DIAMONDS AS CURRENCY

In at least 15 cases that were provided by the countries, diamonds were used as an alternate currency. As indicated previously, criminals will often purchase diamonds as a means of laundering proceeds of crime and then sell the diamonds to obtain cash at a later date or a different location. In this case, ML is engaged in to purchase the diamonds and then the diamonds are sold to recover cash. This amounts to laundering of the proceeds of crime.

Diamonds bear features which enable their use as a form of currency. This is demonstrated perfectly by the use of diamonds to finance armed conflicts. These features of diamonds bring criminals to use diamonds in a similar way while conducting other offences. Several cases from team members and open source information show that such use of diamonds is mainly prevalent with drug traffickers in different countries around the world. The use of diamonds as currency was also discussed during the workshop held in Dakar, where it was pointed out that in South African diamonds are used as a payment means by criminal syndicates, for example as payment to rhino poachers. Cases also show that diamonds are smuggled between countries along with drugs or other commodities, probably as payment between parties.

This form of payment, just as cash payments, is untraceable and allows criminals to avoid the use of financial institutions while conducting their criminal activity thus avoiding rigorous KYC procedures put forth by banking institutions where diamond dealer's accounts are managed. This provides the criminal with security that suspicious activity reports would not be filed to the FIU. The use of diamonds as currency, and the fact that the trade in diamonds is international, opens up options for the criminal or money launderer such as smuggling the diamonds to other countries and exchanging them for other forms of payment such as cash or cheque, or laundering them through much less regulated diamond dealers locally or abroad.

TECHNIQUE: DRUGS TRAFFICKING RELATED USE OF DIAMONDS AS CURRENCY

The most noted predicate offence related to the use of diamonds as a currency is drug trafficking[128]. Canada, Australia, the United Kingdom and the United States provided cases for such use. Drug traffickers/producers use these commodities for a number of reasons in support of their criminal enterprise. The drug business generates huge amounts of cash which is a well-known fact by reporting entities and law enforcement. It isn't surprising that criminal organisations that are involved in drug production and trafficking are looking for other ways of payment. Cases provided by team members have shown that diamond and jewellery are actually used by drug traffickers of different levels as a mean to finance the purchase and distribution of drugs.

128 See Annex 2 - predicate offences.

A sophisticated scheme provided by Canada illustrated the use of diamonds as a form of payment received by street-level drug dealers and the mode in which diamonds (including jewellery) are used to finance this criminal activity throughout the drug distribution/production chain. Additional cases showed drug traffickers apprehended with drugs, cash, diamonds and jewellery in their possession and changing proceeds of crime to diamonds and jewellery, smuggling them to other countries where they are laundered through local diamonds trade industry.

Case 1: ***Financing drugs trafficking with diamonds and ML through retail level***	
This case involved an organised criminal group that distributed drugs and controlled several low level (street-level) drug dealers. The higher placed distributor would distribute drugs to the street-level dealer and receive *diamonds*, *gemstones* and *jewellery* as payment, as well as cash. Likewise, the street-level drug dealer traded drugs for diamond jewellery and then traded up to the higher placed drug dealer for more drugs and debt payments. The higher placed drug distributor would then sell the diamonds and jewellery at small incremental amounts (CAD 3 000-CAD 8 000) to the jewellery market (jewellers) and **in** return would receive payment by way of *cheque*. The drug distributor also received high end jewellery (watches) instead of payment for the illicit jewellery.	
Predicate offence/s	Drug trafficking
Stage of Trade	Retail
ML/TF Stage	Placement (precious stones proceeds of crime in jewellery market)
Money/Trade flow	-
Types of financial/trade activities	Sale of diamonds and jewellery for cheques
Sums involved	-
Red flag indicators	■ Link to organised crime ■ Sale of diamonds and jewellery at small incremental amounts ■ Frequent deposits of small denomination cheques drawn on jeweller(s) where this is not typical for the customer ■ Link with other precious stones
Source	Canada (response to collection plan, 2013)

Case 2: ***Link between use of diamonds and drug trafficking***	
In October 2011 officers from the Metropolitan Police Service's Central Task Force arrested Daniel McNeill-Duncan, Aaron Bowell, Karl King and James Bailey at Bailey's Neasden home. A drugs search found more than GBP 92 000 in cash, almost 2 kilos of cocaine (street value GBP 1m+). A search of King's home found large quantities of cocaine cutting agents Boric Acid, Phenacetin and Lignocaine, scales and a money counting machine. A search at Marlon Okeowo's address - Bailey's associate – found GBP 80 000 worth of *cut diamonds*. All pleaded guilty to conspiracy to supply cocaine. Sentenced on 24/04/12 : King (6 years, 9 months), Okeowo (7 years, 3 months), Bowell (6 years) Bailey (6 years), McNeill-Duncan (5 years).	
Predicate offence/s	Drug trafficking
Stage of Trade	Manufacturing/retail
ML/TF Stage	-
Money/Trade flow	-
Types of financial/trade activities	Diamonds as currency
Sums involved	GBP 80 000 in diamonds, GBP 92 000 in cash, GBP 1 000 000 (drugs)
Red flag indicators	-
Source	United Kingdom (response to limited collection plan, 2013)

METHOD 2: ACQUISITION OF DIAMONDS WITH PROCEEDS OF CRIME AS A MEAN TO STORE WEALTH

Prices of diamond are relatively stable and provide the security that the value invested in their purchase would not depreciate significantly over long periods of time. By changing proceeds of crime into diamonds and jewellery, criminals can:

i. conceal proceeds of crime over long periods of time and avoid seizure and confiscation,

ii. transfer very high value across borders while keeping their investment relatively safe,

iii. transfer very high value across borders without a need to declare carrying value as requires by FATF standards and local legislation with regard to bearer negotiable instruments (BNIs)[129],

iv. use as a form of payment after long periods of time, and

v. insure the value of the diamonds in case of loss or theft.

At any level of the trade, a purchase of a large sum worth of diamonds or jewellery by a customer, whether in cash or any other means of payment, may be an attempt by a criminal to place proceeds

[129] For the FATF definition of BNIs see FATF glossary at: www.fatf-gafi.org/pages/glossary/a-c/.

of crime into diamonds as a vehicle to store wealth, making the diamond trade a target for placement and layering of criminal proceeds.

TECHNIQUE: DIAMONDS BOUGHT AND KEPT FOR A PERIOD OF TIME AND SOLD UPON THE CRIMINAL'S REQUEST

Case 3: ***Placing diamonds bought with proceeds of crime in safes as a mean to store wealth***

An Austrian bank filed an STR saying that a Brazilian national conducted illogical transactions. He paid a large sum (profit from sale of real property) into an account for investment. He did not make any investment but wanted to transfer the "total amount" to the USA.

Austrian FIU conducted appropriate analyses and decided to initiate criminal police investigations. Austrian FIU filed report to the competent Public Prosecutor's Office and discussed further steps with the bank obliged to report. During his next visit at the bank, the above mentioned national was contacted; his statements only reinforced suspicion of ML; therefore, surveillance was initiated. Surveillance revealed extremely conspicuous behaviour; he went to a different bank (vault). Another report of facts of the case was filed to the Public Prosecutor's Office. Finally, a court order to open the bank safe was obtained. The content of the safe revealed further safe keys, which were also opened by Court order. Austrian FIU seized a large number of false passports and diamonds.

First analysis of documents seized sufficed for the issuance of an arrest warrant regarding the Brazilian national, and execution of the warrant. Interrogation revealed that he was laundering money for a large-scale fraudster from the United States. They transferred funds to accounts of offshore companies; fraudster handed funds to money launderer; he took over the funds and purchased diamonds at "jewellers". He handed these diamonds over to middlemen who smuggled the diamonds to Austria. They placed these (precious) diamonds in safes and as the fraudster needed most of the money, he ordered for the money to be wire transferred. The money launderer sold some of the diamonds and deposited the profit into above mentioned account.

Predicate offence/s	Fraud, Smuggling of diamonds, false passport
Stage of Trade	-
ML/TF Stage	Layering
Money/Trade flow	Austria to United States (money)
Types of financial/trade activities	Use of safes, Wire transfers
Sums involved	-
Red flag indicators	■ Frequent visits to a safe. ■ Visits to a safe followed with cash deposits and a request to transfer the funds abroad
Source	Austria (2012)

Case 4: ***Drug dealer Launders jewellery received as payment for drugs and buys jewellery as a mean to store wealth***	
This case involved a drug dealer/producer who sold drugs and traded drugs for collectively over USD1 million in stolen and purchased jewellery. The drug dealer who had strong industry, commodity and market knowledge sold the least valuable (scrap) jewellery as scrap to jewellery stores and bullion dealers. Jewellery that had some aesthetic or residual market value above the component parts was sold as estate jewellery to jewellers. In return, the drug dealer received cash, gold and silver bars and coins and diamond jewellery. The drug dealer used some of the proceeds of crime from the sale of drugs and sale of jewellery obtained through trade for drugs to purchase specific diamond jewellery and gemstones items (jade) as a mean to store wealth. The drug dealer used appraisals to define the value of jewellery that was stored as wealth and to help negotiate fair prices for the resale of the jewellery to the market.	
Predicate offence/s	Drug trafficking
Stage of Trade	Retail and wholesale
ML/TF Stage	Placement through jewellery
Money/Trade flow	-
Types of financial/trade activities	Jewellery sold for cash, Jewellery sold for gold and silver bars and coins, Jewellery sold for diamond jewellery and gemstones
Sums involved	CAD1 million
Red flag indicators	■ Frequent selling of jewellery ■ Jewellery traded for jewellery ■ Jewellery traded for gold and silver
Source	Canada (response to collection plan, 2013)

METHOD 3: LAUNDERING THROUGH STAGES OF THE DIAMOND TRADE

The "diamond pipeline" is very long and complex. Each level of the trade chain offers opportunities for those seeking to exploit the nature of the trade and the unique features of the commodity traded for the purpose of ML or TF. Cases collected show the use of all levels of the trade from mining companies, dealers in rough and loose polished diamonds through diamond wholesalers to retailers and pawn shops with little information regarding ML through the mining sector where an intelligence gap exist due to limited contributions from African mining countries.

A distinction, which was detailed in the overview section of the report, can also be seen in the cases. This distinction is between on the one hand:

a) ML conducted through the trade in diamonds where proceeds are generated by crimes not related to the diamond trade (e.g., drug trafficking).

And on the other hand:

b) Laundering diamonds or jewellery generated by crime (*i.e.,* theft, diamond used as payment for drugs, illegal mining) by "legitimising" these proceeds of crime through the trade.

Cases show a variety of techniques used by criminals to use different levels of the trade for ML purposes. Some techniques may be used in a similar way in different stage of the trade. An example of this may be the laundering of illegally mined rough diamonds by way of commingling through the mining sector or commingling through a rough diamond dealer. The following techniques were identified:

a) Commingling of illegally gained diamonds through the mining sector.

b) Laundering *illegally gained diamonds* through wholesale, retail jewelleries, pawnshops or trade shows.

c) Laundering *proceeds of crime* through wholesale or retail jewelleries – these cases were mostly presented by large retail markets such as the US and Canada where large sums of money would be more easily placed.

d) Using accounts of diamond dealers as a conduit to transfer funds, particularly in favour of *third parties* which are *not part of the diamond trade* – this type of ML activity was identified by several countries and is more common in trade centres such as India, Israel and Belgium. Canada and the US also identified this type of behaviour. FinCEN indicated in a SAR analysis performed by the FIU that the diamond industry entities interacted with charitable foundations, electronics manufacturers, automobile dealers, real estate businesses and unknown entities in unknown locations. Australia submitted a case where a charity interacted with diamond industry entities. This type of activity seems to be indicative of the industry in light of the pattern spanning across the globe. It seems large amounts of money are *transferred through* the diamond sector from *unrelated entities* with a purpose to hide the source of funds, the destination of funds or both.

e) Amounts involved are high, indicating that large amounts of money are funnelled through the industry in favour of undeclared entities.

Some of the cases feature more than one technique which may result from the change of the *modus operandi*. Some cases show large scale ML activity amounting to tens and even few hundreds of millions of USD. These cases are instances of what was previously portrayed as a vulnerability, namely that since the diamond trade amounts to almost USD300 billion per annum, characterised by very large transactions, it provide an opportunity to launder very large sums.

Trade Based Money Laundering and *Smuggling* are both prevalent in the diamond industry. Since these are methods not unique to trade in diamonds and since they are not particular to a specific stage of trade, they are dealt separately.

TECHNIQUE: COMMINGLING OF SMUGGLED DIAMOND AT THE MINING LEVEL

Case 5: *Attempt of commingling illegally mined diamonds via exporting companies*

In 2005, the Guyanese government caught an attempt by a company to export 8 500 carats of rough stones with allegedly illegal origins. Given the owner's Venezuelan connections, discovered by investigators, the stones were believed to have originated in Venezuela and laundered through the company for legal export out of Georgetown.

The Guyanese government investigated in 2007 another company over a 4 000-carat batch of diamonds with nefarious origins, presumably from Venezuela, Brazil, or even West Africa, according to government documents.

Predicate offence/s	Illegal diamond trade
Stage of Trade	Rough diamond trade
ML/TF Stage	Placement and layering
Money/Trade flow	Venezuela to Guyana (suspected illegal trade)
Types of financial/trade activities	Rough diamond export
Sums involved	-
Red flag indicators	■ Lack of KP certificate for rough diamonds or certificate seems to be forged
Source	Open source: Logan, Samuel (2009)

TECHNIQUE: LAUNDERING ROUGH DIAMONDS BY CUTTING AND POLISHING

This technique provides two main benefits to the money launderer: first, once a rough diamond is cut it is almost impossible to verify the source of the stones. Second, once a diamond is cut and polished it no longer falls under the KPCS and may be exported without the controls established by the Kimberley process.

Case 6: *Illegal diamonds sent to foreign jurisdiction to be cut and polished*

A case of non-Kimberley Process rough diamonds smuggled into Canada, then the diamonds were smuggled to a foreign jurisdiction to be cut and polished (as Canada has few independent diamond cutters) and then the diamonds were sent legally back to Canada as they were now cut and polished and no longer subject to Kimberley Process protocols (this case engaged the rough diamond production and diamond cutting sector of the industry).

Predicate offence/s	Smuggling diamonds
Stage of Trade	Rough diamond production, cutting and polishing
ML/TF Stage	Laundering illegal diamonds through cutting and polishing
Money/Trade flow	-

Case 6: *Illegal diamonds sent to foreign jurisdiction to be cut and polished*	
Types of financial/trade activities	Cutting and polishing
Sums involved	-
Red flag indicators	-
Source	Canada (response to collection plan, 2013)

TECHNIQUE: LAUNDERING ILLEGAL DIAMONDS THROUGH DIAMOND DEALERS

The following case concerns a technique which facilitates illegal trade in diamonds where diamonds are smuggled into Russia circumventing the KPCS. The illegal diamonds are laundered by the criminal establishing diamond companies for the purpose of selling the stones without a KP certificate.

Case 7: *Trafficking of illegal Gemstones*	
Mr. M, an Israeli national, sets up a company "M" in St. Petersburg specializing in an unauthorised distribution of precious stones (diamonds). According to the documents, precious stones are supplied by five companies that are registered in Russia and founded by the same Mr. M. According to intelligence provided by law enforcement, the said companies were set up to launder precious stones that are smuggled into Russia. Company "M" handled the smuggled stones without keeping any written records of transactions, with all deliveries being made on the basis of customers' requests. Deliveries of diamonds to the company office were made by couriers and involved no supporting documentation. The proceeds were channelled abroad in the form of interest-bearing loans to foreign companies with bank accounts in Israel and Hong Kong, China. A criminal investigation revealed that the said foreign companies owed Company "M" a total of over USD 2 million. However, a close study of STRs revealed that more than USD 8.9 million had been credited to the accounts of these companies. Yet, the total amount of Company M's debt to the suppliers of diamonds stands at more than 90 million rubles.	
Predicate offence/s	Smuggling diamonds
Stage of Trade	-
ML/TF Stage	Layering
Money/Trade flow	Israel (money Out); Hong Kong, China (money Out)
Types of financial/trade activities	Loans to foreign companies
Sums involved	USD 9 million

Case 7: *Trafficking of illegal Gemstones*	
Red flag indicators	■ Loans are provided by a diamond company to legal entities not in the diamonds industry ■ Loans provided by the diamond company are not repaid. ■ No supporting documentation to the international transactions conducted in the diamond company account
Source	Russia (response to collection plan, 2013)

TECHNIQUE: LAUNDERING ILLEGAL DIAMONDS VIA RETAIL LEVEL – JEWELLERIES, PAWN SHOPS

One of the risks identified by the team members was the risk of theft which is relevant for every stage of trade in all countries involved in diamonds trade. The jewellery market is prone for theft and is perhaps and broadly speaking the sector where the risk is the highest since in the mining sector and the trade centres control and supervision are more stringent. Retail jewellers are everywhere and constitute the largest sector of the trade in terms of entities involved and turnover per annum. These stolen items must be laundered through appropriate venues in what may be called laundering of illicit diamonds/jewellery as opposed to ML per se. The cases below present the techniques used to launder illegal diamonds or jewellery in the US.

Case 8: *Theft Case Example – Operation Cut and Run*

During January 2004, a handful of South American immigrants from New York City stole nearly USD 100 000 worth of Rolex watches from a jewellery store in Cranston, Rhode Island. They fled the scene in a minivan, with local police in hot pursuit. Minutes later, they slammed into a police cruiser. They jumped out of the van and fled on foot, but four were immediately caught and arrested.

This lead to massive investigation (Operation Cut and Run) by the FBI, the New York City Police Department, the Bureau of Immigration and Customs Enforcement (ICE)[130], the U.S. Attorney's Office in the Southern District of New York, the Queens County District Attorney's Office, and other law enforcement partners.

In the end, this multi-agency initiative uncovered and ultimately took down a criminal enterprise that had stolen more than USD 3 million worth of high-dollar pieces of jewellery across the eastern seaboard in more than 90 separate thefts. At least 16 members of the crew have been arrested or indicted, and one has pled guilty.

This case is considered by FBI to be a 'textbook" jewellery theft case. Mainly because the thefts were orchestrated by a signature international enterprise (*i.e.,* a SATG – South American Theft Group) that operated out of New York City, one of the common bases for jewellery theft rings. The ring was also sophisticated. For example, the thieves would enter jewellery stores in small groups, with some

130 Now Homeland Security Investigations (HSI).

Case 8: ***Theft Case Example – Operation Cut and Run***

members distracting sales and security personnel while others operated as lookouts. Once they determined it was safe to proceed, some of them would stand around a showcase to shield it from view while others used a tool to cut the silicone holding the case together and remove the goods. The group would then leave the scene and meet a waiting vehicle to escape.

The thefts in this case extended across state lines which brought in the FBI with its national and international network of agents. Like most other cases, "fences" (individuals who knowingly buys stolen property for later resale - see case 9 below) played a role in receiving and moving the stolen goods. The intelligence gained by law enforcement--including the modus operandi of the group and descriptions of suspects—was entered into a database. This information helps law enforcement partners nationwide coordinate any related investigations and better understand the jewellery and gem criminal enterprises operating in the United States.

Predicate offence/s	Theft
Stage of Trade	Retail
ML/TF Stage	-
Money/Trade flow	-
Types of financial/trade activities	-
Sums involved	USD 3 million
Red flag indicators	-
Source	United States (response to collection plan, 2013)

The case bellow illustrates the manner in which stolen diamonds are laundered in the United States.

Case 9: ***Trafficking in Stolen Goods***

Diamonds taken from large scale robberies, thefts and burglaries are sold to "second hand" dealers to include pawn shops, estate jewellery dealers and other high-end retail outlets. Diamonds are often targeted by highly professional groups noted above and other organised crime groups from the Balkans (e.g., former Yugoslavia, Albanian, and Kosovo). Picking up on the examples described above, professional theft crews can sell stolen goods to their fences for between 20% and 30% of retail value.

Reporting by law enforcement indicates that pawn shops may also be used or operated by criminal gangs as "front companies". Diamonds sold for cash in pawn shops are often owned by Russians affiliated with organised crime who have contracts in the Diamond District. According to the FBI it is not difficult to sell stolen property. Criminals sell stolen property at a deep discount to the pawn shops, which in turn have to negotiate with "legitimate" dealer who take stolen goods at 40% or 50% on dollar. These diamonds enter the legitimate stream of commerce in the Diamond District.

Pawn shops are required to have a license from New York to be a second hand dealer. However, the secondary market for stolen diamonds is segmented. Diamonds stolen could be "used" property or

Case 9: *Trafficking in Stolen Goods*	
they may be stolen new product from wholesalers with the "tickets" still intact. Additionally, thieves can target select high-end or estate dealers as noted above.	
Predicate offence/s	Diamond theft, robbery, burglary
Stage of Trade	Retail
ML/TF Stage	Placement of illegal diamonds or jewellery
Money/Trade flow	-
Types of financial/trade activities	-
Sums involved	-
Red flag indicators	■ Diamonds are sold for less (third to half) of their retail value, particularly if customer is not previously known ■ Links to organised crime groups ■ Frequent cash withdrawals from an account managed by jewellery dealer or pawn shop where this is unreasonable.
Source	United States (response to collection plan, 2013)

Case 10: *Buying diamond over the internet with stolen credit card numbers and laundering the goods via jewellery retailers*	
A diamond dealer has been arrested on organised crime charges allegedly laundering more than USD 100 000 in high-quality diamonds stolen by a local ring of thieves. According to court records, diamond and jewellery dealer Mr B purchased the diamonds from thieves who stole credit card information and bought the stones from Internet retailers across the country, according to the Dallas Morning News. Mr B could face five to 99 years in prison and a fine of up to USD 10 000. Mr B is one of eight people indicted in the identity-theft ring. The thieves searched trash containers for credit card receipts and then used the card numbers to purchase diamonds using a prepaid mobile phone, arranging to either pick up the stones from UPS offices or intercepting the packages as they were being delivered to the homes of the people whose identity had been stolen. Court documents charge that Mr B paid the other suspects USD 173 700 for approximately 40 stolen diamonds. The documents charge that he sold the jewellery to other retailers nationwide. It is estimated Mr B bought the stones at 50% below their real price.	
Predicate offence/s	Theft, Credit card fraud
Stage of Trade	Retail
ML/TF Stage	Placement, laundering through retail
Money/Trade flow	-

Case 10: ***Buying diamond over the internet with stolen credit card numbers and laundering the goods via jewellery retailers***	
Types of financial/trade activities	Buying diamonds with credit card online, Selling diamonds for cash
Sums involved	More than USD 100 000
Red flag indicators	■ diamonds are sold for half their value ■ customer selling diamonds at jewellers which he has no clear link to (E.g. his home and business address are remote)
Source	Open source (USA): International Diamond Exchange (2005)

TECHNIQUE: MONEY LAUNDERING THROUGH WHOLESALE AND RETAIL JEWELLERY STORES

Several cases show that these same features of the retail market described under the previous technique (*Laundering illegal diamonds via Retail level*) are exploited for ML. Proceeds generated in other predicate offences are placed in wholesale and retail jewellery store in very large amounts. As a first step in the laundering scheme these proceeds are changing their form from financial instruments received as payment for crime (cash, money orders, cheques, etc.) to diamonds and jewellery. This is done instead of depositing the proceeds of crime at a financial institution. This first stage may then be followed by using other features of the diamonds or jewellery, some of which are represented in the following cases:

- smuggling to another jurisdiction,
- using them as means of payment,
- selling the diamonds in return for payment in cash or within a financial institution locally or abroad,
- selling the diamonds over the internet exploiting the relative anonymity of the internet payment system,
- using the diamonds as a mean to store and hide wealth for long periods of time and avoid confiscation, etc.

The first case below involves a huge amount of money. Large scale ML can go unnoticed for long periods of time. This may be attributed to low level of transparency and high secrecy of the industry and to low level of enforcement. Two cases are linked to drug trafficking as a predicate offence and in a third case the predicate offence was fraud. A link to ML through gold was found in one case which is indicative of a wider link found between ML through diamonds and ML through gold based on additional cases. In one case the internet as a trading platform for diamonds was used as part of the ML scheme to quickly move the diamonds by selling them with no mark up.

Case 11: ***Laundering the proceeds of Narcotics through a jeweller (Celebrity Jeweller)***
Mr A, a New York diamond merchant, who has outfitted countless rappers and NBA players, was sentenced in 2008 to two and a half years in federal prison for lying to investigators about his part

Case 11: ***Laundering the proceeds of Narcotics through a jeweller (Celebrity Jeweller)***

in a multistate drug ring. Mr A was also fined USD 50 000, and ordered to forfeit USD 2 million to the US government.

Mr Av was arrested at his Manhattan shop in 2006 and accused of being part of a conspiracy to launder about USD 270 million in drug profits. He was among 40 people indicted in the scheme orchestrated by the Black Mafia Family, which ran drugs out of Detroit beginning in the 1990s. Mr A facilitated the purchase of jewellery utilizing drug proceeds of other defendants in order to conceal the true nature, source and ownership of the funds involved in these transactions. After receiving payments in cash, money orders and cashier checks, amounting to hundreds of thousands of dollars for each payment, Mr A would fail to report these cash payments to the IRS (Form 8300) or would falsify these records. Officials dropped the money-laundering charges against the jeweller as part of his plea agreement.

Predicate offence/s	Drug Trafficking
Stage of Trade	Wholesale
ML/TF Stage	Placement through jewellery
Money/Trade flow	-
Types of financial/trade activities	Jewellery for cash, Jewellery for money orders, Jewellery for cashier's check
Sums involved	USD 270 million
Red flag indicators	■ Jewellery is paid with money orders and cashier's check ■ Jeweller Frequently deposits money orders and cashier's check (or carrying any other financial transaction with these instruments)
Source	United States (response to collection plan, 2013), Open source

Case 12: ***Money Laundering Case Example – New York Diamond Dealer***

In 2005, Roman Nektalov, a jewellery district gold and diamond dealer, was sentenced to 10 months imprisonment for ML. The prosecution of Nektalov was part of "Operation Meltdown," an undercover investigation targeting narcotics ML activities in the 47th Street jewellery district in Manhattan.

Operation Meltdown targeted a ML method commonly used by Colombian drug traffickers. Under this method, drug traffickers and money brokers who provide laundering services to the drug traffickers employ couriers to pick up cash at designated locations and deliver the cash to gold jewellers and suppliers. The jewellers or suppliers then exchange the cash for gold, diamonds or other precious commodities, which are then smuggled to Colombia, either via couriers or hidden in cargo. Once the diamond and gold arrives in Colombia, it is sold for Colombian pesos, which are then ultimately delivered to the narcotics traffickers.

Roman Nektalov, an owner of Roman Jewellers, operated a scheme to launder what he believed to be narcotics proceeds. Cooperating Witnesses (CW) and Under Cover (UC) law enforcement agents

Case 12: ***Money Laundering Case Example – New York Diamond Dealer***

indicated that they and their associates had narcotics proceeds in the New York City metropolitan area which they wanted to exchange for gold and diamonds, and then wanted to smuggle the gold and diamonds to Colombia. In particular, at trial, the Government presented testimony and audiotape recordings of meetings in which the CW, the UC known as "Angel," and Nektalov discussed the sale by Nektalov of diamonds to the UC in exchange for cash believed by Nektalov to be drug money.

The evidence at trial showed that on 4 June 2003, Nektalov met with the CW and the UC at Roman Jewelers to exchange a large number of diamonds for USD 500 000 in cash. After the diamonds were placed on a table in a back room where the transaction was to take place, federal agents entered Roman Jewelers and arrested Nektalov seizing the diamonds.

Predicate offence/s	Drug Trafficking, Smuggling of gold, diamonds and precious commodities
Stage of Trade	Wholesale and retail
ML/TF Stage	Placement through jewellery
Money/Trade flow	United States to Colombia (smuggling)
Types of financial/trade activities	Cash payments for gold and diamonds
Sums involved	-
Red flag indicators	■ Frequent large cash purchases of diamonds ■ Link to gold
Source	United States (response to collection plan, 2013)

Case 13: ***Laundering proceeds of crime through purchase of diamonds and resale at wholesale prices to jewellers and to final customers via the internet***

This is a case where fraud was the predicate offence. The criminals had jewellery industry contacts at the wholesale level. To launder the proceeds of crime they purchased CAD 1 000 000 + of diamonds that were then re-sold back to the jewellery market and also to the general public through the internet. They did not mark up the value of the diamonds for retail purposes instead sold them to retail customs at wholesale prices and therefore moved them quickly. The diamonds were all in a size and quality class that are the most desirable and resulted a quick turn over of the diamonds. The money received from the sale of the diamonds was wired direct to their bank from the various sales locations.

Predicate offence/s	Fraud
Stage of Trade	Retail and wholesale
ML/TF Stage	Placement and layering through trade in diamonds
Money/Trade flow	-

Case 13: ***Laundering proceeds of crime through purchase of diamonds and resale at wholesale prices to jewellers and to final customers via the internet***	
Types of financial/trade activities	Wire transfers
Sums involved	CAD 1 000 000
Red flag indicators	■ Diamond bought and resold quickly ■ Diamonds are sold to retail customers at wholesale prices
Source	Canada (response to collection plan, 2013)

TECHNIQUE: LAUNDERING OF SMUGGLED DIAMONDS THROUGH TRADE SHOWS.

In the following case, smuggled diamonds are laundered through a trade show. Trade shows are held in different trade centres around the world (Hong Kong, China; Switzerland; Singapore; Israel; United States, etc.) where cash is still used to a large extent. The diamond will be sold for cash without proper certification which will then be disposed of by usual means. The case presents one of the techniques by which the illegal trade is conducted. The case also exposes the lack of expertise by custom authorities to identify diamonds that are misclassified.

Case 14: ***Selling Smuggled diamonds at gem shows***	
Homeland Security Investigations (HSI) received information that a Guinean National was attempting to sell uncut smuggled diamonds at local area Gem Shows. HSI undercover agents (UCA) conducted surveillance at several Gem Shows and negotiated with the Guinean national the sale of rough uncut diamonds from Zimbabwe. UCAs purchased one rough uncut diamond weighing approximately seven carats for USD 15 300. The subject admitted to UCAs the diamonds were smuggled to the United States and lacked the required Kimberley Certificates. During the UC meeting, two additional associates where present with a gem inventory that included rough-cut *diamonds*, *aquamarines*, and *tourmalines*. The Guinean National admitted that the rough cut diamonds had been smuggled and did not contain the Kimberley Process certificates. He also admitted that the organisation smuggles diamonds into the United States, or *misclassifies* them, depending on the quantity; and stated that the *US Customs authorities don't know what they are looking at*. An expert gemmologist certified the purchased stone was a diamond. Based on this information, HSI agents obtained a search warrant, which resulted in the seizure of 11 665 carats of rough-cut diamonds, other precious and semi-precious stones and the arrest of all three subjects. A follow-up interview was conducted with the Guinean National who admitted to have imported 12 000 carats of un-cut diamonds and *misclassified* the Customs entry paperwork as miscellaneous coloured stones. He also admitted to have purchased the diamonds from a mine in Zimbabwe from where he then flew to Thailand, then Amsterdam and arrived to the United States. All three subjects were arrested on violation of Title 18 USC 545 Importation Contrary to Law and 19 USC 3907 violation of the Clean Diamond Trade Act. It is believed that through the smuggling of diamonds, this criminal organisation generated over USD 500 000 in illicit proceeds.	
Predicate offence/s	Smuggling diamonds, misclassification of shipments in order to deceive customs authorities
Stage of Trade	Rough trading
ML/TF Stage	Layering (smuggling and moving diamonds through a number of states)
Money/Trade flow	Zimbabwe to Thailand to Netherlands to United States (illegal trade)
Types of financial/trade activities	Sale of rough stones at gem trades
Sums involved	USD 500 000
Red flag indicators	Lack of KP certificate for rough diamonds
Source	United States (response to collection plan, 2013)

TECHNIQUE: ML THROUGH DIAMOND DEALERS ACCOUNT AND USE OF A DIAMOND DEALER ACCOUNT TO TRANSFER FUNDS FOR THIRD PARTIES

Large number of cases relate to the use of diamond dealers' accounts as a conduit to transfer funds for parties not related to the diamonds trade. This technique is therefore used mainly for the

layering of funds generated in criminal activity by conducting numerous transactions between accounts to conceal their source. This is perhaps the most common activity identified in cases submitted by team members. Some of the cases show activity which may well be trade-based ML, however the information submitted refers mainly to financial transaction through the diamond dealer's account with no information as to the manner in which the trade was used to launder funds[131]. The fact that the transaction originated from, or destined for, real estate companies, charities, textile companies, metal trading companies, money service businesses, etc. is a clear indication that diamond dealers are used as a front for funds generated in criminal activity.

One of the interesting points is that this type of activity takes place in different jurisdictions[132] serving as trade centres for the diamond trade. This is indicative of the global nature of the diamond trade, the connectivity between different stages of the trade cycle and the fact that diamond dealers in many cases have an international presence and are sometimes involved in more than one stage of the trade. When a diamond dealer turns to the wrong side of things this can be exploited to transfer funds between accounts held by the same entity worldwide as part of the usual business doing.

Three cases present the activity of the diamond dealers' accounts and an additional case presents the activity of a non-diamond trade entity transferring funds to and from diamond dealers in a tax fraud case through a charity submitted by Australia. Two of the cases submitted by India and Australia show large scale ML cases amounting to tens of millions of USD.

131 TBML is dealt with as a separate method which entails use of the diamond dealer's account.

132 Australia, Belgium, India, Israel. Canada also indicated in the response to the collection plan that based on the SAR analysis, one of the red flags identified was transactions of entities not involved in the diamond trade such as construction and renovation, and the food industry.

Case 15: *Sanitised STRs relating to diamond trade Inputs from Financial Intelligence Unit*

ABC is a company represented by its directors Mr. XXX and Mr. YYY. The company opened a bank account in June 2011. The aggregate turnover in the account from April 2012 to July 2012 was INR 321 million. The total turnover in the account from July 2011 to May 2012 was INR 687 million and the average balance in the account during the period was INR 0.5 million. This triggered the suspicion that the account was being used only for *layering* of funds. The funds were received in this account through Real Time Gross Settlements (RTGS)/clearing and by transfer from other firms whose activities consisted of *real estate*, *metal trading*, *textiles*, *exporters/importers*, *diamond trade* and *steel & alloys*.

The funds were transferred to different entities whose activities were related to diamond trade. The company had also sent foreign outward remittances of INR 5.6 million to Hong Kong, China ostensibly for the purpose of import of *polished diamonds* during the period July 2011 to May 2012. The transactions happened between ABC and other diamond traders but the funds never stayed in the account of ABC except on few occasions when the funds were kept just for a day.

Mr. XXX and Mr. YYY also have their personal savings account with the same bank. An analysis of the transaction activities in this account revealed that the company used to transfer funds through RTGS to *real estate* companies and *stock-trading* firms as well. These transactions raised doubts that the company, being active in the diamond trade, may be facilitating the integration of funds received from diamond merchants in favour of real estate/share trading companies. During enhanced due diligence carried out by the bank, the directors were not forthcoming in explaining the genuineness of the transactions and as to why the fund transfers happen on the same day. The very high turnover followed by low end of day balances in the account shows that the customer was using the banking system only for fund collection and transfers.

The main points of suspicion were: 1. The operation of the account by the customer, the layering of transactions carried out by them and their business activity point to a suspicion that they may be acting as a *front for third parties*. 2. The company projected an annual aggregate turnover of INR 100 million in the account whereas the actual turnover was six times higher. 3. The fund transfers through several layers gave rise to a suspicion that the funds were transferred on behalf of certain persons to certain beneficiaries who may not have relationship with one another.

Analysis of FIU-IND's revealed heavy cash transactions in several other bank accounts of the main company and the accounts of related entities.

Predicate offence/s	-
Stage of Trade	Polished diamond trade
ML/TF Stage	Layering
Money/Trade flow	India to Hong Kong, China (money)
Types of financial/trade activities	International transfers
Sums involved	INR 687 million
Red flag indicators	-

Case 15: *Sanitised STRs relating to diamond trade Inputs from Financial Intelligence Unit*	
Source	India (response to collection plan, 2013)

The following case also demonstrates the importance of international cooperation between FIUs. This enables to confirm ML suspicions while respecting the confidentiality of the exchanged financial intelligence. After highlighting the serious ML indications, the relevant information was structured and promptly forwarded to the judicial authorities.

Case 16: *Commingling proceeds of theft in an account of a diamond trade company*	
CTIF-CFI received a disclosure from an Asian counterpart. An investigation conducted in this Asian country revealed that the main figure, of Asian origin, had deposited a large amount in cash on his account with a bank in Asia. Shortly afterwards he had these funds transferred to an account in Belgium held by a Belgian company. Based on the financial documents provided by the Asian FIU, the Belgian FIU, CTIF-CFI, was able to obtain more details on the transactions conducted in Belgium. CTIF-CFI also detected a large number of transactions that were not previously known. It became clear that the company traded in diamonds. It held an account with a bank in Belgium, on which the transfer from the country in Asia took place. The manager, of Asian origin and residing in Belgium, held power of attorney. CTIF-CFI's analysis showed that numerous transactions took place on the account: many international transfers debited and credited the account. The money he transferred from Asia to the diamond company in Belgium was clearly a layering transaction. He was suspected of ML linked to theft with violence in Asia and seemed to have used the diamond company as a cover to purchase diamonds with proceeds of this crime. Mixing funds of illicit origin with proceeds of business activities is typical of ML. The Asian FIU granted CTIF-CFI permission to use the intelligence in the request and the file was reported to the Belgian judicial authorities for theft.	
Predicate offence/s	Theft
Stage of Trade	Wholesale
ML/TF Stage	Layering
Money/Trade flow	Asian country to Belgium (Money)
Types of financial/trade activities	Cash deposits (in Asia), International transfers
Sums involved	■ Large cash deposits followed by international transactions ■ Frequent international transactions in a diamond company account (both credit and debit) without logical explanation
Red flag indicators	Belgium (response to collection plan, 2013)
Source	Theft

Case 17: *Activity in the Designated Diamond Account Deviates From Normal Practices of the Diamond Trade*

The Israel Money Laundering Prohibition Authority (IMPA) received Unusual Activity Reports (UARs) regarding person X. Analysis of the information about X revealed he held 50% of the shares of company B, operating in the diamond trade.

According to the UARs, W transferred tens of thousands of dollars to beneficiaries abroad, which did not seem to be related to the diamond trade in their countries. X transferred money to beneficiaries abroad, while the true name of the beneficiary in his order of transfer was different from the actual beneficiary stated in the Diamonds Importer Declaration form, made by him according to the AML/CFT banking order.

Moreover, X made a deposit of travellers' cheques in an amount exceeding USD 100 000 that was stated as "diamonds export return", traveller cheques as a form of payment for export return is highly irregular.

At the time, information had already been received indicating a suspicion that X had a connection to organised crime groups. The connection of X to the head of a criminal organisation raised the supposition that X assisted the criminal organisation to transfer money for its illegal operations and launder funds by giving guise of precious stones deals to the fund transfers. The information of this case was subsequently forwarded to law enforcement.

Predicate offence/s	Link to organised crime
Stage of Trade	Rough diamond trade
ML/TF Stage	Layering
Money/Trade flow	-
Types of financial/trade activities	International transfer (out), Deposit of travellers cheques
Sums involved	Over USD 100 000
Red flag indicators	■ Transfers to entities which seems to be unrelated to the diamonds trade ■ Discrepancies between names of foreign beneficiaries of the transactions in the bank account with the names of suppliers indicated on the importer declaration form ■ Unusual form of Payment in the diamond trade (use of travellers cheques) ■ link to organised crime
Source	Israel (response to collection plan, 2013)

Case 18: *Laundering of tax fraud proceeds through the diamond industry*

Over a seven-year period suspect A and his family members operated a complex ML scheme in which approximately AUD 42 million was transferred from Australia to Israel. The services provided by suspect A and his family involved the laundering of undeclared and untaxed cash from business earnings of various clients.

Suspect A opened an account in the name of a non-existent charity, a fictitious entity with no legal basis. The charity was not an incorporated company and it did not have a registered business name.

The account was used to deposit, move and launder undeclared earnings from business activities of clients of suspect A. The cash deposits made by suspect A and his family members were subsequently transferred to Israel. The funds were transferred through the bank under the guise of charitable donations. Clients used the services of suspect A specifically to launder funds with the intention of not declaring income and to avoid tax.

Suspect A also used the diamond industry to launder funds. Over a three-month period law enforcement officers observed suspect A travel from an Australian-based airport to the offices of two diamond dealers. On each occasion, suspect A left the diamond dealers' offices in possession of a plastic shopping bag which he had not taken into the dealers' offices. The following day, suspect A deposited a large amount of cash into the account of the charity and transferred the funds to Israel.

Authorities alleged that most of the money laundered by suspect A came from the cash sale of diamonds which had been imported illegally into Australia. Following the cash sale of the diamonds, the proceeds were collected by suspect A and deposited into the account of the charity. The funds were then transferred back to the overseas-based diamond suppliers under the guise of charitable donations. This method facilitated the avoidance of sales tax on the sale of the diamonds and the payment of income tax on the profits from the sale.

Enquiries identified that three bank accounts in Israel and one in Sweden received funds sent by suspect A and his family. A further two overseas-based accounts were identified. These accounts also received funds and both accounts were associated with diamond merchants in Israel and Belgium. These diamond merchants supplied wholesale diamonds to Australia.

Suspect A was convicted of conspiracy to defraud the Commonwealth and sentenced to five years imprisonment.

Suspect A's family members were convicted of conspiracy to defraud the Commonwealth and sentenced to periods of imprisonment ranging from nine months to 15 months, suspended for periods ranging from three years to five years during which, the family members are to be of good behaviour.

Predicate offence/s	Tax offences, illegal import of diamonds
Stage of Trade	Wholesale?
ML/TF Stage	placement, layering
Money/Trade flow	Belgium and Israel to Australia (trade), Australia to Israel & Sweden (money)

Case 18: *Laundering of tax fraud proceeds through the diamond industry*	
Types of financial/trade activities	Cash deposits, International transfers
Sums involved	AUD 42 Million
Red flag indicators	■ Use of account of a non-existing charity ■ Purpose of transaction (charity donation) does not correspond the activity of the account (diamond dealer) ■ Use of diamond dealer's family members to transfer funds
Source	Australia (response to collection plan, 2013)

METHOD 4: TRADE-BASED MONEY LAUNDERING AND CUSTOMS INFRACTIONS

Dealers in precious metals and precious stones are perhaps the only sector covered by the FATF 40 Recommendations in which all its activity is trade-related. By definition, almost all cases involving the use of diamonds relate to trade. Almost, since smuggling is an illegal activity outside the normal or routine trade and not part of it. Diamonds are a commodity traded worldwide through different distribution channels. This also applies to cases presented under the various methods and techniques presented in this part of the report. However, the cases presented under this method refer to specific techniques used to transfer funds through the financial system as part of a ML scheme under the guise of trade-related activity. These cases are less indicative of the characteristics of the diamonds as a commodity (diamonds as currency) or where diamonds are themselves the proceeds of crime as in the cases of theft and robbery) or where the account was just used to as a conduit to transfer funds without any reference to actual trade practices.

Some of the techniques produced by team members are known TBML techniques, such as over-valuation of the price of the traded goods as in the case provided by India, or misrepresentation of transactions as in the case provided by Israel where an "underground bank" activity was carried out under the guise of transactions misrepresented as import and export of diamonds. Where the ML activity in these two cases is conducted through trade centres and cutting and polishing centres, an additional case submitted by Sierra Leone illustrates the use of TBML in the mining sector.

As in previous cases presented, the amounts laundered in TBML cases can be huge and ML activity spans over a long period of time. In one of the cases submitted by Israel, the amounts laundered reach hundreds of millions of USD. The case presented by India exposes how through overvaluation diamonds were shipped at a value that was tens of millions of USD higher than the real value. This kind of overvaluation cannot be done in goods with a fixed or even relatively fixed price.

TECHNIQUE: ML THROUGH OVERVALUATION OF DIAMONDS

The case below submitted by India is a case of overvaluation the diamonds are exported at an extremely higher value than their real or market value. In the case of most products exported or imported, such gross overvaluation would not be possible. This kind of overvaluation cannot be done in goods with a fixed or even relatively fixed price. When the price or value of the goods shipped is more apparent, gross overvaluation may be more easily detected by customs authorities.

This case shows the level of manipulation which may be conducted through the diamond trade due to the specific characteristics of diamonds such as the very high value of the commodity and the lack of known and stable prices for diamonds which allows for the manipulation of price.

Case 19: *Overvaluation of Imports and Round-Tripping of Diamonds*[133]

Four importers of diamonds located in Surat and Mumbai imported 28 packages of rough diamonds, falling under Chapter 710231.00 of the Indian Customs Tariff Headings, from four Hong Kong, China-based suppliers. On investigation, these importers were found to have been involved in fraudulent imports by grossly overvaluing these goods to USD 544.8631 per carat, apparently with a view to transfer huge amounts of foreign exchange outside India. The goods were also not accompanied by valid Kimberley Process (KP) certificate, which is required under various regulations of the Government of India.

The consignments consisting of 28 packages of rough diamonds imported by India based importers with a declared value of **USD 98 951 493 (INR 4 880 million)** were placed under detention by Customs authorities. Subsequently, the Hong Kong, China-based exporting firms approached the Indian Customs to amend the declared value to **USD 353 328.45** (INR 17.4 million) which was not allowed by the Customs, as it appeared to be an afterthought in the light of the detention already made by the Customs. As per investigations conducted, there appears to be gross overvaluation of approximately Indian Rupees 4 860 million (USD 98.5 million) by the said companies.

All the four Hong Kong, China-based exporting firms appear to be registered in the name of the same proprietor who is an Indian national, and managed by another Hong Kong, China-based Indian national.

The table below shows the values declared before the Indian Customs and the value which was sought to be amended after detention of the goods by Indian Customs, as follows:

Name of Exporter	Original declared value (in USD) in Invoice	Value (in USD) as per revised invoice after the goods in question were detained by DRI	Difference in value (in USD)
A	24 489 997	84 787.36	24 405 209.64
B	24 585 844	90 090.07	24 495 753.93
C	21 282 561	72 906.30	21 209 654.70
D	28 593 090	104 544.75	28 488 545.25
	4538	2678.48	3857.52

Investigations have revealed that the 28 packages exported from Hong Kong, China appear to have been originally imported into Hong Kong, China from India at much lower value in the name of different Hong Kong, China-based firms. This suggests that the same diamonds have been round-tripped and brought back in India at an exorbitantly inflated price.

Further, the same four Hong Kong, China exporters have also exported 15 packages of rough diamonds at a declared value of INR 2 600 million (USD 47 million) to the same four importing firms earlier, which was cleared from Customs a week before the consignments of 28 packages were

133 Further discussion on round tripping in India was published by Chaim Even-Zohar in Evan-Zohar (2013). It was stated by Even-Zohar that a duty of 2% was put on polished diamonds import which significantly reduced this activity.

Case 19: ***Overvaluation of Imports and Round-Tripping of Diamonds***[133]

detained. The earlier consignments also appear to have been grossly overvalued and the same are also looked into by the Indian Customs.

Mr. XXX who is an authorised representative of all the four exporting companies in Hong Kong, China has earlier also come to the adverse notice of the Indian Customs in similar cases of overvaluation and circular trading of diamonds.

The investigation in this case is still going on and if the charges are proved, the offences are punishable with long imprisonment and fines.

Predicate offence/s	Fraudulent diamond import
Stage of Trade	Polished diamond trade
ML/TF Stage	-
Money/Trade flow	India to Hong Kong, China (trade) Hong Kong, China to India (Money)
Types of financial/trade activities	International transfers Export/import of polished diamonds
Sums involved	USD 98.5 million
Red flag indicators	■ Diamonds are grossly overvalued ■ Lack of valid KP certificates ■ Circular trading of diamonds ■ Proprietor and mangers of foreign counterparts Are both nationals ■ Average price per carat does not correspond to trade practices ■ Numerous counterparts are affiliated
Source	India (response to collection plan, 2013)

TECHNIQUE: PROVIDING MONEY SERVICES IN THE GUISE OF DIAMOND TRADE/USE OF FALSE INVOICES

The case below details the activity of an "underground bank" managed by a diamond dealer facilitating the transfer of large amounts of money to locations abroad to the request of the "bank's" customers. The activity is conducted by use of the diamond dealer's accounts and is declared by him to the customs and to the bank as an import and export activity, although no diamonds are being sent. In fact, these funds were received by him in cash which were then sent through his account abroad. In this manner, the diamond trade was used as a mean to transfer funds internationally through accounts of a diamond dealer. In many cases this was undeclared cash that was sent abroad so as to avoid paying tax.

Case 20: *"Underground Bank" in the guise of diamond trade*

Mr. A is a licensed diamond dealer and the owner of a designated diamonds account in a bank branch designated to serve the diamonds trade sector. In order to create import of diamonds documentation, required by the bank to conduct payment transactions, Mr. A entered Israel numerous times. He went through the customs "red Lane" and declared that he was importing diamonds purchased abroad ("by passenger" import), while actually carrying a parcel that contained low value, but good quality gems.

Later, every such shipment was presented by Mr. A in the designated customs station, operated by the Inspector of Diamonds in the Diamonds Exchange complex, for clearance. This was done after real diamonds were inserted in the shipment. There Mr. A claimed that the value of such a shipment exceeded several millions USD. Thus, A obtained a validated official importation statement from the customs which he used later at the bank to facilitate transactions abroad.

Mr. A presented the documents to his Bank together with fake invoices, to enable him to perform international foreign currency transfers to entities abroad in the guise of payment for the imported goods. Actually, these transfers did not represent any real high value acquisition of diamonds by A. The fake import was only done in order to produce the documents required by the bank to authorize the international transactions. These transactions were made to other countries for himself and other diamonds dealers wanting to receive funds abroad while avoiding questions by the bank and reports to IMPA concealing revenues and avoiding tax. Fictitious invoices were also issued to diamond dealers for the purpose of avoiding tax. In this manner Mr. A was providing money services for others of transferring funds abroad through his account in the pretence of a diamond import transaction, providing loans, discounting foreign currency checks and conversion of foreign currency.

According to open source information, indictments will be served against the entities involved, pending a hearing on suspicion of fictitious import, fictitious invoicing, tax offences and ML in amounts of many hundreds of millions of NIS (several hundred million USD).

Predicate offence/s	Smuggling/fictitious import, fictitious invoicing, unregistered MSB
Stage of Trade	Rough and polished trade
ML/TF Stage	Placement, layering
Money/Trade flow	-
Types of financial/trade activities	■ International transfers (out) ■ Physical transfer of diamonds/gems
Sums involved	Several hundred million USD
Red flag indicators	■ Frequent deposits of large FC cheques to a diamond dealer's account, particularly followed by large cash withdrawals ■ Unreasonable turnover for the diamond dealer ■ International transactions to entities not involved in the diamond trade ■ Use of fictitious documents
Source	Israel (response to collection plan, 2013)

TECHNIQUE: USE OF KP CERTIFICATE TO CONCEAL SOURCE OF ILLEGAL DIAMOND OR FOR ML PURPOSES

Case 21: *Illegal Trafficking in diamonds*

A shipment of rough diamonds arrived at Amsterdam Airport Schiphol (the Netherlands) from Dar Es Salaam, Tanzania. The airway bill indicated Brussels, Belgium, as the destination. The 2012 Kimberley Certificate (KC) specified Tanzania as the origin of the diamonds. A forensic investigation was carried out after shipment had passed and showed poorly legible stamps dating from 2007. The address of destination on the airway bill differed from the diamond dealer´s official address. It is not known whether the diamonds reached their final destination. If the KC was false, it is not possible to establish were the diamonds are coming from.

Predicate offence/s	Illegal trafficking in diamonds
Stage of Trade	Rough trade
ML/TF Stage	-
Money/Trade flow	Tanzania to Netherland (trade), Netherland to Belgium (trade)
Types of financial/trade activities	-
Sums involved	-
Red flag indicators	■ Shipment is not sent directly to destination ■ Forged KP certificate ■ Low invoice amount (possible undervaluation) ■ Fictitious legitimate origin ■ Address of destination on the airway bill differs from the Diamond dealer's official address.
Source	Netherlands

Case 22: *Operation Carbon' - Diamond fraud*

A report published by Partnership Africa Canada (PAC) in 2006 revealed a suspicion of "massive diamond fraud" in which almost half of Brazil's diamond export was fraudulent. According to PAC, the police raided three Brazilian cities in February 2006, resulting in the arrest of ten people – diamond miners, diamond dealers and money changers. Suspicions of fraud, tax evasion and ML were raised.

The case involved Mr A, a diamond dealer from Africa. Mr A was one of those arrested and was responsible for more than half of Brazil's diamond exports in 2004 (Ahmad's business exported some 54% of all Brazilian diamonds registered that year, according to Brazilian Federal Police documents). In 2005 PAC detailed a series of frauds involving one of his government-certified exports to Dubai. Mr A claimed to have purchased the diamonds from a company that in reality deals only in mineral pigments. Mr A further claimed that the diamonds had been mined in the space of seven days, from untouched ground – by a dead man (the report indicated that the sixth largest

Case 22: *Operation Carbon' - Diamond fraud*	
producer in Brazil was already dead and the fourth largest was a homeless). On top of all that, the diamonds were *undervalued* by more than USD million. Mr A's diamond smuggling operation, working under the legal cover of a company known as "Primeira Gema", used falsified documents to obtain legitimate Kimberley Certificates to obscure, or launder, the origin of his rough stones. The production statistics, the export numbers, and PAC's research all point to one conclusion: 50% of Brazil's diamond production and export was fraudulent or from highly suspect sources[134].	
Predicate offence/s	Smuggling diamonds, forgery of documents,
Stage of Trade	rough diamond trade
ML/TF Stage	-
Money/Trade flow	Brazil to Dubai (trade)
Types of financial/trade activities	-
Sums involved	-
Red flag indicators	-
Source	Open source: Partnership Africa Canada (2006a and 2006b)

TECHNIQUE: TBML THROUGH BUYING COMPANY AT THE MINING LEVEL

Case 23: *Laundering of drug trafficking proceeds through mining/buying company*	
A Foreign national registered a series of corporate vehicles including a diamond mining/ buying agency to facilitate the laundering of proceeds from alleged drug trafficking. The Law enforcement agency received a tip-off from Interpol of a possible drug trafficking ring involving the subject. Investigation revealed that the subject has received huge wire transfers of about USD 500 000 from a European country and there was no apparent justification for such proceeds. The diamond and other string of businesses were used as a cover-up to engage in more dubious business activities.	
Predicate offence/s	Drug trafficking
Stage of Trade	Mining
ML/TF Stage	Layering
Money/Trade flow	Europe (Money in)
Types of financial/trade activities	International transfers
Sums involved	USD 500 000

134 At the time Brazil suspended itself from the KPCS.

Case 23: *Laundering of drug trafficking proceeds through mining/buying company*	
Red flag indicators	Large international transfers with no apparent justification Foreign national registering numerous corporate vehicles
Source	Sierra Leone

METHOD 5: USE OF FINANCIAL HUBS AND FTZS

As mentioned at the start of this chapter, the cases that are presented here usually display more than one ML method or technique. Several cases already presented in previous chapters introduced the use of trade centres and financial hubs to launder illegally gained funds or diamonds. At the very least they presented some involvement or link to financial or trade hubs.

A significant feature of the cases below is the huge amounts of money or huge value of the diamonds laundered. The cases presented, mainly from open source information, show ML schemes amounting to ***billions*** of USD/EUROs, where the trade was conducted through trade centres such as the United Arab Emirates, Switzerland, Israel, Belgium and Panama. These cases also show additional offences committed such as smuggling, falsifying documents including invoices and large scale tax fraud. The cases show instances where the use of FTZs like Dubai or Geneva helps to lower tax payments and tax fraud, by registering the profit in the FTZ where tax levels are low.

One of the cases below (case no. 26) gives an example of the possible use of *courier services*, which form part of the industry providing services of secure transport of diamonds between different locations around the globe but also provide services as a customs agent sending and releasing diamond shipments from the customs authorities. These services were abused according to the case for smuggling, tax-evasion and ML. In another case Panama was used on the one hand as an emerging trade centre for diamonds linking the US were drug proceeds were generated and Colombia where the drug traffickers were located and as a FTZ on the other hand for the laundering of drug trafficking proceeds.

Case number 25 also illustrates a method in which the Kimberley process is circumvented by sending the diamond through the United Arab Emirates and then resending them with a certificate indicating an origin of multiple mining countries to facilitate the laundering of offences conducted in Belgium.

Case 24: *Diamonds trader involved in corruption, drugs and arms trafficking*

In 2011, a financial intermediary submitted an STR to Money Laundering Reporting Office Switzerland (MROS) concerning his client X who had made his fortune in the trade with diamonds and precious metals in Africa for counter-parts in the Middle East and the European Union. Initially, the assets were held in accounts of various branches of European banks in Switzerland. In 2004, X forwarded these assets to another foreign bank in Switzerland – which had filed the report to MROS.

Conducting research on the external database, the bank discovered that X and his company Y were subject to sanctions issued by the US authorities (OFAC Specially Designated Narcotics Trafficker Kingpin) for trafficking of weapons and drugs. X was also believed to be a member of a criminal organisation. A press article also suggested that X was involved in a case of arms trafficking,

Case 24: *Diamonds trader involved in corruption, drugs and arms trafficking*	
corruption of judges and ML in a country in South America - where he was known as a property developer. Analysis of MROS confirmed the suspicion of the financial intermediary and highlighted also other elements. Very important information was further obtained from the FIUs of other countries that have given the permission to transmit this information to the Swiss competent prosecution authorities.	
Predicate offence/s	Arms trafficking, Drug trafficking, Corruption
Stage of Trade	Rough trade (trade with diamonds in Africa)
ML/TF Stage	Layering
Money/Trade flow	-
Types of financial/trade activities	National transfers
Sums involved	-
Red flag indicators	■ Link to criminal organisations ■ Money transfer from various accounts to another account managed in foreign banks
Source	Switzerland (response to limited collection plan, 2013)

Case 25: *Laundering illegal diamonds through smuggling and financial hubs*	
Police in Antwerp investigated a massive diamond fraud in which a family smuggled diamonds worth an estimated EUR 1.3 billion over the course of several years. The family has not been named, and most of the income from the scheme is thought to have been exported to Lebanon. The investigation started with a warning from the state security service that the family had connections with known dealers in illegal diamonds. The diamonds were allegedly brought into Antwerp and the takings then exported, both undocumented, to evade huge sums in tax. The illegal diamonds, including stones originating from conflict zones (possible conflict diamonds) were mixed with legal diamonds and the whole shipment KPC indicated that the origin of the diamonds was from multiple mining countries. . The family managed to get around the Kimberley system by passing the stones through the United Arab Emirates and Switzerland before bringing them into Belgium. Meanwhile, the profits were laundered by means of false invoices and fake bookkeeping.	
Predicate offence/s	Smuggling diamonds, Tax evasion/Tax fraud, false invoices, fake bookkeeping
Stage of Trade	Rough trade
ML/TF Stage	-
Money/Trade flow	Lebanon (money in), Belgium (commodity in), United Arab Emirates (commodity in/out), Switzerland (commodity in/out)

Case 25: *Laundering illegal diamonds through smuggling and financial hubs*	
Types of financial/trade activities	
Sums involved	EUR 1.3 billion
Red flag indicators	■ Connections with known dealers in illegal diamonds ■ Documents seems to be forged
Source	Open source: Flanders today (2012)

Case 26: *Use of Companies in a FTZ - Diamond fraud*	
This case involves a large scale fraud which targeted 220 suspects. According to open source the fraud was estimated at EUR 800 million. The investigation concerned 220 individuals, including 107 diamond traders and companies charged with falsifying documents, ML and criminal conspiracy. The case centres on Company A, which once held a quasi-monopoly on diamond delivery, but which was closed down by authorities in 2005 after a courier was stopped with a huge sum of cash. Investigation suggested the company was using the *free trade zone* in Geneva, which is intended to simplify customs restrictions, to smuggle diamonds and escape tax. Swiss authorities cooperated and turned over more than 35 000 seized Company A shipping dossiers, which showed that diamonds supposedly for export, were instead rerouted to Antwerp to be sold on the black market. The 220 suspects have been identified from four fraud circuits used by Company A to launder money and avoid tax. In 2012, the case came to court. The prosecution charged 36 diamond companies and 96 people on various counts, main case being fraud. Eleven of Monstrey's employees were charged with running a courier service that transferred diamonds and jewellery without proper legal disclosure. The case presented to the court discusses EUR 66.7 million.	
Predicate offence/s	Tax fraud, forgery of documents, smuggling
Stage of Trade	Rough and polished trade
ML/TF Stage	-
Money/Trade flow	-
Types of financial/trade activities	-
Sums involved	EUR 66.7 million
Red flag indicators	Documents seems to be forged
Source	Open source: Flanders today (2013), International Diamond Exchange (2012)

Case 27: *Tax fraud and ML through financial/trade hubs*

Company D, a major market maker, came under investigation, and its executives fled Belgium, when an employee of the company revealed in 2006 how Company D had traded diamonds out of Africa for years, avoiding taxes by transacting deals through Dubai, Tel Aviv and Geneva, then moving the profits back to Belgium. The former employee is a native of Belgium with Israeli citizenship who has also spent years in Africa and Southeast Asia.

The charges allege that Company D traded diamonds out of Angola and Congo over a period of years, avoiding tax by moving the transactions through Dubai, Switzerland and Israel. Representatives from the company allegedly earned billions of Euros by buying diamonds cheaply on the black market in Angola and the Democratic Republic of the Congo. They then traded the stones to companies in Dubai, Tel Aviv and Geneva for profit and laundered the proceeds. Later they sold the diamonds to companies in Belgium, in price only slightly larger than they paid in Dubai and Geneva – so they paid tax in Belgium only on the gap between these rates were systematically neglected.

Officials who investigated the case believe that Company D did not declare considerable amounts of its profits and moved cash overseas. It is believed to have laundered money through a complex scheme of around two dozen firms and banks around the world managed by family members of the two key suspects.

Early This year it was published that in a settlement between Company D and the Belgian authorities Company D has agreed to pay a sum of EUR 150 million.

Predicate offence/s	Fraud, Tax evasion/Tax fraud
Stage of Trade	Rough diamond trade
ML/TF Stage	-
Money/Trade flow	■ Angola (commodity out), Congo (commodity out), Dubai (commodity in/out), Tel Aviv (commodity in/out), Geneva (commodity in/out), Belgium (commodity in/out) ■ Dubai (money in/out), Tel Aviv (money in/out), Geneva (money in/out), Belgium (money in)
Types of financial/trade activities	International transfers
Sums involved	EUR 2 – EUR 3 billion
Red flag indicators	Many firms and bank accounts are opened by family members
Source	Open source

Case 28: *Laundering drug proceeds through a wholesale jeweler located abroad*

More than USD 40 million worth of gold, silver and jewellery forfeited in international ML case.

US indictment of an offshore business engaged in the illicit black market peso exchange, an ML operation through which narcotics proceeds earned in the United States are exchanged for Colombian pesos and then used to purchase goods in the *Colon Free Zone in Colon, Panama*. During the course of the investigation, two natural persons were identified as major money launderers based in Panama. The two used a wholesale jewellery business, engaged in the sale of gold and silver jewellery and precious metals to many retail and wholesale customers throughout Central and South America and in Europe and the Middle East, and a related company to facilitate their illegal ML activities.

Based on a joint investigation conducted by the US and Panama, the natural persons and the related companies were charged with laundering millions of dollars in narcotics proceeds through the said companies in Panama.

According to evidence presented in the case, drug proceeds from the United States were sent to Panama through cash pick-ups, wire transfers, cashier's checks and third party bank checks. Through the companies, which together did more than USD 100 million in business annually, the two natural entities knew that the primarily South American-based customers were laundering millions of dollars in drug money from the United States through bulk purchases of jewellery. According to court documents, the companies were heavily involved in the black market peso exchange.

On 17 May 2006, a US District Court Judge signed a final order of forfeiture directing that the government of Panama transfer custody of the assets seized in Panama to the government of the United States. The assets transferred to the United States include approximately 468 boxes of gold and silver jewellery, as well as gemstones and watches, weighing ten tons, seized from the wholesale jewellery company.

From the judgment:

"*A primary modus was to sell jewellery to drug lords, knowing that it was being paid for with drug money, thus allowing them to convert dirty money into glistening clean jewellery.*"

Predicate offence/s	Drug trafficking
Stage of Trade	Wholesale
ML/TF Stage	Placement and layering
Money/Trade flow	■ United States to Panama (Money) ■ Panama to Colombia (Jewellery)
Types of financial/trade activities	■ Cross-border cash pick-ups, wire transfers, cashiers checks and third party bank checks ■ USD exchanged to Colombian pesos
Sums involved	USD 40 million worth of jewellery forfeited

Case 28: *Laundering drug proceeds through a wholesale jeweler located abroad*	
Red flag indicators	■ Use of cashier's checks and third party bank checks to purchase jewellery ■ Deposit of cashier's checks and third party bank checks to an account managed by a wholesale/retail jeweler. ■ Unusual international transaction/checks in large sums transferred/ deposited to a wholesale/retail jeweler ■ Funds are transferred from a different country than the commodity is sent to
Source	Open Source: US Department of Justice (2013), US District Court (nc)

METHOD 6: SMUGGLING OF DIAMONDS AND CASH

Diamonds are smuggled into jurisdiction for several purposes:

a) Sale of illegally gained diamonds or jewellery, either by illegal mining, by theft or robbery or by criminals accepting diamonds as forms of payment and laundering them through smuggling abroad.

b) Hide value and store wealth in another jurisdiction thus avoiding confiscation.

c) As part of a ML scheme to sell diamonds and jewellery bought with proceeds of crime.

d) As part of a TF scheme were diamonds are bought with clean money with a purpose to finance terrorist organisations.

Cases regarding smuggling of diamonds were provided by a majority of team members: Australia, Austria, Belgium, Canada, Israel, the Netherlands, Russia, Sierra Leone, South Africa and the United States. Open source information provides additional examples of instances were smuggling of diamonds occurred in Brazil, South Africa and Israel. These cases provide a clear indication that the illegal trade exists. Within the framework of this report it is not possible and outside the scope of this project to establish the extent of the illegal trade. However cases provided by team members, discussions held at team meetings and open source information indicate that illegal trade is a significant problem. Illegal trade may facilitate all the purposes detailed above.

Two cases also show the smuggling of cash by diamond dealers. Cash transactions are part of the diamond trade. In instances where the trade is used to launder illegally gained funds, cash transactions may also be used. Smuggling of cash may be part of a ML scheme, or may also be done as part of a scheme to avoid tax payments.

Case 29: *Trafficking of illegal diamonds and jewellery*
Mr. N, an Indian national who arrived on a flight from Dubai, was stopped for customs inspections by officials at a Moscow airport while attempting to pass through the Green Corridor for passengers who have nothing to declare. The ensuing luggage inspection and body search produced several pieces of jewellery (pendant and earrings) and a total of 30 401 natural diamonds valued at RUB 4 691 047, all of which were confiscated.

Case 29: *Trafficking of illegal diamonds and jewellery*	
Predicate offence/s	Smuggling diamonds
Stage of Trade	Illegal rough trade, illegal jewellery trade
ML/TF Stage	-
Money/Trade flow	United Arab Emirates to Russia
Types of financial/trade activities	Physical transfer of diamonds
Sums involved	RUB 4 691 047
Red flag indicators	-
Source	Russia (response to collection plan, 2013)

Case 30: *Smuggling polished diamonds*	
South African police have arrested a man who they say swallowed 220 polished diamonds in an attempt to smuggle them out of the country. The man was arrested as he waited to board a plane at Johannesburg airport. Officials said a scan of his body revealed the diamonds he had ingested, worth USD 2.3 million (GBP 1.4 million; EUR 1.8 million). The man was travelling to Dubai. According to the information, authorities believe the man belongs to a smuggling ring. Another man was arrested in March also attempting to smuggle diamonds out the country in a similar way.	
Predicate offence/s	Diamond smuggling
Stage of Trade	-
ML/TF Stage	-
Money/Trade flow	South Africa – Commodity Out Dubai – Commodity In
Types of financial/trade activities	-
Sums involved	USD 2.3 million
Red flag indicators	-
Source	South Africa (response to collection plan, 2013) Open Source: BBC (2012)

Case 31: *Trade in illegal diamonds*	
A Diamond Exchange has blown the whistle on one dealer who seems to be actively engaged in trading with Venezuela. The dealer, who was claiming to represent the diamond exchange, said that he was a member of the another Diamond Exchange and the WFDB. It was said that he had even submitted a request, in the name of the diamond exchange, for the government of Panama to declare his business premises as a 'Free Zone'". In the absence of official Kimberley Certification, Venezuelan rough diamonds sold by the dealer in the diamond exchange are illegal.	
Predicate offence/s	Smuggling diamonds, forgery of documents
Stage of Trade	Rough diamond trade
ML/TF Stage	-
Money/Trade flow	Venezuela to Panama (suspected smuggling)
Types of financial/trade activities	-
Sums involved	-
Red flag indicators	lack of KP certificate for rough diamonds or indication that the certificate is forged
Source	Open source: Tacy Ltd (2008)

Case 32: *Diamond smuggling network*	
An investigation of a suspected tax evasion case of a woman who operated a small kindergarten led to the discovery of a diamond smuggling network. According to the tax authorities the network operated in Israel, Belgium and Russia. During the kindergarten inquiry, investigators found that the owner's husband had travelled abroad 245 times in the past eight years, on trips that usually lasted just two days. During the investigation, 15 men and women were arrested, all suspected of being involved in the smuggling ring. The suspects were relatives who have allegedly carried out more than 500 such diamond operations in a value of hundreds of thousands of USD and were paid USD 600 per trip plus travel expenses. Among the suspects are hi-tech executives and an education advisor. The report adds that the diamonds were hidden inside "private" body parts.	
Predicate offence/s	Smuggling
Stage of Trade	-
ML/TF Stage	-
Money/Trade flow	■ Russia to Israel, Belgium to Israel (illegal trade) ■ Israel to Belgium, Israel to Russia (illegal trade)
Types of financial/trade activities	-

Case 32: *Diamond smuggling network*	
Sums involved	Hundreds of thousands of dollars
Red flag indicators	■ Family members involved ■ Frequent travels abroad
Source	Open source: Haaretz (2008

TECHNIQUE: CASH SMUGGLING BY DIAMOND DEALER

Case 33: *Cash smuggling by an employee of a diamond company*	
An employee of a Diamond company was found in possession of large amount of cash on the way from South Africa. The cash was found hidden. The suspect failed to satisfactorily explain the source of the cash. The cash was confiscated and the suspect was charged with contravening the Prevention of Organized Crime Act, 2004 (Act No. 29 of 2004). Further net worth analysis is being conducted on the suspect.	
Predicate offence/s	Customs infractions
Stage of Trade	-
ML/TF Stage	-
Money/Trade flow	South Africa to Namibia (money)
Types of financial/trade activities	Physical transfer of cash
Sums involved	-
Red flag indicators	Cash transactions conducted by an employee of a diamond company
Source	Namibia (response to collection plan, 2013)

Case 34: *Smuggling of cash by a diamond dealer and international transfers from entities not related to the diamond trade through a Diamond Dealer account*
Person A was caught by customs upon leaving the country, carrying cash in an amount higher than the amount he actually declared. Further inquiries made by the Israel Money Laundering Prohibition Authority (IMPA) revealed many UARs according to which person A was involved in several companies operating in the diamond trade. The inquiries also revealed that person A made thirteen customs declaration with reference to trans-border foreign currency transfers made by him between the years 2003-2008. The declarations showed discrepancies and errors in the data provided by person A in the declaration forms e.g., omission of letters from his name, misrepresentation of his ID number, illegible data, insertion of his passport number in place of ID number, in a manner that render the relevant data almost impossible for collation and retrieval. Person A's bank transactions were matched with dates of his exits and entries from\to the country.

Case 34: ***Smuggling of cash by a diamond dealer and international transfers from entities not related to the diamond trade through a Diamond Dealer account***

This showed additional instances where a few days after his arrival to the country a foreign currency deposit in a sum higher than the declaration threshold was made to his bank account without person A submitting a currency declaration to the customs during his entry to the country.

Moreover, STRs regarding Designated Diamonds Accounts of companies that A was connected to showed that the banks reported the transfers of value for exports from a foreign entity that was not known to be a trader in diamonds. The name of the entity was similar to names of an MSB. IMPA submitted a request for information to another FIU that confirmed the suspicion that the creditor company was known as a money services bureau.

This affirmed the suspicion that A used his Designated Diamonds Accounts as a "pipeline" to perform large foreign currency transfers, posturing as payments related to diamonds export / import activity.

Person A was brought before a sanctions committee which decided on imposing a financial sanction of ILS 80 000. After an appeal the amount was reduced to ILS 7 500.

Predicate offence/s	Cash smuggling
Stage of Trade	-
ML/TF Stage	Placement and layering
Money/Trade flow	-
Types of financial/trade activities	Cash deposit, International transfers
Sums involved	-
Red flag indicators	■ Discrepancies and errors in provided data (customs declaration) ■ Proximity between entering to the country and deposits of foreign currency to the account ■ Deposits of foreign currency to a diamond dealer's account without customs declaration about entering money to the country ■ Transactions in a diamond account to/from money service business
Source	Israel (response to collection plan, 2013)

METHOD 7: LINK WITH OR USE OF GOLD AND/OR OTHER PRECIOUS STONES TRADE

Several cases presented above display a link between ML through diamond and ML through other precious stones and/or gold. Since the project initially focused on both diamond and other precious stones, relevant cases were provided before the scope of the project was narrowed down to diamonds only. Few additional cases display similar links. This is just an initial indication that gold and/or other precious stones are used in ML schemes. Further research is required to understand

the characteristics of the trade in these commodities and to establish their vulnerabilities to ML and TF and the extent they are used in practice for ML and TF purposes.

Case 35: ***Link between proceeds of drug trafficking and diamond jewellery used as currency***	
This case involves a drug courier/trafficker who was found carrying CAD 40 000 worth of drug money. The courier's cash bag also contained a quantity of *diamond* jewellery and loose *sapphire gemstones* that collectively were valued at CAD 60 000. The jewellery had been appraised by a third party. The appraisal value listed the jewellery for its cash value if it were sold as wholesale (just below wholesale). (Aside for the appraisal obtained, the jewellery trade is not as yet being engaged in this case as the diamonds/gemstones is being used between criminals as an alternate currency).	
Predicate offence/s	Drug trafficking
Stage of Trade	Appraisal
ML/TF Stage	-
Money/Trade flow	-
Types of financial/trade activities	Physical transfer of cash Physical transfer of diamond jewellery
Sums involved	CAD 60 000
Red flag indicators	■ Request for an appraisal for high value jewellery where source of stones is not clear ■ A customer (not a diamond dealer or a jeweller) requests wholesale price on jewellery he tries to sell.
Source	Canada (response to collection plan, 2013)

CHAPTER 9.
TERRORIST FINANCING THROUGH TRADE IN DIAMONDS[135]

Only a few cases were provided by team members with regard to TF related to the trade in diamonds. Additional information based on SAR analysis was provided by Canada and the United States. The SARs and one of the cases provided by the United States are related to the Lebanese-Canadian bank (see case 37 below). While indications of involvement of terrorist organisation in the diamonds trade may be traced in open source information[136] such indication are at this point limited to the cases received from team members[137].

TECHNIQUE: CAPITAL INCREASE TO SUPPORT A TERRORIST NETWORK

Case 36: *Capital increase to finance terrorism*

The Belgian FIU CTIF-CFI, received a disclosure from an auditor regarding company A. He noticed that Mr. X, manager of company A, carried out a capital increase of several million EUR. The auditor found it suspicious that the origin of the funds was unknown. Moreover, company A appeared to be a dormant company.

Apart from a disclosure by the auditor, the notary executing the deed and the bank holding company A's account also disclosed these facts to CTIF-CFI. Through the capital increase by means of a contribution in kind Mr. X obtained a majority interest in company A.

Mr. X was a candidate refugee from the Middle East. Company A was a night shop, which is considered to be a sensitive business with regard to TF. Multiple cash deposits were carried out on company A's account. Mr. X was known to the police for ties with a terrorist organisation. He was suspected of employing illegal foreigners and using the night shop's profits to finance terrorist activities. Part of the night shop's profits was sent to the Middle East to support a terrorist network.

Furthermore, certain elements revealed a link between the invested funds and conflict diamonds of terrorist groups. This reinforced the serious indications of TF.

Predicate offence/s	Terrorist Financing, trade in conflict diamonds

135 FIU sanitized cases, Law enforcement, open source cases / investigation.

136 In April 2003 global witness published a report claiming to present "evidence that confirms that Al-Qaeda has been involved in the rough diamond trade since the 1990s. Firstly in Kenya and Tanzania and then in Sierra Leone and Liberia, where they began to show an interest in diamond trading in 1998, following the crackdown on their financial activities in the wake of the US embassy bombings in Kenya and Tanzania." See Global Witness (2003).
Additional information was published in: Republic Of Liberia Truth And Reconciliation Commission (2009), *pp.* 30.
See also Farah, Douglas (2005): "Diamonds have also been used extensively by Hezbollah and other terrorist groups in the Middle East that have a long tradition of access to diamonds in West Africa ".

137 Two cases were also provided in FATF (2003) typologies report which included a section on diamonds.

Case 36: *Capital increase to finance terrorism*	
Stage of Trade	Wholesale
ML/TF Stage	-
Money/Trade flow	Europe to the Middle East (Money)
Types of financial/trade activities	Cash deposits, capital increase
Sums involved	Millions of EUR
Red flag indicators	■ Unknown origin of funds ■ Use of a dormant company ■ Use of sensitive business (night shop) ■ Multiple cash deposits followed by international transfers ■ Link with terrorist organisation
Source	Belgium (response to collection plan, 2013)

TECHNIQUE: USE OF LEGITIMATE BUSINESSES

Similar to regular ML cases, legitimate businesses are often used as a cover to funnel funds to terrorist organisations. The involved entities are also using money coming from diamonds smuggling or drug trafficking to support these organisations.

Case 38 is an open source case and therefore has few indicators on the *modus operandi*. Although there were indications of terrorist support in the United States, the main subject wasn't convicted for this in Belgium.

Case 37: *Car businesses to transport value*
An investigation by the Drug Enforcement Administration (DEA) and other federal law enforcement agencies discovered a scheme to launder money through the United States financial system and the United States used car market. As part of the scheme, funds are transferred from Lebanon to the United States in order to purchase used cars, which were are shipped to West Africa and sold for cash. Cash proceeds of these car sales are then transferred, along with the proceeds of narcotics trafficking and other crimes, to Lebanon. The cash is often moved through bulk cash smuggling. In 2012, the US District Court-Southern District of New York (SDNY) issued a civil ML complaint and "in rem" forfeiture action involving a number of Lebanese financial institutions and exchange houses. The SDNY civil complaint stated that prior to being identified as an entity of primary ML concern by FinCEN in a Section 311 (of the U.S.A. Patriot Act) Action, Lebanese Canadian Bank (LCB) had poor anti-ML controls and, indeed, knowingly conducted business with Hizballah-controlled entities and individuals and entities linked to, among others, African diamond smuggling, ML, and narcotics trafficking. The SDNY civil complaint also mentioned that the LCB maintained a banking relationship with individuals and entities involved in the African diamond smuggling trade. In all, hundreds of millions of USD a year went through the accounts, held mainly by Shiite Muslim

Case 37: *Car businesses to transport value*	
businessmen in West Africa, many of them known Hezbollah supporters, trading in everything from **rough-cut diamonds** to cosmetics and frozen chicken, according to people with knowledge of the matter in the United States and Europe. The companies appeared to be serving as fronts for Hezbollah to move all sorts of dubious funds, on its own behalf or for others. The system allowed Hezbollah to hide not only the sources of its wealth, but also its involvement in a range of business enterprises.	
Predicate offence/s	Diamond smuggling and drug trafficking
Stage of Trade	
ML/TF Stage	
Money/Trade flow	■ Lebanon (Money IN) ■ West Africa (Cars OUT) ■ Lebanon (Money OUT)
Types of financial/trade activities	
Sums involved	
Red flag indicators	■ Use of legitimate business ■ Goods used to transfer money ■ Link with terrorist organisation ■ Bulk cash smuggling
Source	The United Sates (response to collection plan, 2013) Open source: The New York Times (2011)

Case 38: *Cover companies to transfer money*
The U.S. Department of the Treasury designated Kassim Tajideen and Abd Al Menhem Qubaysi, two Africa-based supporters of the Hezbollah terrorist organisation. Under E.O. 13224. E.O. 13224 targets terrorists and those providing support to terrorists or acts of terrorism by freezing any assets the designees have under US jurisdiction and prohibiting U.S. persons from engaging in any transactions with them. Kassim Tajideen is said to be a financial contributor to Hezbollah who operated a network of businesses in Lebanon and Africa. He has contributed *tens of millions of dollars* to Hezbollah and has sent funds to Hezbollah through his brother, a Hezbollah commander. In addition, Kassim Tajideen and his brothers run cover companies for Hezbollah in Africa. In 2003, Tajideen was arrested in Belgium in connection with fraud, ML, and diamond smuggling. Abd Al Menhem Qubaysi was a Cote d'Ivoire-based Hezbollah supporter and was the personal representative of Hezbollah Secretary-General Hassan Nasrallah. Qubaysi communicated with Hezbollah leaders and has hosted senior Hezbollah officials traveling to Cote d'Ivoire and other parts of Africa to raise money for Hezbollah. Qubaysi played a visible role in Hezbollah activities in

Case 38: ***Cover companies to transfer money***	
Cote d'Ivoire, including speaking at Hezbollah fundraising events and sponsoring meetings with high-ranking members of the terrorist organisation.	
Predicate offence/s	Terrorist financing, fraud, ML and diamond smuggling
Stage of Trade	
ML/TF Stage	
Money/commodity flow	Open source: US Department of Treasury (2009)
Source	Terrorist financing, fraud, ML and diamond smuggling

Canada submitted three cases which were linked to a listed terrorist organisation in Canada. The first case involved several jewellery businesses, some of which were suspected of sending funds to the terrorist organisation. Some of the jewellery businesses were located in Canada, as well as in two foreign jurisdictions (hereafter referred to as Country A and Country B).

The similarity of the business names, and the fact that many were registered and operating at the same address, made it challenging to follow the flow of funds. Some of the businesses ordered funds to the benefit of other jewellery businesses located in Country A and two other jurisdictions.

Another case involved an STR that was reported on a jewellery business that is believed to support a listed terrorist organisation in Canada. Again, this case involved similar jewellery business names registered and operating from the same address. The jewellery business ordered funds from Canada to the benefit of other jewellery entities in Country B.

One final case connecting the diamond industry to potential terrorist financing activities is that of an individual who was intercepted by foreign authorities with diamonds. According to the case, it was suspected that the individual was acting on behalf of a terrorist organisation.

In the framework of a SAR analysis, the United States also submitted several SARs that reported suspected terrorist financing activities, including overall transactions totalling over ***USD 3 billion***. The SARs appear to report newly identified transactions involving activities that occurred as long as 10 years ago involving individuals who have since been designated as terrorists by the US Department of the Treasury, Office of Foreign Assets Control (OFAC). Others reported newly identified transactions involving now-closed Lebanese banks that enabled Hezbollah fundraising transactions.

CHAPTER 10.
MONEY FLOWS RELATING TO SUSPECTED ML/TF RELATED TO THE DIAMONDS INDUSTRY

Some limited information was collected for the study on money flows pertaining to suspected ML/TF, as they relate to the diamond industry. Information is particularly scarce with regard to TF, where flows are typically quite small. Many countries noted that they have reported very few suspicious transactions to their FIUs involving the trade of diamonds and other precious stones.

Some overall trends can be noted, however, and in some countries, typical financial flows can be discerned through sanitised cases and reports from FIUs.

Generally, there has been a trend away from purely cash transactions, likely due to ML/TF requirements in the precious stones sector introduced several years ago. The most commonly used methods of payment by precious stones dealers are cash deposits and national and international transfers. Many countries noted funds transfers to high-risk countries, including those where a significant diamond trade does not exist. Multiple cross-border transfers enable layering of transactions to take place.

Where countries provided information on money flows pertaining to suspected ML/TF as they relate to the diamond industry, it is included below.

Australia did not provide aggregate information on suspected illicit financial flows; however, its case studies included an example whereby funds (primarily resulting from undeclared and untaxed cash from business earnings) were transferred from Australia to Israel under the guise of charitable donations. The transfers also involved the proceeds from the cash sale of diamonds to bank accounts in Israel and Sweden; the accounts were linked to merchants in Israel and Belgium. Another example cited by Australia involved financial flows relating to a money exchange business operating in South-East Asia.

Belgium provided significant analysis on money flows related to ML. A trend was noted whereby diamonds and funds formerly flowed from Africa directly to Antwerp; however, more recently both diamonds and funds transit through the United Arab Emirates. Financial flows in 105 disclosures of cross-border cash movements involving diamonds show that the majority of the funds were physically transported to Belgium from Congo (DRC); Hong Kong, China; Japan; and Thailand. The main countries of destination were France; Guinea; Hong Kong, China; Italy and South Africa. With regard to suspected trafficking of diamond cases in 2011-2012, the majority of funds were transferred internationally to Belgium from accounts from Hong Kong, China; India; Israel; the United Arab Emirates and the United States. Nearly 60% of funds were transferred to United Arab Emirates and Switzerland from Belgium. In other cases of suspected ML related to diamonds (predicate offences besides illicit trafficking of diamonds), the financial flows were mostly transfers in USD sent from India, Israel and Switzerland to the United Arab Emirates. Belgium also noted the

use of numbered[138] accounts in foreign countries (Liechtenstein and Switzerland) to conceal transactions. A major problem is the identification of the actual/principal beneficiary of incoming or outgoing international transfers on the account of diamond companies.

In Canada, diamond money-laundering schemes appear to frequently relate to drug trafficking. Illicit financial flows are most often between Canada and the United States. Other countries include Belgium, Cambodia, China, Israel, Panama and Switzerland.

India reported a relatively large number of sanitised cases (12) in which suspicious transaction reports were received. In these specific cases, Hong Kong, China is a destination for illicit cash flows related to the diamond trade.

Israel reported that international bank transfers were the most common method of payment used. In the case of unusual activity reports (UARs), major financial transfers occurred from Switzerland (28% of the total amount), Cyprus (15%) and Hong Kong, China (13%). Some of the countries sourcing funds (*i.e.,* Cyprus, Panama) do not appear in the customs export data. This means that funds are coming from countries to which diamonds are not exported. According to reports disseminated to law enforcement, major amounts come from Belgium (52%), United States (28%) and Great Britain (15%). Among the reported countries of destination, major amounts are going to China (30%); United States (26%); Hong Kong, China (20%); and Switzerland (10%).

Namibia identified South Africa and ZAR currency transactions as being the most commonly used.

The Netherlands noted that it is a transit country for diamonds into and out of the European Union, because diamonds are transported by airplane and Schiphol airport offers a wider range of destinations. Nonetheless, it had very few cross-border transactions relating to diamonds reported as suspicious.

The Russian Federation only cited examples where the predicate offence involved the smuggling of diamonds, notably from Dubai and Thailand. However, one case pertained to a company specializing in the unauthorised distribution of diamonds, the proceeds of which were transferred to the bank accounts of foreign companies in Israel and Hong Kong, China.

In the United States, diamond money laundering schemes appear to frequently relate to the trafficking of drugs and stolen goods. The United States noted that, based on their SAR analysis, no significant specific trends or patterns appeared to be particularly unique to diamond trading. The examined SARs revealed patterns of incoming and outgoing wire transfers involving multiple and regionally diverse countries that often appeared as points of transaction origin, destination, transit, a suspect's domicile, and/or location of foreign-based financial institution accounts. These include:

- Angola
- Austria
- Botswana

[138] A numbered bank account is a type of bank account where the name of the account holder is kept confidential, and they identify themselves to the bank by means of a code word known only by the account holder and a restricted number of bank employees, thus providing accountholders with a degree of bank privacy in their financial transactions.

- Belgium
- Brazil
- British Virgin Islands
- Canada
- Czech Republic
- China
- India
- Israel
- Latvia
- Lebanon
- Liechtenstein
- Mauritius
- Panama
- Peru
- Portugal
- Russia
- Sierra Leone
- St Vincent and the Grenadines
- Switzerland
- The United Arab Emirates
- The United Kingdom
- The United States

In the United States, diamond money-laundering schemes appear to frequently relate to the trafficking of drugs and stolen goods.

CHAPTER 11.
MAIN FINDINGS

Diamond trade, as an international phenomenon, needed a complete and global analysis to understand and determine ML and TF threats and vulnerabilities related to this unique trade. This report has aimed not only to provide a general overview of the diamond trade with its specific business practices, funding methods and risks, but also seeks to highlight a number of significant issues that require further consideration. The report has identified different issues that require consideration as to the sufficiency of the current measures mitigating new risks (see next chapter for issues for consideration).

In the process of this project, a sample of 17 countries submitted contributions. All contributions have been relevant to the project and have helped to address the questions that were raised at the beginning of this project.

TRADE PRACTICES AND FIGURES

344. Some important changes within the trade practices were identified such as a reduced use of cash, the appearance of new trade centres like China, India and the United Arab Emirates, Botswana becoming a trade centre due to the move of De Beers from London to Gaborone, De Beers no longer being an all-inclusive monopoly opening the diamond industry to more trade actors, an increase in interest from several diamond producing countries in diamond beneficiation, the emergence of synthetic diamonds and the Internet as a new trade platform for diamonds.

345. KP public statistics and other open sources provided a general overview of the trade in rough and polished diamonds. These figures show that almost 80% of the mining activity is concentrated in the Botswana, Canada, Democratic Republic of Congo, Russian Federation, Zimbabwe and that China, after India, is becoming a major cutting and polishing centre. In 2012, Belgium, Israel, Switzerland and the United Arab Emirates were the main trade centres for rough diamonds and the United States had the largest consumer market for polished diamonds (jewellery). What stands out from the figures is the change in the role played by the United Arab Emirates, and its significance in terms of the worldwide rough diamond trade and indications on the role it might have on ML/TF activity.

LEGISLATION AND REGULATION

Diamonds have been recognised by the FATF as vehicles for laundering the proceeds of crime and therefore diamond dealers were included in the definition of Designated Non-Financial Business and Profession (DNFBP). Specific attention goes out to the fact that Recommendation 22 on customer due diligence for DNFBPs and Recommendation 23 on other measures for DNFBPs are only based on cash transactions. All other transactions in which diamond dealers are or could be engaged in are not covered. With regard to Recommendation 32 it can be stated that diamonds are not included in the definition of currency or bearer negotiable instruments. Therefore, countries are not required to have measures in place to detect the physical cross-border transportation of

diamonds through a declaration/disclosure system, even though cases show considerable use of cross-border value transfer via the use of diamonds.

Although specific FATF Recommendations are applicable to diamond dealers, several countries have not yet implemented these in their national AML/CFT legislation. In those countries that do have national AML/CFT regulation on diamond dealers, the overall compliance of the sector is assessed to be medium. Only in a few countries are licences and registration required for business activity in the diamond trade. Although there are supervisory authorities, no sanctions were imposed in the last two years, an indication of the low level of enforcement in the sector.

348. Cross-border transportation of diamonds falls under customs control. There are some major differences between countries, especially on polished stones. In most of the countries there are no specific import export controls on diamonds and none of them have specific AML/CFT requirements where one has to declare diamonds when entering/leaving the country.

FUNDING OF THE TRADE

The trade is primarily funded by financial institutions such as banks. Several countries have specialised diamond banks or designated divisions or branches that diamond dealers must use for doing business and/or that provide financial services to them. In most countries, the banks and credit institutions do not apply special “know your customer” or due diligence procedures to diamond dealers. The main methods of payment used by diamond dealers are wire transfers or electronic funds transfer. The use of cash is still a common method of payment in the diamond business in countries where cash is widely used such as in mining centres like some African and Latin American countries, or in trade centres like Hong Kong, China.

THREATS, VULNERABILITIES AND RISKS

The different and unique characteristics of diamonds and the diamond trade make the industry vulnerable to ML and TF. The diamond supply chain in all of its stages, from production to consumption, can be the gateway to profitability, for laundering proceeds of crime, for ML and for moving proceeds of crime into the financial system. It is important to keep in mind that the complexity of the international diamond trade means that the ML and TF vulnerabilities and risks may differ from one segment of the "pipeline" to another and from one jurisdiction to another. For example whereas mining countries are facing the threat of illegal mining, trade centres are more vulnerable to transfer pricing. Cutting and polishing centres have to be more aware of the fact that diamonds become untraceable. Retailers are faced with other criminals that use their business to launder their proceeds of crime. Nonetheless theft, commingling and smuggling of diamonds can occur at all stages of the trade.

Diamonds can be used to earn, gain or store value, and are easily moved or smuggled. Their low weight, very high value, high durability, exchangeability for other commodities, ability to remain undetected, changeability, unsteady price and the ease in which they can be traded outside the formal banking system are just some of the characteristics that make them vulnerable to ML/TF and other crimes such as theft.

The fact that diamonds are used as an alternative currency by criminals who use them to acquire other goods (such as tobacco, guns, and drugs) is important to note, since diamonds are not included in the concept of cash/currency or a bearer negotiable instrument (FATF Recommendation 32). The emphasis on cash transactions (Recommendation 22) only and the fact that several countries have not yet subjected diamond dealers to AML/CFT legislation causes major vulnerability in international and national legislation. Cases show that criminals are taking advantage of this vulnerability. Few compliance assessments on diamond dealers have been carried out, no fines have been issued and no other AML/CFT civil enforcement actions have taken place in the last two years. Enforcement of the diamond sector is also exposed to a degree of vulnerability due to limited awareness of the sector, lack of evidence to collect and difficult international police cooperation. The low number of successful cases that were reported to judicial authorities or brought before court can be seen as a major vulnerability in the prevention of ML/TF. All these figures show low levels of enforcement which may be the outcome of the complexity of the industry, traditional ethics of trust of within the sector and the lack of sufficient expertise of relevant regulating and law enforcement bodies.

The concerns related to KP certificates are the fact that current enforcement efforts related to diamonds are directed more at ensuring compliance with the KPCS rather than preventing smuggling, fraud, or ML; there is no transparency for controlling officers at the border; the ease with which new KP certificates can be issued by authorities and the requirement of KP certificates only for import and export of rough diamonds alone. In this respect the KP certificate might also serve unintentionally as a ML tool since the existence of the certificate may signify that the source is legitimate overlooking ML/TF considerations. It should be considered that the localization of the beneficiation process may be a possible way to circumvent the purpose of the KP since exports will turn to be more of polished diamonds where KP certificates is not required.

In earlier studies, diamonds were also identified as goods that are more susceptible to TBML due to the difficulty in identifying the true value of the goods. The diamond industry is tremendously vulnerable to TBML primarily because of the high subjectivity in the valuation of diamonds, the ability of diamonds to change their form, the trade-based and global nature of the diamond market, the high value of the product which may facilitate large scale ML/TF and the long production chain involving many actors. In some countries the tariff for customs declarations is based only on carat, which creates a gap within the export/import systems which may be easily exploited for over/under valuation while making it hard to establish whether there is an infringement of customs laws and regulation.

The Internet, being a relatively new trade platform, not only entails vulnerabilities that may be applicable to all sales and purchases on the Internet (fraud with online rough diamond sale) but also create specific vulnerabilities related to KYC/CDD measures. Not only the increased anonymity of the customer but also the fact that almost all payments are facilitated through banking and credit institutions or Internet payment means (which are not covered by FATF Recommendation 22) make it harder to conduct and enforce proper KYC/CDD procedures and conduct investigations if such a case arise. Another upcoming technique is the laundering of stolen diamonds via the 'Darknet', where jewellery with diamonds is sold on the 'silk road' using e-currency such as 'bitcoin'.

With regard to the financing of the trade, several vulnerabilities and risks appear. Advance payments, return shipments, fork transactions, deficiencies in the KYC procedure, the use of cash, consignment agreements and promissory notes create opportunity for ML/TF.

Although cash is diminishing for large-scale business to business (B2B), cash usage still poses a risk for ML/TF in the diamond trade. At retail level, where cash is a frequent means of payment, not all countries have proper AML/CFT legislation to report cash transactions above a specific threshold. Vulnerabilities also arise when diamond trade credit is extended at concessionary terms, thus making it more attractive in comparison to rates of credits in other sectors.

The free and unrecorded circulation of promissory notes, which may take a bearer negotiable instrument form, creates an unofficial and unmonitored "banking system" which provides financing for traders, outside the official banking system, facilitates the transfer of high value assets and makes it possible to avoid KYC procedures and reporting to the FIU with no audit trail of the transaction. Although consignment agreements are a very common trade method, especially in international trade, they may bear some ML/TF risks. These risks are linked to the potential variation of the prices of the diamonds evaluated (over or understated), and to the possibility of fraud committed by the consignee.

RED FLAG & INDICATORS

This report provides red flags and indicators to identify potential ML/TF activity through the trade in diamonds, which are divided into several categories. The first category of indicators is intended for regulated entities and covers many indicators which would perhaps be relevant to other types of financial activities but that should be addressed from a diamond trade perspective and requires a good understanding of the diamonds trade practices. They are related to trade practices, to transactions/financing of the diamond trade, customer profile, use of third parties and the use of missing/suspected/falsified documents. The second category of red flags and indicators is targeted at diamond dealers and jewellers themselves and refers to the sale/purchase of diamonds or jewellery, the customer/supplier, use of third parties and the use of missing/suspected/falsified documents. The last category is aimed at customs officials and gives indicators related to the export and import of diamonds.

CASE STUDIES

The case studies illustrate the ML/TF methods and techniques used in the diamond industry in its various stages. Besides the more conventional cases of ML, this report also provided several sanitised cases where diamonds are used as an alternative currency (for asset movement, storage and protection) and a few cases related to TF. What is of importance is the fact that many cases illustrate that criminals are taking advantage of the vulnerabilities entailed in the trade, many of these vulnerabilities were identified in the relevant sections of this report. It is not possible to ascertain, within the scope of this research, the level of risk posed by the diamonds trade, but the cases presented are an indication of such risk, which may be seen for example in the large volumes of ML the cases present.

In total, 64 cases were received from team members or located in open source analysis conducted as part of the information collection process. An analysis of the means of payment revealed:[139]

a) In 30 cases non-cash payment means were used.

b) In 19 cases cash was used as payment method.

c) In 30 cases there is no indication as to the payment method (many cases involve smuggling and/or the use of diamond as currency).

d) In only 6 cases the only method of payment used was cash.

The cases collected show very large scale money laundering, which spread across jurisdictions involving different trade centres and may even amount to few billions of dollars. One case of "round tripping" shows overvaluation where by the diamonds are imported at a much higher value than their market value and the value in which they were exported. This is one example showing the level in which the price of the diamond might be manipulated in a TBML case. Other cases show large scale smuggling and very large tax fraud and money laundering cases.

Finally, it was noted that in most large scale theft or robbery cases, which may amount to many tens of millions of dollars, the diamonds are almost never found. This shows the ease in which illicit diamonds can be laundered through the diamond trade but also the possible ease in which money may be turned into diamonds and laundered in the same way.

CONNECTION TO TF

Based on the information that was received from all countries involved in the project, experts in the diamond trade and literature review, no hard evidence was found that proved a strong link between the diamond trade and terrorist financing activities. Some indications were found but the risk of misuse of the sector for TF purposes does not seem higher than in other sectors.

MONEY FLOWS

The last section of the report looked at money flows pertaining to suspected ML/TF, as they relate to the diamond industry. Although information was scarce, some trends were noted. There has been a trend away from pure cash transactions and many countries noted funds transfers to high-risk countries, including those where a significant diamond trade does not exist.

139 Some cases feature more than one payment method.

CHAPTER 12.
ISSUES FOR CONSIDERATION – SUGGESTED WAYS TO MITIGATE RISKS TO THE DIAMONDS TRADE

There appear to be a number of issues that could be considered to improve the capacity to mitigate the ML/TF risks associated with the trade in diamonds.

Building a better awareness: Criminals use creative schemes to exploit the diamond sector. Lack of awareness of ML and TF risks associated with diamonds and the trade in diamonds could contribute to the risks of ML/TF posed by the abuse of the trade. This lack of awareness amongst key players about their role in the process of fighting illicit activities is a significant vulnerability, particularly since certain expertise is required to improve understanding and awareness. Understanding the ML/TF risks associated with the trade in diamonds by government bodies and the private sector, including financial institutions, would assist in addressing this vulnerability and taking any needed steps to mitigate the risks. Awareness-raising may prove to be very useful by enhancing enforcement of existing regulation. This would require resources for outreach, training or other cooperative activities, and may result in enhanced information exchange.

FATF Recommendation 22 and 23 are only based on cash transactions. The findings of the reports point to issues that may be considered by the FATF with respect to the extent cash is used in the trade and the risks identified in the research, which are not related to the use of cash.

Some jurisdictions as well as private sector response stated that almost no cash is used, particularly not in international trade. On the one hand this reduces the risk of laundering cash proceeds of crime. On the other hand, since the FATF diamond dealer definition covers only cash-based transactions when a diamond dealer[140] is engaging in a transaction with a customer, then most of the trade in terms of volume (carat) and value (tens or even hundreds of billions of USD) is not covered by AML/CFT requirements. However, the report notes that these parts of the trade are still vulnerable to ML/TF, while the current FATF Recommendations applicable to diamond dealers do not directly address such risks.

AML/CFT duties are dependent on the form of payment which in many cases is not known until a substantial period of time has passed from the day in which the diamonds were sold. Since diamonds themselves can be used in ML and TF schemes, the transaction and the laundering process may be completed with no requirement for CDD or suspicious activity reporting at the time of the transaction.

Consideration should be given by the FATF to broadening AML/CFT duties to non-cash payment means.

FATF Recommendation 32: Countries are currently not required to have measures in place to detect the physical cross-border transportation of diamonds through a declaration/disclosure system. The report noted that diamonds were often moved across borders as part of ML/TF

140 As previously indicated the FATF recommendations applies to DPMS which include diamond dealers.

schemes allowing for the cross-border transfer of very high value. The report also showed the use of diamonds as currency by criminals. While a person who would transfer cash or other negotiable bonds would be required to declare the amounts he is carrying, when transferring the same value by using diamonds he is not required to declare. The FATF may wish to consider including diamonds in a similar manner as cash/currency or as bearer negotiable instrument.

Definition of a diamond dealer: There is no definition given by FATF of a dealer in precious stones (which includes a diamond dealer). This results in different national legislation and interpretation of diamond dealers. Pawn shops and retailers are often not seen as diamond dealers and therefore not under any national AML/CFT legislation and regulation. Consideration should be given to defining a dealer in precious stones including a diamond dealer, which could mitigate the risk of ML/TF.

Enhancing transparency through cooperation with the private sector: Although the sector is specialised and there are barriers to entry, engagement with the private sector during this project has indicated that they are not unwilling or reluctant to cooperate. In general, AML/CFT authorities need a better understanding of legitimate commercial practices for diamonds (including KPCS functions) as well as what they perceive as suspicious, and the measures taken to mitigate the risk.

TBML: A significant risk as shown by some of the cases is large scale TBML through the trade in diamonds. Countries do not always have experts or risk-based control on diamonds import and export. More inspection by expert gemmologists working within or on behalf of customs may mitigate the risks for TBML and narrow the room for price manipulation through international trade.

Availability of information: Information on the diamonds trade was assessed low to medium by the jurisdictions who participated in the project. Most information collected for the project came from FIUs, law enforcement and private sector along with information through investigational analysis by way of statistical accounts. The collection and availability of more complete information by all AML/CFT stakeholders involved in the trade in diamonds would support a more accurate and complete understanding of the ML/TF risks associated with the diamonds trade.

International co-operation: Difficulties in the international exchange of information and the use of tax havens are major obstacles in the detection and prosecution of ML through the trade in diamonds. Since the trade is multi-jurisdictional, involving several countries from mine to market, a multi-jurisdictional cooperation is required to investigate ML/TF cases. International co-operation and information-sharing are key factors in the fight against ML given the international dimension of the market. Countries need to work cooperatively to identify and combat the use of diamonds for ML/TF purposes.

Regulatory level playing field: Given the international character of the trade in diamonds, it is important to encourage a level playing field for AML/CFT regulation. Where there are major discrepancies between jurisdictions, this may attract criminals to conduct their transactions in jurisdictions with low or no AML/CFT regulation on the diamonds trade. For a sector which is mainly based on trust and long-lasting partnerships, the application and enforcement of the AML/CFT legislation and the obligation of diamond dealers to collect identification documents from each client and report suspicious transactions, has a large impact on the competitiveness vis-à-vis diamond dealers in other countries who are not subject to similar obligations. This may have the

adverse effect of diverting the diamonds trade to less regulated jurisdictions, generating higher levels of ML/TF risks associated with the diamonds trade. When analysing the over-all level of risk associated with a particular jurisdiction the FATF may consider the level of risk posed by the local diamond industry.

National risk assessment- With respect to jurisdictions where diamonds trade is a significant part of the economy or where trade volumes are high, relevant national authorities should incorporate the diamonds trade as part of their national risk assessment and impose proportionate AML/CFT measures.

ANNEX 1 – GLOSSARY OF TERMS

Alluvial mine – mines in which diamonds are recovered from deposits such as river bed and ocean floor contrary to a kimberlitic hard rock mine. These are considered to be secondary deposits, *i.e.,* that diamonds from primary kimberlitic mines were washed away. Alluvial mines may spread over huge geographical areas.

Business to Business (B2B) - commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.

Broker – a person mediating between a seller and a buyer, usually for a commission. The level of involvement of the broker may vary between one who only mediates between a buyer and a seller to a broker who perform the sale, receives payment from the buyer and transfers the funds to the seller.

Conflict diamonds – according to the Kimberley process web site a "*conflict diamonds, also known as 'blood' diamonds, are rough diamonds used by rebel movements or their allies to finance armed conflicts aimed at undermining legitimate governments*"[141].

Diamond Bourse – a bourse is the diamond industry term for a diamond exchange centre, located in large cities and providing secure trading environments for diamond dealers. Bourses are self-governing, setting sales standards and arbitration provisions. There are 28 diamond bourses members in the WFDB. In a way, the bourses have developed some "universal diamond trading laws". Disciplinary action in one bourse, which may include membership suspension or even expulsion, will automatically apply in every single diamond bourse in the world. Therefore members of the diamond bourses prefer trading among themselves, as they have comfort in verbal agreements. WFDB commented that the strength of this legal framework also means that the bourses can compel members to, for example, adhere to the Kimberley Process, refrain from mixing natural and synthetic diamonds, enforce the writing of warranties on invoices, etc. Dispute resolution, sometimes involving millions of dollars, is immediate – without a need for court actions. WFDB commented that in virtually every diamond trading country, arbitration decisions by WFDB affiliated bourses are generally automatically confirmed by courts.

Diamond dealer – since the scope was narrowed to diamonds excluding other precious stones the report will in many cases address diamond dealers only. The term refers to a person dealing in rough or polished loose diamonds (unless otherwise specified).

"Diamond pipeline" – a term refers to the whole diamond trade chain from mining to retail level where the diamonds reach the final customer.

Harmonized Commodity Description and Coding System (HS) - An internationally standardised system of names and numbers for classifying traded products. The system was developed and is maintained by the World Customs Organization.

141 See FAQ on the KP web site - www.kimberleyprocess.com/en/faq.

Kimberlitic Mine – named after Kimberley, South Africa where a hard rock pipe was first found. These are hard rock mines where diamonds are located. The diamonds were brought to the surface by magma flowing from deep within the earth[142].

Kimberley Process (KP) – *"The Kimberley Process is an international certification scheme that regulates trade in rough diamonds. It aims to prevent the flow of conflict diamonds, while helping to protect legitimate trade in rough diamonds"*[143].

Kimberley Process certification scheme (KPCS) – an international initiative aimed at preventing conflict diamonds from entering legitimate trade. It seeks to ensure that diamond purchases are not used to finance violence by rebel movements seeking to undermine legitimate governments. The KPCS imposes extensive requirements on its members to certify shipments of rough diamonds as 'conflict-free'. The KPSC also bans trade in rough diamonds with non-participants to reduce the illicit trade in conflict diamonds.

Polished Diamond – a diamond which has been cut and polished from a rough diamond to gain its final shape which will then be used in diamond jewellery.

Loose diamond – cut and polished diamonds which have not yet been set in jewellery.

Mounted diamond – a polished diamond which was set in jewellery such as ring, watch necklace, etc.

Rough Diamond – a diamond in its rough form before being cut and polished.

Synthetic diamonds – man made diamonds which are manufactured by artificial means.

Other precious stones – the term refers to all precious stones apart from diamonds.

Beneficiation –The term has been used to describe the process whereby more stages of the "pipeline" mainly but not limited to cutting and polishing are conducted in the mining country generating additional economic benefits to the mining country[144].

142 See http://science.howstuffworks.com/environmental/earth/geology/diamond1.htm.

143 See FAQ on the KP web site - www.kimberleyprocess.com/en/faq.

144 See for example www.israelidiamond.co.il/english/news.aspx?boneid=741&objid=3138. See De Beers policy for beneficiation www.debeersgroup.com/Operations/Sales/About-Benefication/

ANNEX 2 – PREDICATE OFFENCES RELATED TO THE DIAMOND TRADE

	Australia	Belgium	Canada	India	Israel	Namibia	Netherlands	Russian Federation	Sierra Leone	South Africa	United Kingdom	United States
Fraud	+	+	+		+			+	+		+	+
Theft/robbery	+		+							+	+	+
Drugs trafficking		+	+						+		+	+
Cigarette trafficking		+										
Trade in Conflict Diamonds		+	+									+
Trade in/possession of illegal diamonds						+		+				
Link to Criminal Organisations		+	+									+
Tax/Customs offences		+			+		+					+

ANNEX 3 – BIBLIOGRAPHY

BOOKS

Even-Zohar, C. (2004), Diamond Industry Strategies to Combat Money Laundering and Financing of Terrorism, ABN AMRO, 191 p.

Even-Zohar, C. (2007a), From mine to mistress- Corporate strategies and government policies in the international diamond industry, Mining Communications Ltd, 943 p.

Even-Zohar, C. (2007b), Diamond mining in the world, policies and strategies of the diamond mining countries, Hebrew edition, Tacy Ltd., 395 p.

Lallemand, A. (2012), *L'Anvers du diamant*, Lannoo Editions, Belgium, 160 p.

Robinson, J. (2003), *The Sink: How the real world works- Terror, Crime and Dirty money*, McClelland & Stewart Ltd, Toronto, Canada, 288 p.

Ross, K. (2008), *The Fifth "C": The criminal use of diamonds*, universe-Indigo, 200 p.

Siegel, D. (2009), The Mazzel Ritual: Culture, Customs and Crime in the Diamond Trade, Springer, 244 p.

OTHER

APG (2012) "*Typology Report on Trade Based Money Laundering*", www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

Antwerp World Diamond Centre - www.awdc.be/en/homepage, accessed October 2013.

Antwerp World Diamond Centre (nc), *Antwerp Diamond Tender Facility,* www.awdc.be/nl/antwerp-diamond-tender-facility, accessed October 2013.

Bain & Company (2011), *The Global Diamond Industry, Lifting the Veil of Mystery*, www.bain.com/Images/PR_BAIN_REPORT_The_global_diamond_industry.pdf

Bain & Company (2012), *The Global Diamond Industry, Portrait of Growth*, www.bain.com/publications/articles/global-diamond-industry-portrait-of-growth.aspx

BBC (2012), *South Africa holds diamond smuggler who swallowed 220 gems*, BBC, London, United Kingdom, www.bbc.co.uk/news/world-africa-20330080

Cuyvers, L.; De Ruyver, B. & Vander Beken, T. (2004), *Measuring the vulnerability of legal economic sectors for organised crime*, Science Policy Office, Brussels, Belgium, p. 13.

CNN (2013), *33 arrests in Belgium diamond heist*, 8 May 2013, http://edition.cnn.com/2013/05/08/world/europe/belgium-heist-arrests.

De Beers (nc), *Beneficiation program*, www.debeersgroup.com/en/Operations/Sales/About-Benefication/, accessed October 2013.

Diamonds A to Z (nc), *The diamond Industry*, www.photius.com/diamonds/the_diamond_industry.html, accessed October 2013.

Diamond Shades (n.c.), Diamond Charts, www.diamondshades.com/diamond-industry/charts-diamond-prices/diamond-charts/polished-diamonds-charts/, *accessed October 2013.*

Even-Zohar, C. (2013), *Diamond Intelligence Brief,* 6 Feb. 2013, Vol.28, No.745

Farah, Douglas (2005), *Terrorist Responses to Improved U.S. Financial Defenses*, Testimony of Douglas Farah before the House Subcommittee on Oversight and Investigations, www.investigativeproject.org/documents/testimony/231.pdf

Farah, Douglas (n.c.), *Press Release: Blood From Stones, The Secret Financial Network of Terror,* www.douglasfarah.com/reviews/press-release.php, accessed October 2013.

FATF (2003), *Report on Money Laundering Typologies 2002-2003*, www.fatf-gafi.org/documents/documents/moneylaunderingtypologies2002-2003.html

FATF (2008a), *RBA Guidance for Dealers in Precious Metal and Stones*, www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Dealers%20in%20Precious%20Metal%20and%20Stones.pdf

FATF (2008b), *Best Practices Paper on Trade Based Money Laundering*, www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf

FATF (2010) "*Money Laundering Using New Payment Methods*", www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

FATF (2012) , 40 *Recommendations*, www.fatf-gafi.org/recommendations.

Flanders News (2012), *"Perfect" synthetic diamond scam in Antwerp, 27 November 2012,* www.deredactie.be/cm/vrtnieuws.english/News/1.1491172

Flanders Today, Belgium - www.deredactie.be/cm/vrtnieuws.english, accessed October 2013.

Flanders Today (2012), *Massive diamond fraud uncovered,* www.flanderstoday.eu/current-affairs/massive-diamond-fraud-uncovered

Flanders Today (2013), *Diamond fraud case targets 220 suspects,* www.flanderstoday.eu/content/diamond-fraud-case-targets-220-suspects

GAO (2002), *International trade - Critical issues remain in deterring conflict diamond trade*, Gao-02-678, www.gao.gov/assets/240/234898.pdf

GAO (2003), *Terrorist Financing - U.S. agencies should systematically assess Terrorists' use of Alternative financing Mechanisms*, GAO-04-163, www.gao.gov/new.items/d04163.pdf

Global Witness (2003), *For a Few Dollars More, How Al Qaeda moved into the diamond trade*, www.globalwitness.org/sites/default/files/import/Few%20Dollars%20More%200-50.pdf

Haaretz (2008), *Tax Authority stumbles onto diamond-smuggling ring after questioning tax evador*, Tel Aviv, Israel, www.haaretz.com/print-edition/business/tax-authority-stumbles-onto-diamond-smuggling-ring-after-questioning-tax-evader-1.251282

IMF (2010), 'IMF Project to Help Africa Crack Down on Illicit Diamond Trade', *IMF Survey Magazine*, Washington, United States, www.imf.org/external/pubs/ft/survey/so/2010/new031210a.htm

International Diamond Exchange (2005), *Dallas Diamond Dealer Arrested on Laundering Charges*, IDEX Online, www.idexonline.com/portal_FullNews.asp?id=24507.

International Diamond Exchange (2012), *100 on Trial as Monstrey Case Arrives at Antwerp Court,* IDEX online, www.idexonline.com/portal_FullNews.asp?id=36774

JCK (2012), *Undisclosed Synthetc Diamonds Appearing on Market,* 21 May 2012 www.jckonline.com/2012/05/21/undisclosed-synthetic-diamonds-appearing-on-market.

Jewish Daily Forward (2013), *'Pink Panther' Heist of Jewish Diamond King Levl Leviev in Cannes Soars to $136 M*, http://forward.com/articles/181367/pink-panther-heist-of-jewish-diamond-king-lev-levi/.

Kimberly Process (2012), *Annual Global Summary: 2012 Production, Imports, Exports and KPC Counts*, https://kimberleyprocessstatistics.org/static/pdfs/public_statistics/2012/2012GlobalSummary.pdf, accessed October 2013.

Kimberly Process, public area statistics, https://kimberleyprocessstatistics.org/ , accessed October 2013.

Kimberly Process (nc), *KPCS Core Document*, www.kimberleyprocess.com/en/kpcs-core-document, accessed October 2013.

Logan, Samuel (2009), *Dirty Diamonds in Panama*, International relations and security network, ISN, Zurich, Switzerland, www.isn.ethz.ch/Digital-Library/Articles/Detail/?lng=en&id=108972.

Nelson, D.; Collins, L. & Gant, F. (2002), *The Stolen Property Market in the Australian Capital Territory,* Australian Institute of Criminology for the ACT Department of Justice and Community Safety; www.aic.gov.au/publications/previous%20series/other/41-60/the%20stolen%20property%20market%20in%20the%20australian%20capital%20territory.html

Partnership Africa Canada (2006a), "Massive Brazilian Diamond Fraud", *Other Facets,* June 2006, Ottawa, Canada, www.pacweb.org/images/PUBLICATIONS/Other_Facets/OF_20-Eng.pdf

Partnership Africa Canada (2006b), "Fugitives and Phantoms: The Diamond Exporters of Brazil", PAC, the Diamonds and Human Security Project, Occassional Paper #13, Ottawa, Canada, www.ddiglobal.org/login/Upload/fugitives%20and%20phantoms-web-final.pdf.

Pricescope (nc), *Round cut diamond prices | pricing for round shaped diamonds,* www.pricescope.com/diamond-prices/round, accessed October 2013.

RAPAPORT, www.diamonds.net, accessed October 2013.

Republic Of Liberia Truth And Reconciliation Commission (2009), *Volume Three: Appendices, Title III: Economic Crimes And The Conflict, Exploitation and Abuse*, http://trcofliberia.org/resources/reports/final/volume-three-3_layout-1.pdf.

Responsible Jewellers Council (2009), *Principles and Code of Practice*, section 1. 2 on Money Laundering and the Finance of Terrorism, London, United Kingdom, www.responsiblejewellery.com/files/RJC_Prin_COP091.pdf

Statistics on polished diamond trade - www.diamondshades.com/diamond-industry/charts-diamond-prices/diamond-charts/polished-diamonds-charts/, *accessed October 2013.*

Smoking Gun (2007), The case against Jacob the Jeweler, www.thesmokinggun.com/file/case-against-jacob-jeweler, accessed 10 October 2013

Tacy Ltd (2008), 'Smuggled Venezuelan rough channelled through Panama', *DIB Online*, 28 November 2013, Ramat Gan, Israel, www.diamondintelligence.com/magazine/magazine.aspx?id=7454

The New York Times (2011), *Beirut Bank Seen as a Hub of Hezbollah's Financing,* New York, United States, www.nytimes.com/2011/12/14/world/middleeast/beirut-bank-seen-as-a-hub-of-hezbollahs-financing.html?pagewanted=all&_r=0

The New York Times (2013), *Raids Yield Stolen Gems and Arrests in Europe,* New York, United States, www.nytimes.com/2013/05/09/world/europe/in-raids-across-europe-police-recover-some-diamonds-stolen-in-50-million-theft.html?_r=1&

Time (2012) an article published on Aug 20, 2012, in the TIME magazine - http://world.time.com/2012/08/20/not-just-out-of-africa-south-americas-blood-diamonds-network/.

TP Analytics (n.c.), *What is Transfer Pricing,* www.tpanalytics.com/learning-resources/what-is-transfer-pricing/, accessed November 2013.

US Department of Justice (2007), *Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting,* Washington, United States, www.justice.gov/opa/pr/2007/April/07_crm_301.html

US Department of Justice (2013) – 'More than $40 Million Worht of Gold, Silver and Jewelry Forfeited in International Money Laundering Case', *Justice News*, Washington, United States, www.justice.gov/opa/pr/2010/April/10-crm-395.html

US Department of Treasury (2009), *Treasury Targets Hizballah Network in Africa* , Washington, United States, www.treasury.gov/press-center/press-releases/Pages/tg149.aspx

US District Court (nc), United States vs Speed Joyeros, S.A.; Argento Vivo, S.A.; Yardena Hebroni a/k/a Yardena Hevroni; and Eliahu Mizrahi – Memorandum, Order and Judgment, Eastern District Court of New York, 00 CR 960 (JBW), New York, United States, www.nyed.uscourts.gov/sites/default/files/opinions/00cr9605902.pdf, accessed August 2013.

World Federation of Diamond Bourses (nc), *Listing Bourses,* www.wfdb.com/index.php?option=com_content&view=category&id=9&Itemid=17, accessed October 2013.

World Diamond Council, *Diamondfacts.org* - *www.diamondfacts.org, accessed October 2013.*

World Diamond Council (nc), *Alluvial Diamond Mining Fact Sheet,* www.diamondfacts.org/pdfs/media/media_resources/fact_sheets/Alluvial_Mining_Background.pdf, accessed October 2013.

World Diamond Council (nc), Alluvial Diamond Mining Fact Sheet, www.diamondfacts.org/pdfs/media/media_resources/fact_sheets/Alluvial_Mining_Background.pdf, accessed October 2013.